IL CYBERSPACE

Caratteri e riflessi sull'ordinamento internazionale

Università degli Studi di Roma La Sapienza
XXXI Ciclo di Dottorato in Ordine Internazionale e Diritti Umani

Introduzione

Il presente lavoro, svolto durante il corso di dottorato in Ordine Internazionale e Diritti Umani, intende osservare i riflessi sull'ordinamento internazionale del processo di affermazione del Cyberspace a partire dai suoi caratteri qualificanti.

In questa prospettiva il capitolo iniziale si occupa di delineare i caratteri e le dinamiche proprie dello spazio informatico evidenziando, da un lato, il valore, all'interno della società, dell'informazione e delle tecniche volte alla sua rilevazione, memorizzazione, manipolazione e comunicazione. Dall'altro, come i fondamenti teorici su cui poggiano le tecnologie ITC qualifichino il Cyberspace quale autonomo fattore di progresso della società oltre che come spazio di interazione tra attori. I caratteri propri delle tecnologie ITC mostrano, infatti, lo sviluppo di peculiari dinamiche proprie del progresso tecnologico in grado di determinare il progresso della Società Internazionale e dell'Uomo.

I riflessi dello sviluppo delle tecnologie informatiche sulla Società Internazionale vengono presi in analisi nella prima parte del secondo capitolo nella quale sono trattati i temi del Cyber power e delle forme e strumenti del suo esercizio all'interno delle relazioni internazionali. Aspetti che incidono sulla condotta delle relazioni internazionali in particolare per quanto attiene ai temi della sicurezza e della pace internazionali. La seconda parte del capitolo pone attenzione alle dinamiche economiche determinante dallo sviluppo tecnologico e intende evidenziare i fattori alla base di problematiche sociali in grado di incidere sul progresso dell'Uomo.

Il terzo capitolo prende in considerazione l'azione delle Nazioni Unite rispetto ai temi del progresso scientifico e tecnologico e permette di rilevare le problematiche finora emerse in materia. I documenti analizzati evidenziano lo sviluppo di tre aree tematiche principali relative alla tutela della sicurezza e della pace internazionale, allo sviluppo di una cultura globale della sicurezza, sia delle infrastrutture informatiche sia del loro utilizzo e, infine, alla promozione e tutela dei diritti umani nel Cyberspace. Le tre aree tematiche vengono sviluppate dalle Nazioni Unite all'interno della più ampia prospettiva politica volta alla costruzione di una *Società della Conoscenza*.

Sulla base di quanto osservato rispetto ai caratteri del Cyberspace, ai mutamenti dei fattori delle relazioni tra Stati e all'azione delle Nazioni Unite, i successivi capitoli prendono in considerazioni i temi della governance dello spazio informatico e i problemi che lo sviluppo tecnologico pone sul piano del diritto internazionale.

Il quarto capitolo si occupa dei modelli di governance dello spazio informatico mettendo in evidenza, in ragione del particolare ruolo qui svolto dagli attori privati, lo sviluppo di processi multistakeholder entro una governance caratterizzata dall'interazione tra i diversi regimi normativi.

Il quinto capitolo, infine, analizza i riflessi dello sviluppo del Cyberspace sul diritto internazionale. Nella prima parte vengono prese in considerazione le problematiche che lo spazio informatico determina sul sistema delle fonti internazionali. La seconda parte, con riferimento alle tre direttrici dell'azione delle Nazioni Unite, prende in considerazione alcuni dei principali problemi e sviluppi nell'interpretazione e nell'applicazione del diritto internazionale rispetto alla sicurezza internazionale, alla sicurezza dello spazio informatico e alla tutela e promozione dei diritti umani.

Per quanto attiene alla metodologia la presente tesi muove dalla ricostruzione dell'oggetto di studio, il Cyberspace, per poi osservarne il rapporto con il piano delle relazioni internazionali e, infine, i principali riflessi sul piano giuridico.

Rispetto alle fonti utilizzate per lo svolgimento dell'analisi si è fatto riferimento a testi di natura storica, scientifica, strategica ed economica per quanto riguarda i primi due capitoli. Nel terzo capitolo si è fatto esclusivamente riferimento ai documenti elaborati in sede di Nazioni Unite al fine di rilevare le questioni principali finora emerse sul piano internazionale. I temi della governance multistakeholder sono stati affrontati nel quarto capitolo con riferimento a testi di teoria delle relazioni internazionali. Per lo sviluppo degli aspetti di diritto internazionale si è fatto riferimento ai manuali, ai testi e agli articoli scientifici maggiormente accreditati. Sul piano giurisprudenziale, data l'estrema novità della tematica, si è fatto riferimento a pregresse sentenze degli organi giurisdizionali internazionali al fine di delineare i principali problemi di interpretazione e applicazione del diritto internazionale al Cyberspace quale emergente spazio di interazione tra attori internazionali e fattore di sviluppo della Società Internazionale e dell'Uomo.

Capitolo I

Fondamenti e struttura del Cyberspace

Capitolo II

L'influenza del Cyberspace sulle relazioni internazionali

Capitolo III

Le Nazioni Unite e il processo di rilevazione e definizione delle problematiche del cyberspace

Capitolo IV

Modelli di governance nel dominio informatico

Capitolo V

L'influenza del Cyberspace sul diritto internazionale

Capitolo I

Fondamenti e struttura del Cyberspace

Introduzione; 1. L'Informazione; 1.1 Linguaggi e strumenti di comunicazione; 1.2 Le innovazioni dei supporti alla comunicazione quale fattore di progresso; 2. L'interdisciplinarietà dei fondamenti del cyberspace; 2.1 La Cibernetica; 2.2 Il Network quale supporto per la condivisione della conoscenza; 2.3 L'Intelligenza Artificiale; 2.4 Il Cyberspace quale spazio unitario; 3. La struttura del Cyberspace; 3.1 Il livello fisico; 3.2 Il livello logico; 3.3 Il livello sintattico; 4. I caratteri strutturali e dinamici del cyberspace; 4.1 Integrazione e pervasività; 4.2 Big Data; 4.3 Apertura; 4.4 Dual-use; 4.5 Anarchia.

Introduzione

Esiste un rapporto molto stretto tra fantascienza e scienza in ragione del quale la prima molto spesso *"suggerisce idee alle diverse e situate comunità di scienziati, i quali possono proficuamente includerle nelle loro teorie, o stravolgerle a piacimento, mentre la scienza conia talvolta nozioni e individua fenomeni più strani di qualsiasi prodotto inventato dalla fantascienza"*[1] .

Attraverso l'espressione artistica si muove *"il carro inerte"* [2] della società grazie a concetti, idee, visioni il cui contenuto potrà essere delineato in un momento successivo attraverso l'opera della politica e della scienza.

Da questo punto di vista, nonostante il cyberspace sia costituito da tecnologie la cui scienza poggia sulle ricerche dei primi del 900, a loro volta espressione di una nuova forma di conoscenza affermatasi con la diffusione dei testi scritti, la prima utilizzazione del termine la si ritrova in un romanzo del 1984, *Neuromancer* [3] di William Gibson, mentre è alla successiva elaborazione compiuta in ambito prevalentemente militare che si deve una più puntuale rappresentazione della sua struttura e dei suoi caratteri.

Quella che possiamo indicare come *definizione artistica* del CS non è tuttavia priva di interesse. Essa descrive una realtà che negli anni 80 iniziava a concretizzarsi e ne evidenzia i caratteri principali di cui oggi possiamo riconoscerne i segni nelle tecnologie dell'Internet of

[1] BARBARA HENRY, *Scientia ficta, umani e non nati/e da donna nell'immaginario globale: trame robotiche nella letteratura disegnata*, Nuova corrente rivista di letteratura, 1/2017 p.159
[2] WASSILY KANDINSKY, *Lo spirituale nell'arte*, SE, Milano 2005, pag. 23
[3] WILLIAM GIBSON, *Neuromante*, Ace Book, 1986

Things, dei Big Data, delle scienze analitiche, mediche, tecniche, urbanistiche e finanche nell'arte stessa e nell'editing genomico.

L'Autore ambienta il suo romanzo nel 2058 in un contesto urbano, le città di *Chuba* e *Night City* e lo *Sprawl*, un agglomerato urbano che si estende lungo le coste est degli Stati Uniti, iper-antropizzato, caotico, spesso violento. La storia si sviluppa seguendo il tentativo di un'Intelligenza Artificiale, chiamata "*invernomuto*", di eliminare i "*controlli di Turing*" che gli impediscono di evolversi in un'intelligenza superiore. Tentativo che viene contrastato da un'altra Intelligenza Artificiale, "*Neuromante*". Le dinamiche sociali sono dominate e orientate da valori prettamente economici e gli *"affari sono un costante ronzio subliminale"*. La città è qui vista come *"un esperimento dissennato di darwinismo sociale, concepito da un ricercatore annoiato che tenesse un pollice in permanenza sul pulsante dell'avanti-veloce"*.

L'elemento strutturale e al contempo dinamico che sorregge la società delineata nel romanzo è costituito dai dati e dal valore che essi acquisiscono tramite la *Matrice*, il Cyberspace.

Questa consiste in un infinito spazio elettronico a cui è possibile accedere per archiviare, scambiare, carpire dati e informazioni, descritto come *"un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione [...] Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità, linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati "*.

La definizione "artistica" del cyberspace finora tratteggiata, seppur suggestiva e per molti tratti non distante dalla realtà che si sarebbe in seguito affermata, non permette di affrontare un'analisi del cyberspace volta a delinearne i caratteri essenziali.

A tal fine occorre anzitutto ricostruire il valore dell'informazione e l'origine del cyberspace attraverso le diverse scoperte scientifiche e tecniche che, pur muovendo da ambiti diversi e sviluppate per finalità differenti, determinarono i presupposti tecnici e teorici alla base dell'attuale stadio di sviluppo del cyberspace e informano nei suoi caratteri principali il progresso sociale.

Al mutato concetto di informazione è infatti legata la costruzione dell'odierna Società della Conoscenza che, sorretta dal progresso tecnologico, pone in discussione principi e valori finora riferimento della società elaborandone al contempo di nuovi le cui implicazioni appaiono al momento in larga parte indefinite.

In secondo luogo, occorre ricostruire la definizione di cyberspace che, incerta e discussa come ogni aspetto che riguardi le attuali tecnologie della telecomunicazione (ITC), è stata prevalentemente sviluppata in ambito militare.

A tale ambito, in ragione di evidenti interessi di sicurezza, va ricondotta, in terzo luogo, l'individuazione dei caratteri propri del cyberspace dai quali, come si metterà in evidenza nel capitolo successivo, dipendono profondi mutamenti che investono tanto il dominio militare e securitario, quanto la dimensione sociale considerata nel suo complesso.

1. L'informazione

La rilevanza acquisite all'interno delle relazioni internazionali dalle tematiche legate allo sviluppo delle ITC è espressione della capacità del cyberspace di attribuire un nuovo e più ampio valore alle informazioni.

L'*informazione* costituisce infatti l'elemento dinamico dei rapporti sociali poiché per suo tramite, nell'interagire delle sue molteplici forme, si determinano le idee e i comportamenti delle persone e delle masse. Entro gli attuali sviluppi della società globale, sempre più volta a fondare le proprie dinamiche su processi di valorizzazione della conoscenza, l'informazione non trova più il suo valore nell'essere funzionale al raggiungimento di un fine, diviene essa stessa la risorsa indispensabile per il progresso della società umana, per la stessa determinazione del fine da perseguire.

Il concetto di informazione trova la sua origine nel termine latino *informatio* il cui significato era quello di "nozione, idea, rappresentazione" e nella sua accezione classica derivata dal greco, indicava l'azione dell'informare, di dare forma ad un'idea[4].

Ad esso sono oggi attribuiti una pluralità di significati in ragione dei diversi domini[5] in cui l'informazione viene in considerazione così come delle finalità che per suo tramite è possibile perseguire. Come evidenziato da Claude Shannon, al cui lavoro si deve la teoria generale dell'informazione che sorregge l'edificazione del cyberspace, nonostante i diversi significati proposti da più autori rispetto alle

[4] Vedi la voce Informazione su vocabolario Treccani, www.treccani.it
[5] LUCIANO FLORIDI, *La rivoluzione dell'informazione*, Codice edizioni, Torino, 2012

diverse applicazioni dell'informazione, *è difficile individuare un concetto unico di informazione che renda conto in modo soddisfacente delle sue numerose possibili applicazioni in questo ambito generale"* [6].

Tuttavia, all'informazione corrisponde un'azione che ha uno scopo ben definito: *"comunicare qualcosa a un recettore (individuo o massa) con l'intento di produrre effetti, anche difficilmente prevedibili, a livello sociale e comportamentale."*[7].

Ed è proprio nell'atto della comunicazione che l'informazione costituisce elemento dinamico del progresso umano.

Attraverso la comunicazione delle informazioni si sono affermate le conquiste del sapere, le scoperte scientifiche, la cultura, l'arte, le grandi opere. Attraverso essa si sono elaborate e diffuse le idee che hanno sorretto rivoluzioni politiche, economiche, scientifiche e tecniche.

La rilevanza storica dei processi di comunicazione deriva dalla natura stessa dell'uomo, essendone l'atto di comunicare la sua espressione più qualificante. Come è stato rilevato *"vi sono altri animali, oltre l'uomo, che hanno attitudini sociali e che vivono in una costante relazione con i propri simili, ma per nessuno questo impulso alla comunicazione, o meglio questa necessità della comunicazione, costituisce il motivo determinante della intera esistenza"*[8].

Istinto alla comunicazione che ha sorretto la definizione di schemi di linguaggio e di scrittura così come la realizzazione di supporti che permettessero la diffusione, la memorizzazione e l'uso delle informazioni, quali diretta espressione dell'attitudine a comunicare che informa l'uomo: *"se la scrittura è il punto in cui avviene la modificazione del linguaggio, essa è molto evidentemente, inscindibile dalla parola e la Parola (Ha Dubar), per quanto lontano risalga l'esplorazione della nostra memoria, è l'uomo"*[9].

---

[6] CLAUDE ELWOOD SHANNON, *Collected Papers*, a cura di Neil Sloane e Aron Wyner, IEEE Press, New York 1993 citato in Luciano Floridi, *La rivoluzione dell'informazione*, Codice Edizione, Torino 2012, pag XIII

[7] ANTONIO TETI, *Il potere delle informazioni. Comunicazione globale, Cyberspazio, Intelligenze della conoscenza*, Gruppo 24 Ore, 2004, pag. 13

[8] NORBERT WEINER, *Introduzione alla cibernetica. L'uso umano degli esseri umani*, Bollati Boringhieri, 2012 pag. 17

[9] PIERRE CHAUNU in Henri-Jean Martin, *storia e potere della scrittura*, Editori Laterza, Bari 2009, pag. X

1.1 Linguaggi e strumenti di comunicazione

Entro questa prospettiva è possibile tracciare una linea storica[10] lungo la quale si è sviluppato il rapporto tra l'uomo, i modelli logici del linguaggio e gli strumenti di comunicazione dell'informazione che nei diversi momenti hanno costituito i fattori principali per il progresso umano.

Un percorso che muove dalle prime manifestazioni di un pensiero speculativo dell'uomo, che trovarono nel grafismo uno strumento di comunicazione[11] dei meri dati della realtà naturale, e che giunge alla realizzazione delle odierne tecnologie di elaborazione in grado di estrarre dai dati della realtà un nuovo e diverso contenuto informativo determinando l'affermazione di nuove forme di conoscenza suscettibili di modificare la realtà stessa.

Successivamente alla fondazione delle prime città, all'intensificarsi quindi dei rapporti sociali, inizia il percorso di affermazione della scrittura. Un processo di elaborazione di un modello di comunicazione durato tre millenni animato dall'influenza delle diverse società che fiorirono dapprima nell'area mesopotamica e del mediterraneo orientale e da qui nel Mediterraneo di cultura greca per poi consolidarsi nel modello Latino.

La linea, il segno su bastone, che risponde al bisogno di visualizzare e fissare le interpretazioni del mondo esterno, confluisce nel sistema consonantico, caratterizzato da un elevato grado di astrazione, opposto ai procedimenti ideografici tradizionali e alle corrispondenti forme di pensiero per la sua capacità di collegare direttamente lo scritto alla parola, rispondendo in tal modo alle necessità dei mercanti e favorendo l'elaborazione e la diffusione anzitutto della cultura religiosa.

Con l'affermarsi della società Greca si diffonde un sistema di scrittura alfabetico che tende alla separazione del discorso sulla base dei diversi suoni che compongono la parola. Si tratta di una scrittura analitica che ben riflette i caratteri del pensiero classico tendendo a tradurre il flusso del discorso parlato.

---

[10] HENRI-JEAN MARTIN, *storia e potere della scrittura*, Editori Laterza, Bari 2009

[11] Ne sono espressione le prime sepolture che costituiscono un vero e proprio Linguaggio e *"il rito funerario un trattato di metafisica"* allo stesso modo in cui le incisioni rupestri di Lascaux e Altamira forniscono informazioni generali sul contesto naturale in un momento storico in cui *"il dossier precede molto evidentemente la scrittura, e l'arte astratta il figurativo"* (cfr. HENRI-JEAN MARTIN, *storia e potere della scrittura*, Editori Laterza, Bari 2009).

Tale sistema di scrittura troverà poi sistematizzazione e diffusione con l'affermazione della lingua dei Latini ad opera della civiltà romana. Così come la visione politica di Roma anche la scrittura alfabetica esprimeva un carattere universale improntato al criterio dell'efficienza, trovando la loro origine e la loro dinamica entro i variegati e mutevoli rapporti commerciali e culturali del Mediterraneo[12].

Il sistema di scrittura alfabetico, tuttavia, tende da una parte, a privilegiare il suono delle parole e non il loro significato e, dall'altra, ad omettere la separazione tra le parole e tra le frasi.

Sono caratteri che riflettono il rapporto tra comunicazione orale e scrittura. Un rapporto che è profondamente influenzato dal supporto per la scrittura stessa, ovvero, in termini più attuali, dalle tecnologie che permettono la manipolazione memorizzazione e diffusione delle informazioni [13]. Quest'ultime, tuttavia, sembrano riproporre i caratteri propri di una cultura orale. Come è stato osservato si delinea una *"preistoria digitale"* in ragione del fatto che *"la nostra memoria digitale sembra tanto volatile quanto la nostra cultura orale, ma forse in modo ancora più instabile, poiché ci dà l'impressione opposta"* [14].

L'evoluzione del supporto è stata mossa dall'esigenza di superare proprio le difficoltà pratiche legate alla memorizzazione e diffusione dei testi scritti e alla necessità di elaborare nuove forme di pensiero.

Nello sviluppo di tali strumenti si può misurare l'intensità con cui si manifesta l'attitudine alla comunicazione che caratterizza l'uomo.

È un bisogno di comunicazione che si autoalimenta, aumentando con l'acquisizione di nuove capacità di rilevazione, memorizzazione, manipolazione e diffusione delle informazioni che a loro volta determinano i mutamenti sociali, reinventandosi quando tali capacità non rispondono alle necessità di conoscenza dell'uomo.

---

[12] CONTRAMMIRAGLIO VANNUTELLI. *Il Mediterraneo fonte risorgente della civiltà mondiale*, Cappelli, Bologna 1932; BRAUDEL FERNAND, *Civiltà e imperi del Mediterraneo nell'età di Filippo II*, Einaudi, 2010; BROODBANK CYPRIAN, *Il Mediterraneo. Dalla preistoria alla nascita del mondo classico*, Einaudi, 2015; MARIA SILVIA CODECASA, *La rotta di Glauco. Viaggi per terra e per mare*, Exorma edizioni, 2011; HORDEN PEREGRINE, PURCELL NICHOLAS, *The Corrupting Sea*, Wiley-Blackwell, 2010.

[13] Un rapporto che, allo stesso tempo, influenza le strutture sociali definendone le gerarchie all'interno in funzione della padronanza delle *Arti della Memoria* a cui è legato l'esercizio dei poteri pubblici che tramite esse trovano espressione tanto nella giurisdizione quanto nella politica.

[14] LUCIANO FLORIDI, *La quarta Rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano 2017, pag.19

In questa prospettiva è stato osservato come *"la società antica [sia] debitrice del papiro come noi lo siamo dei microprocessori"* [15].

Il papiro infatti è un supporto, differentemente da legno e tavolette di argilla, leggero, commerciabile, facile da imprimere con inchiostro e calamo. Ed è a partire dalla realizzazione di questo primo supporto che la scrittura divenne, soprattutto a Roma, elemento costituente delle principali operazioni e circostanze della vita cittadina[16].

Allo stesso modo il transistor presentato dai laboratori BELL nel 1948 con le sue dimensioni millesimali e la sua ampia funzionalità *"ha dato il via alla rivoluzione dell'elettronica"*[17] determinandone la miniaturizzazione e l'onnipresenza, elementi alla base delle attuali forme di comunicazione.

1.2 L'innovazione dei supporti alla comunicazione quale fattore di progresso.

Tra i due momenti di riferimento da ultimo indicati, si sviluppa il processo di affermazione del libro quale strumento di conoscenza grazie ad un'altra rivoluzione di tipo tecnologico quale è stata la carta[18].

Pur con i mutamenti intercorsi nelle tecniche tipografiche il libro per molto tempo ha costituito il supporto per la comunicazione di una conoscenza tradizionale destinata ad essere acquisita e trasmessa con l'esercizio delle *"Arti della Memoria"* [19].

La memoria e la retorica trovano tuttavia i loro limiti nella quantità e nella qualità di informazione che permettono di immagazzinare, elaborare e comunicare.

Fu un ulteriore progresso tecnico, la stampa di Gutenberg, a sopperire a tali limiti e innovare la funzione del libro aprendo ad una

---

[15] PIERRE CHAUNU in Henri-Jean Martin, *storia e potere della scrittura*, Editori Laterza, Bari 2009, pag. XIII

[16] CLAUD NICOLET , *Le métier de citoyen dans la Rome républicaine*, Pari, 1976, citato in Henri-Jean Martin, storia e potere della scrittura, Editori Laterza, Bari 2009

[17] JEMES GLEICK, *L'informazione. Una storia. Una teoria. Un diluvio*, Feltrinelli 2015, p 11

[18] Introdotta nell'amministrazione cinese della dinastia Han, 105 d.C. come sostituto della seta, la Carta si diffuse in Corea, nel Vietnam, in Giappone e nel mondo arabo, dove fin dall'VIII secolo i bizantini la usarono per la redazione degli atti della loro burocrazia. Una funzione strutturale dunque, che la Carta eserciterà nelle diverse epoche fino alla costruzione dello Stato Nazionale, favorendo da un lato il consolidamento delle strutture amministrative e, dall'altro, i processi di definizione delle diverse lingue e culture nazionali

[19] PAOLO ROSSI, *Clavis universalis. Arti della memoria e logica combinatoria da Lullo a Leibniz*, Il Mulino, 2000

nuova dinamica di elaborazione e diffusione delle informazioni dalla quale scaturirono i fondamenti del pensiero scientifico e politico del XIX secolo.

Questi trovano nel Libro, nell'opuscolo, nelle riviste scientifiche, nelle diverse declinazioni in cui la carta si lascia modellare, il supporto ideale per la memorizzazione, diffusione ed elaborazione di un pensiero ormai slegato dalla dimensione orale e dalle tecniche oratorie.

Allo stesso tempo la diffusione della scrittura, non più confinata a promemoria della tradizione, si presta allo sviluppo di un pensiero articolato volto ad indagare la complessità della natura e dell'uomo stesso la cui diffusione è favorita dall'affermazione di una editoria commerciale che ne sostiene i processi di elaborazione e diffusione.

Si tratta di una rottura con la tradizione che sorregge i processi sociali ed economici della Riforma protestante allo stesso modo in cui permette la diffusione delle teorie scientifiche di Galileo Galilei, di Charles Darwin e delle nuove prospettive aperte nello studio delle leggi della natura e dei processi cognitivi proposte da Isaac Newton e Sigmund Froid.

Le innovazioni apportate dalle tecniche di stampa al processo di memorizzazione, manipolazione e diffusione delle informazioni sostiene, nel contesto della rivoluzione industriale del 1800, lo sviluppo di un nuovo pensiero scientifico e tecnico che troverà il suo apice nella società europea di inizio Novecento[20].

Una linea di progresso che trova la sua espressione nelle Esposizioni Universali e la sua sintesi nei simboli, tra gli altri, della Torre Eiffel e del Palazzo dell'Elettricità che caratterizzarono le manifestazioni parigine del 1898 e del 1900.

Ricerca scientifica e innovazioni tecnologiche costituiscono infatti le due direttrici di progresso che permisero l'affermazione di una

[20] Lo scienziato britannico Alfred Russel Wallace in suo libro pubblicato nel 1898 osservava come la quantità e la qualità dei progressi compiuti giustificavano la definizione di "*secolo meraviglioso*" attribuito all'800. La ferrovia, la nave a vapore, il telegrafo elettrico, il telefono, la luce elettrica, la fotografia, il fonografo, i raggi x, l'analisi spettrale, la conservazione dell'energia, la misurazione diretta della velocità della luce e la dimostrazione sperimentale della rotazione terrestre, nuove cognizioni e differenziazioni della chimica, l'origine dell'uomo, la teoria organica dell'evoluzione, la teoria cellulare e l'embriologia, sono alcune delle innovazioni introdotte in questo secolo che determinarono da un lato, il consolidamento dei collegamenti e delle comunicazioni mondiali, dall'altro l'aumento della quantità e qualità delle informazioni rilevate ed elaborate. cfr. RUSSEL WALLACE, *The wonderful century*, Dodd, Mead and Company, New York, 1899 consultabile in archive.org all'indirizzo web https://archive.org/details/wonderfulcentury028485mbp/page/n8

"Mondialità europea"[21], in particolare nel periodo compreso tra la Conferenza di Berlino e la Prima guerra mondiale.

Questa apri una fase storica che si concluderà nel 1948 con l'affermazione di un nuovo ordine mondiale espressione di nuovi attori geopolitici la cui rilevanza venne sancita nel secondo conflitto bellico che determinò il declino dell'ordine internazionale elaborato a partire dalle relazioni tra gli Stati europei.

Stati Uniti e Unione Sovietica esprimevano visioni politiche di tipo universali che plasmarono tanto la costruzione del nuovo ordine internazionale quanto il confronto bipolare che avrebbe sancito la centralità dei primi nella definizione di una nuova linea di progresso umano. Gli Stati Uniti seppero infatti costruire un sistema economico a vocazione universale, garantito da una capacità militare globale, sorretto da una cultura improntata alla scienza e alla tecnica espressioni di universali valori di libertà del singolo. Scienza e tecnica erano dunque chiamate a costruire gli strumenti atti a garantire tale proiezione universale del progresso umano che sarebbe poi confluita nella globalizzazione dei rapporti internazionali avviatasi negli anni 90 con l'implosione dell'Unione Sovietica e la caduta del Muro di Berlino.

2. L'interdisciplinarietà dei fondamenti del cyberspace

Il XIX secolo è stato teatro di notevoli cambiamenti sociali caratterizzati dall'affermarsi di un'idea di progresso che vedeva nella tendenza alla globalizzazione e nella fiducia nella scienza le sue linee guida.

In questo campo, in particolare, si realizzarono scoperte di primaria importanza nello studio dell'atomo e più in generale dell'infinitamente piccolo[22]. Studi che si svilupparono entro un più radicale mutamento dell'impostazione newtoniana fino ad allora dominante[23]: al determinismo ottocentesco segue l'indeterminismo dei nuovi metodi scientifici i quali vivranno nel XX secolo uno sviluppo che influenzerà le discipline più disparate e porterà alla realizzazione di applicazioni pressoché in tutti i campi.

---

[21] EMILIO GENTILE, *Ascesa e declino dell'Europa nel mondo 1898-1918*, Garzanti 2018
[22] ROBERT JUNGK, *Gli apprendisti stregoni*, Einaudi Editore, 1958
[23] N. WEINER, *Cybernetics or control and communication in the animal and machine*, Cap. I, II° Ed., MIT, 1947

L'interdisciplinarietà è, infatti, la cifra caratteristica di un'intera cultura scientifica che origina nell'Europa di inizio secolo[24], che realizza le sue prime applicazioni durante il conflitto mondiale e che successivamente troverà negli Stati Uniti una società votata al progresso che saprà farla propria dandole infine la dimensione universale che oggi conosciamo.

Il rapporto tra scienza e progresso che si instaura in questo momento rappresenta attualmente il fattore determinante lo sviluppo della società umana.

Le Information Communication Tecnology (ICT) che, come vedremo, sono il frutto di questi primi studi, costituiscono da una parte utili strumenti per l'implementazione delle attività umane, dall'altra determinano profondi mutamenti dell'agire umano che possono porre in discussione il rispetto di interessi e valori primari su cui poggia la nostra idea di dignità dell'uomo.

A tal fine occorre osservare il percorso che ha portato alla realizzazione della rete Internet in ragione della capacità di quest'ultima di determinare l'unità strutturale del cyberspace dalla quale deriva il peculiare valore acquisito dei dati e dalle tecniche di elaborazione degli stessi che, comprese nel generale concetto di Intelligenza Artificiale, determinano l'unità funzionale del cyberspace.

La loro centralità all'interno del cyberspace deriva infatti dalla possibilità di far giungere alle macchine elaboratrici informazioni sul mondo circostante. Informazioni che rappresentano la principale risorsa da cui dipende lo sviluppo del cyberspace e, al contempo, il suo prodotto attraverso il quale la macchina agisce sul mondo circostante al fine di ottimizzarne il progresso secondo i parametri considerati e che essa stessa è potenzialmente in grado di determinare.

Nello sviluppo delle teorie poste alla base del funzionamento del cyberspace e dei primi computer un ruolo di particolare interesse è stato svolto dal comparto militare statunitense.

Questo costituisce un rilevante apparato burocratico composto di plurime agenzie che sviluppano progetti indipendenti che vengono in contatto in molti specifici settori.

Le diverse esigenze manifestate rappresentarono lo stimolo, anche finanziario, allo sviluppo tanto di ricerche di base quanto di prodotti

[24] PIETRO GRECO, *La scienza e l'Europa. Il primo Novecento*, L'Asino d'oro edizioni, Roma, 2018

specifici che contribuiranno alla realizzazione di applicazioni tecnologiche nei più diversi campi dell'attività umana.

Tali studi furono condotti in stretta collaborazione con istituti universitari e centri di ricerca privati così determinando un processo di osmosi per cui le tecnologie sviluppate in ambito militare poterono trovare nuove applicazioni e un proprio mercato anche in ambito civile.

Si tratta di un processo che si è sviluppato progressivamente influenzato dalle diverse contingenze storiche e che vede nell'affermarsi della globalizzazione un momento centrale del suo sviluppo.

2.1 La Cibernetica

I primi importanti studi si ebbero in particolare nell'ambito dei sistemi di controllo automatico [25] che, originariamente legati alla realizzazione di servomeccanismi nell'ambito dell'ingegneria meccanica, trovarono, con lo sviluppo della tecnologia elettronica[26], una propria autonomia scientifica.

Durante i due conflitti mondiali la necessità di sviluppare sistemi d'arma sempre più precisi fornì l'occasione per un ulteriore sviluppo volto a superare le problematiche fino ad allora esistenti.

A ciò contribuirono gli studi condotti nei laboratori del MIT e della BELL dal Prof. Wiener che portarono all'elaborazione dei concetti di

[25] S. BENNET, *A Brief history of Automatic control*, IEEE Control System Society, June 1996; NECULAI ANDREI, *Modern Control Theory – A historical perspective*, Scieri Matematice, February 10, 2005 consultabile all'indirizzo web https://pdfs.semanticscholar.org/b9dc/706a8d092b1ecd0dc2b7d6a025ea22ebf507.pdf ; D. A. MINDELL, *Between human and machine – feedback, control and computing before Cybernetics*, The Johns Hopkins University Press, 2002

[26] L. MCCOLL, *Fundamental Theory of Servomechanisms*, D. Van Nostrand Company inc., 1945, citato più volte da Norbert Wiener in *Cibernetica*, il cui IV capitolo costituisce esso stesso una introduzione generale all'argomento

feedback[27] e di trasmissione delle informazioni all'interno di una teoria che affrontava unitariamente tali problematiche[28].

In altri termini tali studi attribuivano alle macchine computazionali la capacità di apprendere attraverso un semplice processo di circolazione di informazioni sottoposte a elaborazione continua ponendosi, per tale ragione, alla base delle successive ricerche sull'Intelligenza Artificiale. Rispetto agli sviluppi attuali si può notare come le stesse qualifichino il cyberspace, considerato nel complesso dei suoi elementi e della sua dinamica, come un fattore di progresso suscettibile di sviluppare una propria autonomia non solo rispetto al reperimento delle risorse necessarie al suo funzionamento ma, soprattutto, rispetto alla definizione di propri fini da perseguire[29].

Lo sviluppo di un'intelligenza cognitiva delle macchine, tuttavia, comportava la necessità di compiere calcoli estremamente complessi che non potevano essere svolti dalle macchine calcolatrici analogiche fino ad allora costruite[30].

---

[27] Il principio della retroazione (*feedback*) si basa sull'assunto che un fenomeno è in grado di autoregolare il suo output. Pur trattandosi di un semplice processo circolare di informazioni sottoposte ad elaborazione continua in funzione del raggiungimento del risultato, esso troverà applicazione nei campi più disparati tra i quali la simulazione di alcuni meccanismi neurofisiologici rappresentando una *"metodologia di sviluppo di un modello di intelligenza cognitiva che fino a quel tempo risultava completamente assente in tutti i sistemi progettati per eseguire autonomamente determinate funzioni"* (ANTONIO TETI, *PsycoTech. Il punto di non ritorno. La tecnologia che controlla la mente*, Springer, Italia, 2011, pag 88)

[28] N. WIENER, *The Extrapolation, Interpolation, and Smoothing of Stationary Time Series*, Report of the Services 19, Research Project DIC-6037 MIT, February 1942; poi New York: Wiley, 1949.

[29] Aspetti questi che oggi rientrano all'interno delle discussioni sull'idea di singolarità, sul suo affermarsi e sul suo funzionamento, cfr. NICK BOSTROM, *Superintelligenza. Tendenze, pericoli, strategie*, Bollati Boringhieri, Torino, 2018; R. KURZWEIL, *The Singularity is Near: When Humans Trascend Biology*, Viking, New York, 2005; Vernor Vinge, The Coming Technological Singularity: How to Survive in the Post-Human Era, in Vision-21: Interdisciplinary Science and Engineering in the Era of Cyberspace, 11-22, NASA Conference Publication 10129, NASA Lewis Research Center, consultabile all'indirizzo https://ntrs.nasa.gov/citations/19940022856 .

[30] Lo sviluppo di quest'ultime a partire dal 1945 può essere descritto come *"la storia di persone che in momenti critici hanno ridefinito la natura della tecnologia stessa"* [30](cfr. PAUL E. CERUZZI, A history of modern computing, The MIT Press, 2nd ed., 2003, pag. 14). È questo il caso di Eckert e Mauchly che disegnarono e costruirono, all'interno dell'Università della Pennsylvania, il calcolatore ENIA che, sviluppato per le esigenze di calcolo balistico dell'esercito americano, trovo in seguito applicazione nel settore privato. Rinominato "Universal Automatic Computer" ovvero una macchina calcolatrice in grado di risolvere problemi universali, cioè posti da scienziati come da ingegneri o da uomini d'affari, fu adottato da alcune compagnie private per la sua utilità nell'ambito della logistica e dell'attività aziendale in generale. L'IBM realizzò nel 1952 il computer "701" definito *"electronic data processing machine"* il quale trovò anch'esso ampio utilizzo nel settore privato dopo essere stato sviluppato in risposta ad esigenze militari. Provenivano da progetti di ricerca militari anche i

Dal punto di vista tecnico i computer sviluppati in questo momento condividono l'architettura di base influenzata dai lavori di Newman e la tecnologia a schede pre-forate per la programmazione oltre che la tecnica costruttiva e le limitate capacità di calcolo.

Da qui lo sviluppo avviato dagli studi di Wienner di una nuova tecnologia di tipo digitale che permettesse di superare i problemi legati alla trasmissione delle informazioni. In ciò egli si richiamo ad alcune idee elaborate negli stessi anni all'interno dei laboratori BELL da Claude Shannon sul concetto di quantità di informazione e sulla loro trasmissione[31] dai quali origina la logica binaria digitale su cui si basano le moderne tecnologie di telecomunicazione.

Fondamentali alla realizzazione delle nuove macchine furono anche i lavori svolti nel campo della logica matematica da Alan Touring che delineavano un modello di macchina calcolatrice computazionale[32] e quelli di Warren McCulloch e Pitts, neurofisiologi dediti allo studio del funzionamento del cervello, le cui teorie dimostrarono la validità delle tesi sostenute dalla "macchina di Touring" e che il neurone costituiva l'unità logica del cervello[33]. Altrettanto rilevanti furono i lavori di Von Neumann che definirono l'architettura di una macchina calcolatrice[34]. Altri scienziati, come Gregory Bateson, condussero studi nei campi dell'antropologia, della sociologia, della linguistica che trovarono applicazione nello sviluppo delle macchine calcolatrici.

Entro questo quadro generale va posta la teoria dei messaggi estesa allo studio *"del messaggio come strumento di controllo della macchina e della società, [al]lo sviluppo di macchine computazionali e altri tipi di automi, di alcune riflessioni sulla psicologia e sul sistema nervoso, e*

fondatori della Engineering Research Associates, Inc, Howard Engstrom e William Norris, che svilupparono il calcolatore nominato 1103 che rappresento un diretto competitor dl modello 701 sviluppato dalla IBM. cfr. ACHILLE VARZI, *Storie di macchine*, La Rivista dei Libri, 9:11, 1999, pp. 29–31

[31] CLAUDE E. SHANNON, *A Mathematical Theory of Communication*, Bell System Technical Journal, vol. 27, luglio e ottobre 1948

[32] A. M. TURING, a cura di Gabriele Lolli, *Intelligenza Meccanica*, Bollati Boringhieri, Torino,1994; A. M. Turing, *On Computable Numbers, with an Application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society, Volume s2-42, Issue 1, 1937, Pages 230–265

[33] MCCULLOCH, PITTS, *On how we knok univwersal: the perception of auditory and visual forms*, Bulletin of Mathematical Biophysics, 1947, 9:127-147

[34] JOHN VON NEUMANN, *First Draft of a Report on the EDVAC*, 1945 consultabile all'indirizzo web http://web.mit.edu/STS.035/www/PDFs/edvac.pdf

i tentativi di sviluppo di una nuova teoria del metodo scientifico" che tenesse conto della teoria probabilistica introdotta da Gibbs[35].

Questo "complesso di idee" ha preso il nome di *Cibernetica* che, nella definizione di Wiener che per primo delineò le basi di questo settore scientifico, consiste nella disciplina che studia i processi riguardanti *"la comunicazione e il controllo nell'animale e nella macchina"* o più in particolare *"lo studio dei messaggi e particolarmente dei messaggi di controllo"*[36] ovvero quei messaggi che modificano il comportamento del ricevente.

Dal punto di vista teorico la cibernetica parte dall'osservazione che ciò che caratterizza l'uomo è la sua attitudine alla comunicazione: *"questo impulso alla comunicazione, o meglio questa necessità alla comunicazione, costituisce il motivo determinante della intera esistenza"*[37] caratterizzando il comportamento umano. Questo si presenta *"esattamente parallelo al comportamento delle più recenti macchine per le comunicazioni"* [38] che al pari dell'uomo sono dotate di organi di recezione che agiscono come primo stadio del ciclo di funzionamento nel quale le informazioni vengono raccolte dal mondo esterno ed elaborate al fine di porre in essere, sia negli uomini che nelle macchine, un'azione effettiva sull'ambiente circostante[39].

Essa inoltre prende in considerazione il messaggio quale comunicazione inviata non solo da un essere umano all'altro ma anche i messaggi fra l'uomo e la macchina, fra le macchine e l'uomo e fra macchina e macchina. Il modo in cui Wiener esemplifica queste ulteriori forme di comunicazione è particolarmente interessante. Nelle parole dell'autore *"se son pigro e la mattina, invece di alzarmi dal letto, schiaccio un bottone che apre i caloriferi, chiude la finestra e accende un fornello elettrico sotto la caffettiera, io invio un messaggio agli elementi di questi apparecchi. Se invece il bolliuova elettrico fischia dopo un certo numero di minuti, esso invia a me un suo messaggio. Se*

---

[35] NORBERT WEINER, *The Human use of human beings: cybernetics and society*, Free Association Books, London, 1989 (First published 1950), pag. 41

[36] NORBERT WEINER *Introduzione alla cibernetica. L'uso umano degli esseri umani*, Bollati Boringhieri, Torino, 2012

[37] ID.

[38] ID.

[39]Da un punto di vista metodologico la cibernetica si basa sull'utilizzo di modelli a corrispondenza biunivoca ed in particolare fa riferimento a quei modelli che possono essere designati con il termine messaggio, quali, ad esempio, i modelli delle conversazioni telegrafiche e telefoniche. Quest'ultimi, infatti, si differenziano in ragione della funzione per cui sono impiegati ovvero trasmettere l'informazione il cui significato è legato alla scelta di comunicare un dato modello rispetto ad un altro.

il termostato registra una temperatura eccessiva nella camera e chiude il calorifero si può dire che il messaggio funziona come sistema di comando del calorifero stesso" [40].

Questi esempi non sono in fondo molto distanti dalla realtà che oggi si va affermando: L'Internet of Things, e le sue applicazioni, come vedremo, non sono altro che lo sviluppo degli studi sulla comunicazione ed elaborazione delle informazioni sorretti dallo sviluppo delle tecnologie informatiche.

2.2 Il network quale supporto per la condivisione della conoscenza.

Successivamente alla Seconda guerra mondiale un nuovo stimolo agli studi indicati fu dato dal lancio dello Sputnik nel 1957 [41]. La sfida agli Stati Uniti che esso rappresentava, determino l'ampliamento del settore universitario statunitense e l'aumento dei fondi federali diretti alla ricerca e allo sviluppo[42] di applicazioni funzionali alle nuove esigenze di difesa poste dalle manifestate capacità tecniche e nucleari dell'Unione Sovietica[43].

Con particolare riferimento a questo aspetto il sistema di sicurezza statunitense presentava diverse problematiche alla cui definizione contribuì in misura rilevante l'attività di ricerca della RAND Corporation, ente nato nel 1946 con la stipula di un contratto tra la United States Air Force (USAF) e la Douglas Aircraft Company che divenne nel 1948 un'organizzazione indipendente non profit. Albert Wohlstetter, rilevante membro dell'organizzazione, analizzò tali

---

[40] NORBERT WEINNER *Introduzione alla cibernetica. L'uso umano degli esseri umani*, Bollati Boringhieri, Torino, 2012

[41] MARTA WHEELER GEORGE, *The impact of Sputnik: Case study of American Pubblic Opinion at the Break of the space Age,* October 4, 1957: NASA Historical note 22, NASA History Offices Archive.

[42] Nel 1958 venne istituito all'interno del Departement of Defence (DoD) il programma di ricerca Advanced Research Projects Agency (ARPA) con il compito di sviluppare un programma missilistico spaziale. Nei mesi successivi venne istituita la National Aereonautic Space Administration (NASA) che, inizialmente responsabile per gli aspetti civili dei vari progetti, fini con il divenire il centro nevralgico delle ricerche anche in campo militare ed in particolare sul sistema di difesa dai missili balistici sovietici.

[43] RAYMOND L. GARTHOFF, ROBERT A. DIVINE, *The Sputnik Challenge*. *The American Historical Review*, Volume 99, Issue 2, April 1994, New York, pp. 685–686

problematiche in un articolo pubblicato sul Foreign Affairs in cui evidenziava due particolari aspetti[44].

Da una parte che il concetto di deterrenza implica la capacità *"to strike back"* ovvero di rispondere all'attacco nonostante si sia stati colpiti. Dall'altra chiarì come, a tal fine, la struttura difensiva dovesse essere in grado di sopravvivere all'attacco e soprattutto dovesse garantire la comunicazione tra i vari livelli decisionali che avrebbero dovuto ordinare la risposta nucleare. L'intero sistema di sicurezza statunitense poteva essere reso inoperante da *"small, inaccurate Soviet nuclear weapon"*[45] che avessero colpito centri e sistemi nevralgici come lo Strategic Air Command o il Ballistic Missile Early Warning System. Il problema si poneva essenzialmente in termini di resilienza delle strutture e dei canali di comunicazione tra i vari centri operativi e decisionali coinvolti al fine di garantire l'operatività delle infrastrutture di difesa nucleare. In altri termini occorreva costruire un'infrastruttura che garantisse il funzionamento di altre infrastrutture.

I tentativi di dare risposta a queste problematiche, compiuti da diversi enti di ricerca e grazie agli studi di scienziati attivi in ambiti a volte apparentemente distanti tra loro, portarono alla realizzazione, attraverso diverse fasi di sviluppo e in diversi contesti storici, della rete Internet.

La prima elaborazione di un network di comunicazione che rispondesse alle necessità evidenziate fu sviluppata da Paul Baran all'interno dalla RAND Corporation e presentata in undici memoranda[46]. In particolare, la terza soluzione che egli presentò si caratterizzava per l'elaborazione di un metodo di divisione dei dati in pacchetti di dimensioni standard inviati separatamente che ne favoriva la trasmissione sicura e veloce attraverso diversi nodi. L'utilizzo di questa tecnica permetteva da una parte, a più utenti di comunicare contemporaneamente e dall'altra di far viaggiare i pacchetti dati sempre attraverso il link effettivamente libero così velocizzando l'intero processo di comunicazione. Il sistema ideato da Baran venne proposto senza successo alla AT&T e la stessa RAND Corporation lo accolse con poco entusiasmo limitandosi a inviarlo al USAF nel 1965.

---

[44] ALBERT WOHLSTETTER, *The delicate balance of terror*, Foreign Affairs, January 1959, https://www.foreignaffairs.com/articles/1959-01-01/delicate-balance-terror

[45] PAUL BRACKEN, *the Command and Control of Nuclear Forces*, New, Yale University Press, 1983, p. 186

[46] PAUL BARAN, *On a Distribuited Command and control System Configuration*", USAF, Project RAND, Research Memorandum RM-2632, 31 December 1960, consultabile all'indirizzo web http//www.rand.org/pubs/research_memoranda/RM2632.html

Quest'ultima lo sottopose a sua volta alla MITRE Corporation che lo valutò positivamente. Tuttavia, il progetto non trovò in questo momento uno sviluppo applicativo sia per il clima di distensione e al contempo disordine che caratterizzava in questi anni il confronto tra USA e URSS[47], sia per l'inadeguatezza dei sistemi di calcolo dell'epoca[48].

Al di là del dato tecnico, che presenta comunque tutti gli elementi principali dell'attuale rete internet, ciò che appare di particolare interesse nei lavori di Baran è il loro richiamo agli studi scientifici condotti in precedenza e che abbiamo visto potersi ricondurre all'interno dell'ambito di ricerca della cibernetica.

In particolare, egli individua tre *"foundation paper"*. Il primo lavoro preso in considerazione è quello del neurofisiologo Warren McCulloch, che nel 1964 divenne il primo presidente dell'American Society of Cibernetics. Affianco ad esso vi sono i lavori di Von Neumann e Ewuard F. Moore e Claude E. Shannon. Quest'ultimo in particolare aveva pubblicato nel 1949 la fondamentale teoria dell'informazione mentre i lavori di McCulloch condotti assieme a Pitt avevano aperto la strada ad un nuovo settore della ricerca scientifica che poneva la sua attenzione allo sviluppo di una Intelligenza Artificiale. I due scienziati avevano suggerito che il neurone non emettesse energia ma informazioni di natura logica (and-or-not) aprendo così lo studio delle similitudini tra la mente umana e i computer. MacCulluc e Pit a loro volta citano nelle loro opere i lavori di Alan Turing sulle quali si basano i moderni computer. Come è stato osservato *"l'analisi di questo "network of cross-reference" illustra chiaramente lo stretto legame di interdipendenza tra neurofisiologia, information Technologies, teorie dell'informazione e successivamente, psicologia"*[49].

---

[47] Un contesto creato dagli stessi progressi tecnologici che avevano aperto, tramite le immagini dei primi satelliti, una visione per la prima volta globale della Terra suscitando nuove idee politiche che valutavano diversamente e negativamente l'incessante corsa agli armamenti del confronto bipolare rispetto al quale nuovi e imprevisti fronti di antagonismo e conflitto si aprirono nelle aree asiatiche e mediorientali, allontanando in tal modo le preoccupazione di sicurezza nazionale che abbiamo visto esser alla base di molte ricerche scientifiche [47] (cfr. FEDERICO ROMEO, *Storia della Guerra fredda. L'ultimo conflitto per l'Europa*, Einaudi 2009, pag. 174 e seg.).

[48] Tali sistemi rappresentavano sostanzialmente un'evoluzione dei modelli precedenti rispetto ai quali erano dotati sì di capacità di calcolo superiori, ma ne condividevano la struttura sostanzialmente analogica che ne limitava la funzionalità rispetto alle esigenze legate allo sviluppo dei progetti di Baran.

[49] TOMMASO DETTI, GIUSEPPE LAURICELLA, *The Origin Of Internet*, Bruno Mondatori, Milano, 2013, p. 41

L'influenza delle ricerche scientifiche condotte nelle università e negli enti privati statunitensi si rintraccia anche nei lavori dell'inglese Donald W. Davis il quale, seguendo un diverso e autonomo percorso di ricerca, sviluppò un network di computer in molti punti simile a quello di Baran elaborando inoltre soluzioni innovative che affrontavano specifiche problematiche tecniche, quali il problema del Time-Sharing[50]. La particolare attenzione che egli pose alla velocità di trasmissione dei dati era funzionale alla ricerca di una metodologia e di strumenti che potessero sostenere *"a conversation between a computing (or information) system and a human user which can save the human effort"* [51] tanto nelle attività finanziarie che nello sviluppo del sistema commerciale all'interno di un network esteso su grandi distanze.

Problema, questo, affrontato, da una prospettiva militare, anche dalle ricerche svolte all'interno dell'Advanced Research Projects Agency (ARPA) del Dipartimento della Difesa statunitense, ove l'interesse era rivolto alle *"computer applications to war gaming, command systems studies and information processing related to command and control"* [52]. Nel 1962 venne quindi creato all'interno dell'ARPA l'ufficio Information Processing Techniques Office (IPTO) il quale si occupò di sviluppare queste ricerche sotto la guida di Joseph Carl Robenett Licklider. Il contributo che questi diede alla ricerca fu di particolare importanza intrecciandosi con gli studi della cibernetica e con quelli sull'Intelligenza Artificiale[53].

---

[50] Con questo termine si intende *"a series of operations intended to give multipler user simultaneous access to one of the machines through interactive terminals, in order to share its calculating power. In this way every user had the impression of having the computer entirely at their disposal, whitin the limits of its ability"* [50](cfr. TOMMASO DETTI, GIUSEPPE LAURICELLA, *The Origin Of Internet*, Bruno Mondatori, Milano, 2013, p. 41).

[51] TOMMASO DETTI, GIUSEPPE LAURICELLA, *The Origin Of Internet*, Bruno Mondatori, Milano, 2013, pag 44; Questo aspetto tuttavia, è espressione di un diverso orientamento finalistico che caratterizza la ricerca scientifica inglese in ragione della diversa concezione di sicurezza fondata sull'elemento economico piuttosto che su quello della forza militare. La differenza di prospettiva che caratterizza la visione statunitense da quella inglese è espressione, oltre che di dinamiche storiche, anche della duplice natura del cyberspace, le cui applicazioni hanno al contempo rilevanza in termini di sicurezza e di sviluppo economico così che la misura del progresso diviene essa stessa un fattore di interesse securitario. In altri termini non è possibile scindere, nel considerare i diversi aspetti del cyberspace, i suoi risvolti positivi da quelli negativi essendo essi interdipendenti

[52] TOMMASO DETTI, GIUSEPPE LAURICELLA, *The Origin Of Internet*, Bruno Mondatori, Milano, 2013, pag. 56

[53] Da una parte con i suoi studi sulla psyco-acustica evidenzio il rapporto tra due network di comunicazione connessi attraverso l'apparato uditivo: l'uno composto da più persone che comunicano attraverso la voce e l'udito, l'altro formato dal sistema nervoso. Ciò permetteva di

Nel suo testo *Man Computer Symbiosis* propone di sviluppare i computer al fine di *"to enable men and computers to cooperate in making decisions and controlling complex situations without inflexible dependence on predetermined programs"*[54].

Ciò che proponeva era in altri termini un metodo di calcolo che non implicava di formulare in anticipo il problema da sottoporre alla macchina in tutta la sua complessità poiché i computer sarebbero stati in grado di rispondere alle variabili inserite di volta in volta. Il sistema non si basava sui tradizionali metodi di elaborazione analogici basati su schede pre-forate preparate da tecnici ma, piuttosto sullo sviluppo della tecnica del time-sharing che consente a molti utenti di accedere ad un grande mainframe di singoli terminali.

Licklinder, che aveva discusso con Wiener della creazione di una comunità scientifica diffusa, propose l'idea di vari *"thinking centres"*, corrispondenti alle varie aree scientifiche, equipaggiate con computer digitali e librerie contenenti libri e riviste *"adattati per un rapido accesso alle informazioni"* [55].

Ciò che egli proponeva non era una semplice relazione tra uomo e computer bensì una relazione tra uomo e the body of knowledge intesa come un *"rapporto coordinato tra uomo e macchina"* ove le librerie costituivano *"precognitive system chich would promote and facilitate the acquisition, organization and the use of knowledge*" [56].

affrontare il problema della configurazione di un network composto da un numero elevato di elementi posti in dialogo tra essi.

[54] JOSEPH C. R. LICKINDER, *Man Computer Symbiosis*, Cornell University, 1960, consultabbile all'indirizzo web https://fermatslibrary.com/s/man-computer-symbiosis

[55] cfr. JOSEPH C. R. LICKINDER, *The Truly Sage System or Toward a Man-Machine System for Thinking*, 20 August 1957, 1-2, in *Licklinder Paper*, citato in Detti, Lauricella, *The origin of Internet*, cit.

[56] JOSEPH C. R. LICKINDER, *Lybrary of the future*, pagg. 6-21, citato in Detti, Lauricella, *The origin of Internet*, cit.

2.3 L'Intelligenza Artificiale.

Il contributo di Licklinder allo sviluppo della rete internet è stato principalmente di tipo teorico. Sul piano pratico forti erano i limiti della tecnologia allora esistente che egli riteneva potessero essere affrontati approfondendo lo studio di quei settori, allora indicati come Artificial Intelligence e self-organizing automata, che egli considerava legati.

Licklinder venne in contatto con scienziati, come Minsky e Shannon, che si occupavano di Intelligenza Artificiale, durante le Conferenze del Dartmouth College che si tennero a partire dal 1956.

Esse presero avvio da un seminario estivo di sei settimane finanziato dalla Rockefeller Foundation la quale propose uno studio sull'intelligenza artificiale da condursi *"sulla base della congettura che, in linea di principio, ogni aspetto dell'apprendimento o qualsiasi altra caratteristica dell'intelligenza possa venir descritto in modo così preciso da far sì che una macchina possa simularlo. Si cercherà di scoprire come costruire macchine che usano il linguaggio, formulano astrazioni e concetti, risolvono tipi di problemi oggi riservati agli esseri umani e si migliorano da sole"* [57].

Questo diverso filone di ricerca, che può essere ricondotto in termini generali entro la nozione di scienza cognitiva computazionale, si afferma parallelamente agli studi avviati da Weinner sulla cibernetica e alla ricerca che abbiamo visto sorreggere la costruzione dei primi network di comunicazione grazie dalla realizzazione delle prime macchine calcolatrici[58].

Questi sistemi vennero denominati "esperti" poiché capaci di memorizzare, conservare e organizzare *"basi di conoscenza concernenti ambiti ben precisi e delimitati, e di individuare le soluzioni a problemi complessi fino a quel momento non gestibili con le tecnologie informatiche disponibili"* [59].

Alla base di questo orientamento scientifico vi è l'analogia tra la mente umana e il computer per la quale la mente corrisponde alla

---

[57] GRACE SOLOMONOF, *Ray Solomonoff and the Dartmouth Summer Research Project in Artificial Intelligence, 1956*, consultabile all'indirizzo web http://raysolomonoff.com/dartmouth/dartray.pdf

[58] Nel 1951 presso l'università di Princeton venne realizzato il primo computer basato su reti neurali. Nel 1956 due ricercatori della Carniege Tech presentarono un programma in grado di ragionare, ovvero di pensare in modo non numerico e in grado di risolvere il problema della simulazione del rapporto mente-corpo. Ancora nel 1958 venne presentato un ulteriore programma in grado di elaborare la conoscenza per identificare la soluzione ai problemi.

[59] ANTONIO TETI, *PsychoTech*, citato, pag. 38

componente software della macchina mentre il corpo umano alla componente hardware[60].

Entro questo paradigma trovano applicazione gli studi condotti a partire dagli anni '50 nell'ambito dell'Intelligenza Artificiale. Tali studi hanno l'obiettivo di automatizzare alcune attività intellettive, in particolare il ragionamento e il comportamento con l'obiettivo di renderle schematiche e applicabili a qualsiasi contesto del pensiero umano.

Il rinnovato interesse che si produsse attorno a questo filone scientifico è legato da una parte, ai lavori del matematico Alan Mathison Turing e alla "macchina di Touring" con la quale dimostro che l'intelligenza, indipendentemente dalla presenza di un corpo fisico *"è un fatto esprimibile e riconoscibile mediante sequenze ben costruite di simboli"* [61]. In altri termini Touring evidenzia l'indistinguibilità tra un dispositivo tecnologico e un essere umano aprendo così la strada alla ricerca scientifica volta alla costruzione di un'Intelligenza Artificiale. Dall'altra, il modello di neurone elaborato nel 1943 da McCulloch e Pitts che costituì la base per lo studio e lo sviluppo delle reti neurali che rappresentano il modello di base degli attuali sistemi di calcolo computazionale.

I primi risultati di questa nuova scienza furono volti soprattutto ad offrire una dimostrazione delle sue potenzialità realizzando macchine il cui scopo era dimostrare che era possibile svolgere un dato compito[62].

Questi sistemi, tuttavia, non giunsero all'elaborazione di una Intelligenza Artificiale che fosse non solo in grado di imparare dall'esperienza, ma anche in grado di interpretare sensazioni, motivazione, emozioni e stato d'animo.

---

[60] Da questa distinzione deriva poi la separazione tra scienze della mente e neuroscienze. Mentre quest'ultime attengono allo studio del cervello quale componente hardware, lo studio della mente, del software, rientra nell'ambito della psicologia. A partire da questo modo di intendere il rapporto mente-macchina si è sviluppato il collegamento tra psicologia e informatica e di conseguenza la scienza cognitiva computazionale. Successivamente gli studi di Noam Chomsky sulla linguistica generativa e sulla teoria della grammatica hanno fornito nuovi contributi per la comprensione dell'utilizzo del computer come elemento di simulazione delle caratteristiche dell'uomo.

[61] ANTONIO TETI, *PsychoTech*, citato, pag. 29

[62] Appartengono a questo periodo il sistema Logic Theorist capace di dimostrare alcuni teoremi di matematica. Il programma General Problem Solver che era in grado in linea di principio di risolvere problemi posti in modo formale. Il robot Shakey che dimostrò la possibilità di integrare il ragionamento logico e con la percezione riuscendo così a indirizzare e controllare l'attività fisica.

Furono gli sviluppi successivi, in campo scientifico e tecnico, a determinare le condizioni perché si realizzassero progressi nei diversi settori e nella complessiva architettura e funzionalità del cyberspace.

2.4 Il Cyberspace quale spazio unitario.

Lo sviluppo degli studi sull'Intelligenza Artificiale presenta anch'esso il carattere della interdisciplinarità che abbiamo visto esser proprio della comunità scientifica del 900. I lavori dei singoli scienziati nei diversi campi si intrecciano nelle medesime università e centri ricerca e, anche se attendono alla risoluzione di problemi differenti, si influenzano a vicenda rispondendo a comuni interessi securitari. Allo stesso tempo, tuttavia, la consapevolezza da parte di questi uomini di far parte di una comunità di scienza amplia gli orizzonti in cui i loro lavori potevano trovare applicazioni concrete.

Viene così ad affermarsi un'idea di progresso che giunge oggi a manifestarsi nell'attuale società della conoscenza attraverso un percorso caratterizzato da diverse fasi di innovazione e, si potrebbe dire, di riflessione ora in un campo della scienza ora nell'altro.

Lo sviluppo e l'affermazione delle diverse tecnologie che sorreggono il cyberspace è durato un cinquantennio dipanandosi lungo tre fasi coerentemente volte verso l'implementazione dell'accessibilità alla tecnologia, dell'interattività tra i diversi elementi tecnologici e della diffusione delle fonti di origine dei dati. Parallelamente la ricerca scientifica traeva da ciò gli strumenti per nuove elaborazioni teoriche che a loro volta determinavano nuovi avanzamenti tecnologici.

Così, a partire dai diversi studi indicati, si giunse nel 1969 alla messa in funzione del network ARPANET che racchiudeva in se i frutti della teoria della comunicazione, dei concetti di feedback e di funzione dell'informazione oltre che dei modelli di elaborazione delle forme di integrazione tra uomo e macchina e dei modelli di comunicazione, sviluppati a partire dagli studi di Wiener, Licklinder e Taylor.

Soprattutto, al di là delle sue applicazioni militari, esso rispondeva da una parte, all'idea che l'informazione non costituisse un oggetto suscettibile di possesso ma piuttosto un processo, un flusso basato sulla condivisione comunitaria delle informazioni.

Dall'altra rispecchia la convinzione propria dei diversi scienziati di far parte di una comunità dedita alla conoscenza e che questa potesse

essere accresciuta dallo sviluppo di processi di comunicazione e collaborazione tra i diversi centri di ricerca.

La rete ARPANET, che originariamente metteva in collegamento le quattro principali università statunitensi, rappresentava quindi lo strumento nel quale trovarono applicazione le diverse teorie scientifiche e attraverso il quale si realizzò un primo nucleo di quella che oggi viene definita società della conoscenza[63].

A partire da questo nucleo di base, e coerentemente con i suoi caratteri, sia la ricerca scientifica che le innovazioni tecniche, si svilupparono ad un ritmo costante che vede la complessità dei processori e quindi le potenzialità di calcolo e di ricerca, raddoppiare ogni due anni, secondo la nota legge di Moore[64].

Tuttavia, sono ancora le dinamiche di competizione esterne al mondo scientifico ad influenzare il progresso tecnologico. In particolare, negli anni '80 fu lo sviluppo economico del Giappone a sostenere la realizzazione di nuovi computer che diedero la spinta alla ricerca che delineerà i fondamenti delle moderne tecnologie[65].

Ciò porterà nella seconda metà degli anni 90 alla elaborazione di *"agenti intelligenti inglobati in un sistema fisico artificiale"* [66], ovvero robot dotati di capacità cognitive, rese possibili dallo sviluppo delle reti neurali, attraverso le quali interagiscono quotidianamente con il mondo circostante grazie alle informazioni che su di esso ricavano attraverso sensori sempre più sviluppati[67].

---

[63] FRANCESCO VESPASIANO, *La società della conoscenza come metafora dello sviluppo*, Franco Angeli editore, 2005

[64] Gli anni '70 e '80 furono caratterizzati dalla realizzazione di nuove invenzioni volte ad affrontare problemi legati da un lato alle forme e agli strumenti di interazione uomo-macchina e, dall'altro ai linguaggi di programmazione. Ciò permise lo sviluppo di personal computer dotati di sistemi operativi general purpose che ne favorì l'utilizzo nei più vari campi, dalla gestione delle prenotazioni dei voli ai videogiochi fino ai mercati finanziari e all'uso domestico. In questo momento le tecnologie dell'informazione iniziano ad acquisire quella dimensione globale e pervasiva che le caratterizza tuttora.

[65] Appartengono a questi anni l'elaborazione delle tecnologie di data mining, i modelli per la comprensione del linguaggio parlato che troveranno applicazione nei sintetizzatori vocali ad uso medico, le reti baynesiane e i c.d. sistemi esperti in grado di agire razionalmente di cui il principale esempio è il sistema operativo Microsoft Windows. Allo stesso tempo sul piano filosofico si sostiene che l'auto-consapevolezza umana è semplicemente il risultato di sistemi seriali implementati da un hardware fornito dall'evoluzione.

[66] NICK BOSTROOM, *Superintelligenza*, Bollati Boringhieri, Torino 2018

[67] È questo l'ambito proprio della scienza cognitiva neurale la quale si basa sull'osservazione che *"la mente umana non è solo intelletto e capacità cognitive, ma è qualcosa di molto più complesso in funzione delle molteplici "antenne" ricettive di cui dispone e che influiscono, in qualche modo, sull'elaborazione mentale dell'individuo"*. Da qui lo sviluppo di nuovi modelli per lo studio delle scienze umane. La psicologia statunitense elaboro questo modello a partire

Gli sviluppi scientifici illustrati avevano portato nel loro complesso alla definizione di un nuovo linguaggio per l'astrazione delle informazioni dalla realtà, il codice binario, così come a nuovi strumenti di estrapolazione e manipolazione dei dati rilevati, le macchine computazionali. Allo stesso tempo erano state elaborate nuove forme di trasmissione e comunicazione delle comunicazioni, le reti internet.

A partire da essi si erano sviluppati numerosi network di dimensioni variabili, collegati a centri universitari o a corporation commerciali, che permettevano la trasmissione di informazione sulla base di protocolli differenti.

Fu solo nel 1989 che si giunse alla definizione di una forma di scrittura, di un alfabeto comune che permettesse di superare i limiti delle nuove tecnologie, rappresentati dalla disomogeneità dei linguaggi informatici, dando loro al contempo un carattere universale.

Tim Berner Lee, informatico al CERN, diede unitarietà allo spazio cyber definendo i protocolli del World Wide Web che facilitarono l'indicizzazione delle informazioni, la loro trasmissione e soprattutto semplificarono la creazione di contenuti da parte degli utenti.

Basandosi anch'egli su ricerche, studi, idee elaborate in diversi momenti e contesti Tim Berner Lee aggiunse alla rete Internet, il supporto per la scrittura, memorizzazione e trasmissione della conoscenza, una scrittura universale, un alfabeto digitale utilizzabile facilmente e liberamente accessibile.

A partire da questo momento il cyberspace acquista una dimensione universale che, attraverso i successivi sviluppi, lo porterà a costituire l'infrastruttura per la società della conoscenza che nel secondo decennio informerà la società sulla base dei suoi intrinseci caratteri, primo fra tutti l'interdisciplinarietà che abbiamo visto caratterizzare la ricerca scientifica che ne è alla base.

---

dagli studi delle reti neurali come modello per l'analisi e la decifrazione di esempi comportamentali basandosi sull'assunto che "le informazioni all'interno della rete neurale, indipendentemente dal fatto che sia biologica o artificiale, sono distribuite nei molteplici "nodi" della rete e non in un unico contenitore"[67] (ANTONIO TETI, *PsychoTech*, citato pag. 70 e ss.). Si delinea in tal modo un paradigma teorico attraverso il quale individuare la struttura della mente umana tramite lo studio del suo cervello, del suo hardware, che non si limiti ad elaborare informazioni ma che sia in grado di interpretare tutte le informazioni generali dell'individuo.

3. La struttura del Cyberspace.

L'affermazione del cyberspace quale spazio unitario e universale resa possibile dalla realizzazione dei protocolli del World Wide Web ha posto la necessità di comprenderne tanto la struttura quanto i caratteri qualificanti di tale nuova dimensione delle relazioni sociali.

I primi studi condotti negli anni 90 del secolo scorso ne hanno delineato la struttura multilivello, logico e regionale, per cui il cyberspace consisterebbe in un *"intangible place between computers where information momentarily exist on its route from one and the global network to the other … the ethereal reality, an infinity of electron spending down … [but also] think of cyberspace as being divided into groups of logical or regional cyberspace – hundreds and millions of smaller cyberspaces all over the word"*[68]. In altri termini il cyberspace sarebbe costituito da *"dinstict entities, whit clearly defined electronic borders … Small-C cyberspace consist of personal, corporate or organizational space … Big –C cyberspace is the National Information Infrastructure … add [coth] and then tie it all up with threads of connectivity and you have all of cyberspace"*[69].

Un rilevante passo in avanti nella comprensione dei caratteri qualificanti il cyberspace è stato compiuto a partire dalle elaborazioni, di natura scientifica, che si sono susseguite tra la fine degli anni Novanta e i primi anni del nuovo secolo. Nel 1998 Edward Waltz chiarì che *"The cyberspace dimension refers to the middle layer – the information infrastructures – of the three realms of the information warfare battlespace. These three realms are the physical (facilities, nodes), the information infrastructure, and the percentual"*[70]. Altre definizioni considerano il cyberspace come *"the environment created by the confluence of cooperative networks of computer, information system, and telecommunication infrastructure commonly referred to as the internet and the world wide web"*[71]. O, ancora, come *"The*

[68] WINN SCHWARTAU, *Information Warfare: Chaos on the Electronic Superhigway*, Thunder's Mouth, New York, 1994
[69] WINN SCHWARTAU, *Information Warfare: Chaos on the Electronic Superhigway*, Thunder's Mouth Press, 2° Ed., 1996
[70] EDWARD WALTZ, *Information Warfare: Principle and Operations*, Artech House, Inc. Norwood, MA, USA, 1998
[71] WALTER GARY SHARP, *Cyber Space and the Use of Force*, Aegis Research Corporation, USA, 1999

information space consisting of the sum total of all computer network"[72].

Infine nel 2001 Gregory Rotray descrive il CS *come "A physical domain resulting from the creation of information systems and network that enable electronic interaction to take place … cyberspace is a man-made environment for the creation in a variety of formats … CS consist of electronically powerd hardaware, networks, operating system and transmission standard"*[73].

Un ruolo di particolare importanza nella costruzione e nella definizione dei caratteri del cyberspace è stato svolto dal comparto militare statunitense. Gli stretti rapporti con il mondo accademico e con centri di ricerca altamente specializzati che caratterizzano le forze armate statunitensi sono alla base della costruzione del cyberspace e della ricerca volta ad individuarne i caratteri principali.

Rispetto al problema definitorio qui affrontato, di particolare interesse è il lavoro svolto dal Center of Tecnology and National Security della National Defence University[74]. L'attività di tale centro studi della Difesa statunitense ha permesso una prima opera sistematica dei diversi aspetti caratterizzanti il cyberspace.

Lo studio parte dall'osservazione che le diverse definizioni indicate suggeriscono tutte che il cyberspace sia qualcosa in più che semplici computer e informazioni digitali. Pur contenendo gli elementi già individuati la definizione proposta ne offre una diversa lettura volta ad evidenziarne la natura globale, la centralità dello spettro elettromagnetico, l'interazione tra le tecnologie dell'informazione e la sua funzionalità rispetto alle attività di rilevazione, comunicazione, elaborazione dei dati.

In questa prospettiva il cyberspace viene descritto come *"a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and*

---

[72] DOROTHY DENNING, *Information Warfare and Security*, Addison-Wesley Longman Ltd. Essex, UK, 1999

[73] GREGORY RATTRAY, *Strategic Warfare in Cyberspace*, MIT Press, Cambridge, MA, 2001

[74] FRANKLIN D. KRAMER, STUART H. STARR, AND LARRY K. WENTZ, *Cyber power and National Security*, Center for technology and national security policy, National Defense University, Washington D.C., University of Nebraska Press; 1 edition, 2009

exploit information via interdipendent and interconnected networks using information – communication technologies"[75].

La sua natura globale è determinata da una componente naturale quale lo spettro elettromagnetico che sorregge il funzionamento e lo sviluppo delle infrastrutture e delle tecnologie delle telecomunicazioni sostanzialmente senza vincoli territoriali mentre l'interazione tra tali tecnologie permette l'operatività all'interno dello spazio cyber al fine di creare, archiviare, modificare estrarre e sfruttare le informazioni.

Gli elementi costitutivi del cyberspace rilevati in queste prime definizioni troveranno corretta sistemazione nelle analisi sviluppate nella seconda metà degli anni 2000 le quali, utilizzando i metodi della stratigrafia, hanno permesso la ricostruzione della struttura del cyberspace e dei rapporti tra i suoi elementi costitutivi.

Il cyberspace viene in questo momento descritto come uno spazio sviluppato su tre livelli: fisico logico e sintattico.

3.1 Il livello fisico.

Lo strato fisico rappresenta le fondamenta dell'architettura complessiva delle tecnologie ITC. Esso è costituito da tutte le infrastrutture e i dispositivi fisici necessari all'elaborazione, memorizzazione e trasmissione digitale dei dati. Include inoltre il segnale che viaggia attraverso questi hardware così come risorse naturali e apparati: alimentazione elettrica, infrastrutture, materiali rari, componenti industriali, circuiti elettronici, protocolli e linguaggi dedicati, sofisticate tecnologie di installazione, stazioni che ospitano i dispositivi di raccolta, smistamento ed immagazzinamento dei dati.

Questo primo strato può essere suddiviso in tre macroaree costituite: a) dai mezzi di comunicazione ottici/rame (cavi sottomarini e terrestri); b) dai sistemi di comunicazione radio-terrestre (ponti radio, standard di telefonia cellulare, wi-fi, WiMax, ecc.); c) dai mezzi di comunicazione satellitare (satelliti geostazionari ecc.)

Accanto a queste strutture di base si possono collocare, in ragione della loro funzione rispetto al funzionamento del CS, le attrezzature ubicate negli Internet Exchange Hub Points che smistano il traffico dati.

---

[75] DANIEL T. KUEL, *From Cyberspace to Cyberpower: Defining the Problem*, in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security*, citato, pag. 28 e ss.

3.2 Il livello logico.

Il secondo livello è costituito dallo strato logico ovvero l'insieme delle connessioni informatiche che esistono tra i vari "nodi" di una rete. Il modo in cui queste connessioni sono state progettate determina la natura del CS al punto che è stato rilevato che *"it would been possible to build a very different Internet within the constraints of the same physics"* [76].

Nel dettaglio il livello sintattico contiene i programmi e i protocolli attraverso i quali le informazioni sono formattate e controllate attraverso i diversi sistemi (come computer e network). Il livello logico, inoltre, governa la connettività fisica (ad esempio il protocollo di funzionamento della fibra ottica); il corretto trasferimento dei bit attraverso determinati protocolli (ad esempio i protocolli TCP/IP); i parametri della qualità del servizio; la formattazione dei messaggi e gli schemi dei database.

Su tali componenti di base, attraverso la loro combinazione logica, vengono determinati servizi sempre più complessi a cui è possibile accedere, ad esempio, attraverso la rete Internet. Il livello base include quindi i programmi di esecuzione dell'ambiente informatico di riferimento, i meccanismi per la trasmissione dati e gli standard per la formattazione dei dati[77]. Su di essi sono costruite le applicazioni quali i programmi di scrittura i database o il Web. Combinando i diversi elementi si possono creare servizi più complessi. Ad esempio, combinando database e Web si ottengono strumenti, quali le "App" che usiamo sui cellulari, in grado di generare contenuti in maniera più dinamica[78].

[76] DAVID CLARK, *Characterizing the cyberspce: past, present and future*, MIT CSAIL Version 1.2 of March 12, 2010

[77] M. C. LIBINKY, *Conquest in Cyberspace. National Security and Information Warfare*, Cambrige University Press, 2007

[78] DAVID CLARK, *Characterizing the cyberspce: past, present and future*, citato

3.3 Il livello sintattico.

Il livello sintattico rielabora i dati contenuti nelle macchine. Quest'ultimi possono essere distinti in dati costituenti il cyberspace e in dati immessi dagli utenti nel cyberspace.

I primi sono l'insieme di regole, protocolli e standard che vanno a costituire le regole di funzionamento del cyberspazio. I dati costituenti trovano la loro importanza nella capacità di incidere su forma e funzionamento del cyberspace determinandone il carattere intrinsecamente mutevole che lo differenzia dai domini interamente naturali.

I secondi sono costituiti dai dati immessi dagli utenti e dalle macchine stesse nel loro interagire quotidiano attraverso le tecnologie dell'informazione.

La produzione, l'immagazzinamento, la diffusione dei dati sono i motivi principali che spingono allo sviluppo del cyberspace. Ed in tale percorso di sviluppo i dati stessi hanno cambiato quantità e qualità. Dal codice morse siamo arrivati alla gestione e elaborazione di Big Data, ovvero pacchetti di dati di dimensioni eccezionali di diversa qualità. Dati ricavati dalle macchine autonomamente.

4. I caratteri strutturali e dinamici del Cyberspace.

Il cyberspace costituisce dunque uno spazio operativo che attraverso l'uso della tecnologia elettronica e delle proprietà dello spettro elettromagnetico permette di operare sulle informazioni attraverso la connessione di reti tecnologiche interdipendenti e interconnesse.

Si tratta di uno spazio determinato a partire da una base naturale, lo spettro elettromagnetico, ma che è definito dall'opera dell'uomo così che sono le tecnologie che esso sviluppa a determinare oltre la struttura anche i suoi peculiari caratteri e le problematiche che da questi derivano.

Da questa prospettiva il cyberspace si presenta anzitutto come uno spazio integrato, in quanto costituito dall'interazione tra le diverse tecnologie dell'informazione, e pervasivo, data la rilevanza di esse in pressoché tutti gli ambiti della vita sociale.

Allo stesso tempo è uno spazio aperto, facilmente accessibile da chiunque in ragione dei bassi costi in termini di competenze e di risorse necessarie per operare attraverso le tecnologie ITC.

Da quest'ultime lo spazio informatico trae il suo carattere dual-use dal quale dipende la rilevanza al contempo civile e militare, tanto delle tecnologie quanto del loro utilizzo.

Il cyberspace si presenta infine come uno spazio anarchico in quanto privo di una disciplina che ne garantisca la sicurezza e ne informi le azioni che i diversi attori pongono in essere al suo interno.

4.1 Integrazione e pervasività.

I caratteri dell'integrazione e della pervasività definiscono il cyberspace quale infrastruttura di infrastrutture la cui rilevanza cresce all'aumentare dei rapporti politici, commerciali ed economici tra i vari attori favoriti dallo stesso sviluppo delle tecnologie informatiche.

La crescente interdipendenza economica tra paesi, realizzata attraverso l'aumento del volume e delle varietà di beni e servizi scambiati internazionalmente, oltre che attraverso la crescita dei flussi internazionali di capitali, è stata infatti sorretta dallo sviluppo delle tecnologie ITC che hanno permesso l'abbattimento dei costi di comunicazione e l'implementazione delle capacità di elaborazione dell'informazione.

A sua volta ciò a favorito la movimentazione di capitali a più breve termine che, assieme alla riduzione delle barriere informative ha creato le condizioni per lo sviluppo di investimenti esteri contribuendo all'estensione dei mercati su scala globale.

La diffusione dell'accesso alle tecnologie ITC ha favorito, in particolare, il trasporto delle idee rendendo più facile e immediata la condivisione di ricerche, studi progetti di ingegneria, rispetto a quanto permesso dai tradizionali sistemi di comunicazione, incidendo profondamente sulla produzione internazionale di beni miniaturizzati ad alto livello tecnologico o di carattere immateriale.

È questo il contesto in cui si sviluppano le tecnologie dell'Internet of Things[79] che, quale implementazione del web, attualmente

[79] Le tecnologie Internet of Things (IoT) possono essere descritte, in termini generali, come *"the many uses and process that result from giving a network address to a thing and fitting it with sensors"* [79] (MERCEDES BUNZ, GRAHAM MEIKLE, *The internet of things*, Polity Press, Cambridge UK, 2018). Esse assumono anzitutto i caratteri di *"emerging global internet based*

costituiscono *"un'infrastruttura globale per la società dell'informazione, che consente servizi avanzati collegando le cose (fisiche e virtuali) basate su tecnologie di informazione e di comunicazione interoperabili esistenti e in evoluzione"*[80].

Attraverso tali tecnologie si determina da una parte, il passaggio dalla connessione in qualsiasi momento e luogo, alla connessione di ogni cosa evidenziando, nella realizzazione di *"a new dynamic network of networks – an Internet of Thnings"*[81] il carattere integrato del cyberspace; dall'altro si concretizza la nozione di Cyber-Physical System con la quale si fa riferimento alla *"next generation of embedded ICT system where computation and networking are integrated whit physical process and they control and manage their dynamics and make them more efficient, reliable, adaptable and secure"*[82], evidenziando in ciò la pervasività delle tecnologie analitiche.

Le diverse applicazioni di questa tecnologia possono essere raggruppate entro tre domini principali.

In primo luogo, il dominio industriale, dove si pongono alla base dei processi di Industry 4.0 trovando applicazione nella logistica, nella manifattura, nel controllo dei sistemi produttivi, nel trasporto

---

information architecture facilitating the exchange of goods and service in global supply chain network" [79](COLF H. WEBER, *Internet of Things – New security and privacy challenges*, Computer Law & Security Review 26 (2010) 23-30; per una panoramica generale sull'argomento, dello stesso Autore, *Iternet of Things – Need for a New Legal Enviroment*, Computer Law & Security Review n. 25 (2009)). Il loro impatto economico si stima possa essere, a partire dal 2025, di 11,1 trilioni di dollari all'anno[79] (MCKINSEY GLOBAL INSTITUTE analysis, *How we can recognize the real power of the Internet of Things?*,, consultabile all'indirizzo web https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-can-we-recognize-the-real-power-of-the-internet-of-things), a fronte di un numero di dispositivi di circa 50 miliardi, corrispondente a oltre 6 dispositivi per persona [79](DAVE EVANS, *Cisco Internet Business Solutions Group, The Internet of Things. How the next evolution changing everything*, Aprile 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf) che salgono a 1000 considerando i sensori che sono posti nelle infrastrutture e negli spazi pubblici (A. SANGIOVANNI-VINCENTELLI, *Let's get physical: adding physical dimensions to cyber systems*, in: Internet of Everything Summit, Roma, July 201). Altrettanto vaste sono le aree in cui le tecnologie IoT possono trovare applicazione grazie alla loro duplice capacità di rilevare dati (relativi ad esempio a fenomeni naturali, parametri medici e altro) e di fornire, sulla loro base, nuovi servizi.

[80] ITU, Recommendation ITU-T Y.2060, 06/2012, Overview of the Internet of Things

[81] ITU, Recommendation ITU-T Y.2060, 06/2012, Overview of the Internet of Things

[82] ELEONORA BORGIA, *The Internet of Things vision: Key features, application and open issues*, Computer Communications 54 (2014), p. 1-31

permettendo il monitoraggio dell'intero ciclo di vita e di utilizzo degli oggetti[83].

Trovano applicazione nell'ambito delle c.d. *smart suistinable city*[84] (SSC), ovvero, nella definizione proposta dall'ITU, *"an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and service and competitiviness, while ensuring that it meets the needs of present and future generations with respect to economic, social, enviromental, as well as cultural aspects"* [85] dove assumono un ruolo centrale nella gestione delle risorse e dei servizi in contesti di forte urbanizzazione [86].

---

[83] Favoriscono, al contempo, l'adozione di nuovi sistemi di sicurezza ad esempio durante il trasporto, dove permettono di effettuare in tempo reale la diagnostica dei veicoli e dei carichi trasportati e l'intervento precauzionale dell'uomo[83] (P. HANK, S. MÜLLER, O. VERMESAN, J. VAN DEN KEYBUS, *Automotive ethernet: invehicle networking and smart mobility*, in: Proceedings of the Conference on Design, Automation and Test in Europe (DATE'13), 2013, pp. 1735–1739). Allo stesso modo può essere monitorata l'attività e la salute del bestiame così come il ciclo di crescita delle piantagioni all'interno di aziende agricole che, sulla base delle informazioni ricavate dall'elaborazione dei dati rilevati, possono garantire una maggiore sicurezza alimentare e offrire nuovi servizi ai consumatori[83] (A.S. VOULODIMOS, C.Z. PATRIKAKIS, A.B. SIDERIDIS, V.A. NTAFIS, E.M. XYLOURI, *A complete farm management system based on animal identification using RFID technology*, Comp. Electron. Agricult. 70 (2) (2010) 380–388. ; J. MA, X. ZHOU, S. LI, Z. LIO, *Connecting agriculture to the internet of things through sensor networks*, in: Proceedings of Internet of Things (iThings/CPSCom), 2011, pp. 184–187; D. YAN-E, *Design of intelligent agriculture management information system based on IoT*, in: Proceedings of International Conference on Intelligent Computation Technology and Automation (ICICTA), 2011, pp. 1045– 1049; S. LI, S. PENG, W. CHEN, X. LU, *Income: practical land monitoring in precision agriculture with sensor networks*, Comp. Commun. 36 (4) (2013) 459–467.; J. CHUN ZHAO, J. FENG ZHANG, Y. FENG, J. XIN GUO, *The study and application of the IOT technology in agriculture*, in: Proceedings of 3rd IEEE Computer Science and Information Technology (ICCSIT), 2010, 2010, pp. 462–465).

[84] H. SAMIH, *Smart cities and internet of things*, Journal of Information Technology Case and Application Research, 21:1, 3-12, https://doi.org/10.1080/15228053.2019.1587572; ILIAS O. PAPPAS, PATRICK MIKALEF, YOGESH K. DWIVEDI, LETIZIA JACCHERI, JOHN KROGSTIE, MATTI MÄNTYMÄKI (EDS.) *Digital Transformation for a Sustainable Society in the 21st Century. 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019 Trondheim, Norway, September 18–20, 2019*, Springer.

[85] ITU-T Y-series Recommendations – Supplement 33, 01/2016.

[86] La centralità di questo dominio è legata al ruolo che la città assume all'interno del più ampio fenomeno della globalizzazione a partire dalla seconda metà del XX° e l'inizio del XXI° secolo. Nel 2014 vi erano 28 mega città nelle quali viveva circa il 54% della popolazione mondiale che si stima sarà il 66% nel 2050. Tali agglomerati urbani devono confrontarsi con fenomeni di rapida urbanizzazione, inquinamento, migrazioni, da cui insorgono problematiche legate alla disponibilità di risorse naturali quali l'acqua, la terra, le fonti energetiche. Altre problematiche sono legate alle infrastrutture per i trasporti, all'accesso all'educazione, alla sicurezza dei cittadini così come alla gestione di un adeguato servizio sanitario

Infine, trovano applicazione nel dominio medico ove il loro utilizzo permette la realizzazione di servizi medici specifici per la singola persona così come l'attività di rilevazione di dati la cui quantità e qualità è alla base dei più avanzati progressi medici.

Lo sviluppo delle tecnologie IoT evidenzia, inoltre, la pervasività dello spazio cyber che con esse diviene elemento strutturale delle attività umane. In questo senso il cyberspace costituisce un'infrastruttura di infrastrutture poiché a partire da esso è possibile costruire e amministrare tanto infrastrutture di carattere pubblico e di rilevanza essenziale per gli stati quanto sviluppare reti di supply chain per i più vari servizi commerciali tanto globali quanto locali e quotidiani.

4.2 Big Data.

Il carattere integrato delle tecnologie ITC viene alla luce osservando lo sviluppo dei dati elaborati all'interno del cyberspace. Rispetto ad essi le tecnologie IoT, tra le altre, contribuiscono in maniera determinante all'incremento esponenziale della quantità e qualità di dati prodotti, immagazzinati ed elaborati nel cyberspace[87].

Si tratta infatti di un fenomeno, quello dei Big Data, legato all'aumento delle fonti di rilevazione e immissione dei dati e alla diminuzione dei costi per la loro conservazione e, dall'altro, allo

[87] Il modello di riferimento delle tecnologie IoT è costituito da quattro livelli ad ogni uno dei quali sono associate competenze di management e di sicurezza. Il primo livello (device layer) ha funzionalità legate ai singoli dispositivi tra le quali, quelle che permettono l'interazione diretta o indiretta con il network di comunicazione; la creazione di ad hoc network; "sleeping and waking-up" per il risparmio energetico. Altre funzionalità sono legate alla gestione della connettività attraverso diverse tecnologie e protocolli di comunicazione. Il secondo livello (network layer) svolge due tipi di funzioni. La prima consiste nel controllo della funzionalità della connettività del network; la seconda attiene al trasporto delle informazioni necessarie al funzionamento delle applicazioni. Il successivo livello (Service support and application support layer) offre competenze generiche nell'elaborazione e memorizzazione dei dati. Queste sono poi alla base di competenze specifiche in grado di fornire supporto alle diverse applicazioni della tecnologia Iot. Il quarto livello (application layer) è costituito semplicemente dalle applicazioni che possono essere create attraverso la tecnologia IoT. Entro questi tre livelli si svolgono le tre fasi di raccolta, trasmissione, elaborazione e utilizzazione dei dati raccolti dai device IoT sull'ambiente a loro circostante, ogni una supportata da tecnologie il cui steso utilizzo determina la direzione del suo sviluppo rispondendo più ad una logica di casualità anziché di progettazione. Da questo punto di vista, acquisiscono, per le ragioni che vedremo più avanti, una particolare importanza le tecnologie utilizzate nella fase di elaborazione dei dati raccolti e che attengono all'elaborazione e utilizzo di Big Data. Cfr. ITU, *Recommendation ITU-T Y.2060, 06/2012, Overview of the Internet of Things*

sviluppo di particolari metodologie per la loro elaborazione al fine di trarre da essi un nuovo contenuto informazionale.

La quantità di dati prodotti dal cyberspazio pone quindi il problema qualitativo di come *"utilizzare questo immenso oceano di dati per attività di ricerca, analisi ed elaborazioni finalizzate alla produzione di una "conoscenza" specifica per tematiche diverse"* [88]. Da questo punto di vista il termine Big Data sta quindi ad indicare *"il complesso di attività di elaborazione e gestione dei dati finalizzate alla loro trasformazione in un elemento di valore"* [89].

Tuttavia, il fenomeno dei Big Data, come gli altri aspetti del cyberspace che sono stati finora osservati, non ha una definizione condivisa, in ragione del carattere mutevole sia dello stesso cyberspace sia del rapporto tra questo e la realtà fisica.

Entrambi, infatti, sono soggetti agli sviluppi della tecnologia e della capacità di trarre da essa nuovo valore in funzione dell'impatto sociale che genera.

Entro una prospettiva ampia, al significato di Big Data possono dunque ricondursi *"le cose che si possono fare su larga scala, per estrapolare nuove indicazioni o creare nuove forme di valore, con modalità che vengono a modificare i mercati, le organizzazioni, le relazioni tra cittadini e governi, e altro ancora"* [90].

Tecnicamente i big Data sono costituiti da raccolte di dati non omogenee, distribuite, accessibili in rete, non strutturate, le cui principali caratteristiche sono Volume Velocità Varietà Veridicità.

Tuttavia, la loro peculiarità risiede nelle metodologie e negli strumenti fondati su architetture di elaborazioni specifiche, volte *"all'analisi di dati su larga scala per estrapolare nuove indicazioni e nuove forme di valore"* [91] in grado di implementare la loro caratteristica "*fruibilità per elaborazioni massive anche in contesti caratterizzati da alta velocità di aggiornamento"* [92].

Tali metodologie di calcolo permettono di individuare associazioni, regolarità nascoste tra i dati, sulle quali costruire un

---

[88] ANTONIO TETI, *Lavorare con i Big Data. La guida completa per il Data Scientist*, pag. XXI Tecniche nuove, 2017

[89] ID.

[90] VIKTOR MAYER-SCHONMERGER, KENNETH COKIER, *Big Data*, Garzanti, 2017, p. 16.

[91] ANTONIO TETI, *Lavorare con i Big Data. La guida completa per il Data Scientist*, pag. XXI Tecniche nuove, 2017.

[92] COSIMO COMELLA, *Origine dei Big Data*", GNOSIS, 2/2017, pag. 132

modello informativo, di tipo descrittivo o predittivo, a supporto dell'attività di decisione[93] .

Il loro tratto caratteristico consiste nella capacità di apprendere dall'osservazione di esempi diversi che si verificano nel mondo osservato senza dover determinare le relazioni esistenti attraverso *"l'applicazione della matematica a enormi quantità di dati per desumerne delle probabilità"* [94].

Le più avanzate di tali metodologie, di conseguenza, non vengono programmate bensì addestrate mediante algoritmi di apprendimento in grado di modificarne il funzionamento così che esse sono in grado di generalizzare, ovvero di fornire valori di output accettabili anche per input diversi da quelli inizialmente definiti

Il Deep Learning consiste infatti in *"un'insieme di pattern architetturali per reti neurali che permettono l'analisi di problemi complessi mediante la scomposizione in sotto-problemi più semplici"*[95]. In questo modo, sostanzialmente, la macchina apprende automaticamente i concetti più complessi lavorando sulla base di concetti più semplici elaborando dati che già gli sono stati forniti o che essa stessa ha raccolto dal mondo esterno tramite plurimi sensori.

---

[93] Lo sviluppo di nuove metodologie di calcolo prese avvio nei primi anni 90 quando, attorno ai concetti di *Data Mining* e *Knowledge discovery in database* (KDD), si creò un movimento scientifico interdisciplinare che portò allo sviluppo di modelli, metodi e algoritmi per l'analisi dei dati quali: database e data mining, machine learning, support vector machine, random forest, deep learning e intelligenza artificiale, sistemi complessi e network science, statistica e fisica statistica, information retrieval e text mining, elaborazione del linguaggio naturale, matematica applicati. In particolare, il KDD può essere descritto come *"the non trivial process of identifyng valid, novel, potentially useful, and ultimatelly understandable patterns in data"*. Secondo altra definizione esso consiste in *"a knowledge-intensive task consisting of complex interactions, protracted over time, between a human and a (large) database, possibly supported by a heterogeneous sute of tool"*. In entrambi i casi viene in evidenza un processo costituito da un insieme di attività complesse per la manipolazione di dati al fine di estrarre informazioni precedentemente sconosciute e potenzialmente utili, in altri termini conoscenza. Tale processo è composto di sei fasi di cui il Data Mining è la più importante. Quest'ultima consiste nell'estrazione di conoscenza implicita, sconosciuta e potenzialmente utile da grandi quantità di dai. La sua principale funzione è quella di individuare associazioni, regolarità nascoste tra i dati, sulle quali costruire un modello informativo, di tipo descrittivo o predittivo, a supporto dell'attività di decisione. Diverse sono le tecniche sviluppate per questa attività, in particolare: gli alberi decisionali, il clustering, l'association rule learning e, infine le reti neurali. Quest'ultime in particolare permettono da un lato di evidenziare la continuità della ricerca scientifica nel tempo, dall'altra rappresentano il punto di partenza degli sviluppi legati all'Intelligenza Artificiale. Cfr Dino Pedreschi, *Data Science. La parola ai pionieri*; GNOSIS, 2/2017

[94] VIKTOR MAYER-SCHONBERGER, KENNETH CUKIER, *Big Data*, Garzanti, 2017, pag. 23

[95] ANTONIO TETI, *Lavorare con i Big Data. La guida completa per il Data Scientist*, cit., p. 358

È evidente in tale attività l'interazione tra le diverse teorie che abbiamo visto esser state elaborate dagli studi sulla cibernetica, il concetto di feedback elaborato da Weinner, e sull'intelligenza artificiale, a partire dalla definizione del neurone come unità logica condotti da Pitt.

Il design di tali metodologie di elaborazione di elaborazioni dati determina profondi mutamenti nel modo in cui vengono ricavate e utilizzate le informazioni la cui centralità nei processi decisionali determina a sua volta profondi mutamenti nella società.

In primo luogo, è ora possibile analizzare una quantità di dati elevata e, in molti casi è possibile processare tutti i dati relativi ad un determinato fenomeno[96]. L'utilizzo dei Big Data permette dunque di osservare i dettagli dei fenomeni fornendone una visione particolarmente chiara della loro struttura granulare. Inoltre, alla enorme quantità di informazioni da processare, è legato il corretto funzionamento dei sistemi di Big Data Analatycs l'attendibilità delle cui analisi previsionali cresce all'aumento della base di dati da analizzare. Occorre evidenziare come la stessa attività di analisi produca ulteriori dati che vengono registrati e utilizzati dai sistemi di analisi per automigliorarsi nel tempo attraverso la registrazione automatica dei sistemi dei segnali e degli andamenti più rilevanti che vengono costantemente monitorati. Entro questa prospettiva si può osservare da una parte, come il cyberspace trovi la sua risorsa essenziale nei dati e dall'altra, che esso produce ormai autonomamente i dati che gli sono necessari per il suo sviluppo.

In secondo luogo, all'aumento della dimensione della base dei dati da analizzare aumenta anche il numero delle imprecisioni che l'analisi può presentare.

In un contesto di Big Data, tuttavia, la precisione diviene un valore secondario rispetto alla possibilità di poter osservare i trend generali di un determinato fenomeno. Sul piano decisionale ciò comporta l'accettazione di un livello di rischio sostanzialmente definito dalla macchina in grado, tuttavia, di incidere sulla dimensione sociale

[96] L'area di applicabilità delle tecniche di Big Data Analytics è infatti definita dalla combinazione di dimensione dei dati e dei relativi tempi per elaborarli. Di conseguenza, l'analisi di molteplici Terabyte nell'ordine di pochi minuti rientra nelle attività di Big Data, diversamente, si fa riferimento a tecniche tradizionali di Data Warehouse e Data Mining se lo stesso risultato lo si può ottenere nell'arco di qualche giorno. (MICHELE COLAJANNI, *Il ruolo dei Big Data Analytics e Machine Learning nella sicurezza*, GNOSIS 2/2017, p. 79)

essendo le informazioni così elaborate la base per l'adozione di decisioni che, a vari livelli, modificano l'ambiente reale.

Infine, l'utilizzo dei Big Data determina il venir meno della centralità del rapporto di causalità. Come è stato osservato *"i big Data riguardano il cosa accade non il perché"*[97].

L'affermarsi dei sistemi di analisi basati su Big Data determina dunque la crisi di alcuni assunti fondamentali che hanno finora sorretto la società umana.

Da una parte viene posta in crisi la convinzione che le decisioni umane si fondino su informazioni limitate ma esatte e rispondenti ad un principio di causalità. È questa la principale conseguenza del passaggio da una lettura del mondo basata su idee di stampo newtoniano ad una di stampo, in senso lato, probabilistico.

Dall'altra, e di conseguenza, l'enorme quantità di dati da analizzare per prendere una decisione, determina la sostituzione delle macchine all'uomo nella stessa attività decisionale.

In questo senso i Big Data costituiscono dunque l'elemento alla base dello sviluppo delle capacità decisionali della macchina quale meta finale degli studi sull'Intelligenza Artificiale, avviati nell'estate del 1956 con il *Dartmouth Summer Project in Artificial Intelligence*[98].

Viene qui in rilievo l'ultimo elemento di integrazione e pervasività delle tecnologie ITC, l'Intelligenza Artificiale, che, al contempo, ne determina l'unità qualificando il cyberspace non solo come uno spazio d'azione entro il quale interagiscono diversi attori, ma anche come un fattore autonomo di progresso dell'uomo la cui dinamica di sviluppo può porre in discussione caratteri essenziali delle nostre società e della stessa idea di Umano.

---

[97] VIKTOR MAYER-SCHONMERGER, KENNETH COKIER, *Big Data*, Garzanti, 2017, p. 26

[98] Nonostante la diretta indicazione dell'oggetto delle discussioni, in cosa effettivamente esso consistesse non era stato ancora chiarito. Nei primi anni 50 si delineava una nuova scienza, caratterizzata dalla ricerca tecnologica e dalla sua interdisciplinarità, alla quale alcuni si riferivano in termini di cibernetica, altri la riconducevano alla teoria dell'automazione, altri ancora alla teoria della comunicazione, infine, in termini generali si parlava *thinking machine* o *Machine that Thinking*. Il termine Intelligenza Artificiale fu utilizzato nel 1955 da John McMcarty, un giovane Professore di Matematica dell'Università di Dartmouth, per la sua neutralità rispetto alle più assertive teorie dell'automazione e della cibernetica. Le diverse posizioni scientifiche ruotavano attorno al fondamento matematico o semantico dei modelli sulla cui base sviluppare le capacità cognitive delle macchine. Il Seminario di Dartmouth viene considerato come il momento di avvio della ricerca sull'Intelligenza Artificiale. Un inizio dalle grandi e confuse aspettative a cui segui un sessantennio caratterizzato da periodi di grande interesse e sviluppo e da altri in cui non si realizza alcun progresso. NICK BOSTROM, *SuperIntelligenza Tendenze, pericoli, strategie*, Bollati Boringhieri, pag 27

Da questa prospettiva è importate rilevare un aspetto che costituisce il carattere centrale della dinamica di funzionamento del cyberspace.

I tradizionali sistemi GOFAI si basavano su regole a loro volta basate sul rigido uso della logica il cui limite era l'instabilità rispetto alle analisi combinatorie più complesse [99]. Diversamente, i nuovi sistemi modellati sul funzionamento della mente umana pongono al centro delle loro analisi le connessioni tra i dati rilevate attraverso l'elaborazione simbolica.

La ricerca scientifica nei vari settori che contribuiscono allo sviluppo dell'Intelligenza Artificiale si orientano quindi verso un modello semantico piuttosto che logico matematico. Viene così ad affermarsi l'idea di un connessionismo che, differentemente dal cognitivismo basato sull'analogia tra mente e computer software e considera la mente come una manipolazione di simboli, rifiuta l'analogia mente/computer e interpreta il comportamento e le abilità cognitive utilizzando modelli teorici che sono direttamente ispirati alla struttura fisica e al modo di funzionare del sistema nervoso.

Reti neurali e algoritmi genetici sono metodi la cui introduzione negli anni 90 suscitò nuovo interesse scientifico attorno all'Intelligenza artificiale[100].

---

[99] Le potenzialità dei primi computer realizzati in quegli anni permisero lo sviluppo di sistemi semplici volti a dare una dimostrazione del concetto mostrando che un dato compito in linea di principio poteva essere eseguito da una macchina. Tuttavia, all'aumentare della complessità del compito da eseguire si registrava un aumento delle operazioni computazionali da svolgere. Si trattava di un'esplosione combinatoria che gli algoritmi disponibili non erano in grado di analizzare. Nuovi progressi si registrarono negli anni 80 grazie alla ricerca scientifica portata avanti dal Giappone. La crescita economica registrata nel periodo postbellico sorresse la realizzazione di un partenariato pubblico privato per lo sviluppo dei computer della quinta generazione. Un'architettura tecnica che si immaginava sarebbe servita da piattaforma per l'intelligenza artificiale. È in questo momento che vengono elaborati i cd sistemi esperti basati su un paradigma logicistico e concentrati sulla manipolazione di simboli ad alto livello. Sistemi tuttavia che presentavano ancora un carattere instabile che ne limita l'utilizzo e conseguentemente lo sviluppo. Negli anni Novanta lo sviluppo delle reti neurali e degli algoritmi genetici sembravano superare tali limiti presentando rilevanti capacità di resilienza e di addestramento grazie all'introduzione dell'algoritmo di propagazione all'indietro che permise la funzionalità di reti neurali multistrato. NICK BOSTROM, *SuperIntelligenza Tendenze, pericoli, strategie*, Bollati Boringhieri, pag 29

[100] Le reti neurali artificiali, o più comunemente reti neurali, possono essere descritte come strutture computazionali il cui funzionamento è ispirato ai processi elaborativi che avvengono all'interno del cervello. Come abbiamo visto trattando dei fondamenti della cibernetica, la possibilità di utilizzare reti di unità logiche costruite sul modello della rete di neuroni del cervello umano, prende le mosse dagli studi di W.S. McCulloch e W.H. Pitts. Il loro tratto caratteristico consiste nella capacità di apprendere dall'osservazione di esempi diversi che si verificano nel mondo osservato senza dover determinare le relazioni matematiche esistenti. Di

Gli studi che in seguito si svilupparono misero in evidenza come *"tecniche all'apparenza disparate si possano interpretare come casi speciali di un'unica struttura matematica"*[101] il cui modello ideale è quello dell'agente baynesiano perfetto in grado di far un uso probabilisticamente ottimo dei dati di cui dispone combinandole al fine di prendere una decisione orientata alla massima utilità attesa.

Sono frutto di questa impostazione, tra gli altri, i modelli di Data Mining più avanzati, gli algoritmi di Deep Learning e Machine Learning, che abbiamo visto esser utilizzati nella Big Data Analytics.

Si tratta di algoritmi che seppur differiscono per aspetti tecnici quali il tempo di elaborazione e lo spazio di memoria richiesta, ai bias induttivi che presuppongono, alla facilità di recepire contenuti dall'esterno e alla trasparenza del loro funzionamento rispetto all'operatore, condividono un carattere intrinsecamente probabilistico.

L'attualità delle tematiche connesse allo sviluppo tecnologico è data, diversamente dal passato, dalle potenzialità economiche che l'applicazione dell'IA riesce a generare nei diversi domini in cui viene applicata, con l'ulteriore caratteristica che la sua stessa applicazione genera nuovi domini entro cui operare: dagli assistenti virtuali alle automobili a guida autonoma; dal riconoscimento vocale alla traduzione automatica fino ai programmi di sintesi vocale e all'aggregazione automatica di notizie su cui si basano le operazioni finanziarie automatiche [102].

---

conseguenza le reti neurali non vengono programmate bensì addestrate mediante un algoritmo di apprendimento in grado di modificarne il funzionamento così che esse sono in grado di generalizzare, ovvero di fornire valori di output accettabili anche per input diversi da quelli inizialmente definiti. Nonostante le loro elevate capacità di calcolo gli algoritmi comunemente usati nel Data Mining non erano stati progettati per gestire la quantità di dati attualmente rilevata. Soprattutto non erano in grado di utilizzare adeguatamente dati che fossero dislocati in più database. Per superare i limiti del Data Mining e delle reti neurali classiche, negli ultimi anni si stanno sviluppando metodologie di elaborazione dati denominate Deep Learning. Si tratta di un insieme di pattern architetturali per reti neurali che permettono l'analisi di problemi complessi mediante la scomposizione in sotto-problemi più semplici. In questo modo la macchina apprende automaticamente i concetti più complessi lavorando sulla base di concetti più semplici. lo sviluppo di algoritmi per l'analisi dei dati ha contributo, al pari dell'aumento delle capacità di calcolo, all'emergere del fenomeno dei Big Data

[101] NICK BOSTROM, *SuperIntelligenza Tendenze, pericoli, strategie*, Bollati Boringhieri, pag. 32

[102] Tra i settori in cui già oggi l'IA determina importanti innovazioni rientrano anzitutto l'ambito medico. In questo settore lo sviluppo di strumenti IoT di rilevazione dello stato di salute del paziente offre ai sanitari dati in tempo reale che permettono di implementare l'efficacia delle cure apprestate ai pazienti così come nuove tecniche di manipolazione delle strutture biologiche del corpo umano. Il progetto "InnerEye" della Microsoft utilizza la tecnologia IA sviluppata per i videogiochi per l'analisi di immagini di risonanza magnetica al fine di fornire agli oncologi informazioni precise e dettagliate sulle problematiche del paziente,

4.3 Apertura.

Le attuali applicazioni dell'intelligenza Artificiale sono innumerevoli e pervadono gli aspetti quotidiani della vite delle persone per il tramite delle tecnologie ITC che, in misura sempre maggiore sono utilizzate dagli individui, o che con essi interagiscono direttamente o indirettamente.

Il numero di sensori che circondano l'individuo nella sua quotidianità, riconducibili entro il generale concetto di IoT, viene calcolato in termini di migliaia di sensori ed aumenta esponenzialmente[103].

Ciò da una parte favorisce le persone nelle loro varie attività, dall'altra, nella misura in cui l'individuo viene in rilievo nella sua dimensione datizzata, le trasforma nella principale risorsa di sviluppo del cyberspace legato, come visto, alla quantità e qualità di dati che le macchine computazionali possono elaborare.

In altri termini l'individuo è posto al centro della dinamica di sviluppo del Cyberspace, complessivamente considerato, con il duplice ruolo di fruitore della tecnologia e risorsa datizzata che sorregge lo sviluppo delle tecnologie stesse.

La posizione dell'individuo nel cyberspace è determinata dal carattere aperto dello stesso spazio informatico.

La facilità di accesso alle tecnologie digitali e alla rete internet, in ragione dell'esiguità delle risorse economiche e di conoscenza tecnica

---

l'utilizzo dei robot permette di effettuare operazioni particolarmente complesse. Un'importante area di applicazione delle tecnologie IA in campo medico riguarda lo sviluppo di applicazioni in grado di migliorare la qualità della vita di persone affette da disabilità. Un esempio è qui offerto da una semplice applicazione per cellulari realizzata da Microsoft e denominata "Seeing AI" che permette a persone non vedenti di interagire con la realtà in cui si trovano fornendo una descrizione audio dell'ambiente circostante e di ciò che vi accade. Di particolare importanza sono gli strumenti di analisi basati su Big Data e Intelligenza Artificiale che permettono il monitoraggio di fenomeni pandemici. Nel 2009 in occasione della diffusione del virus influenzale H1N1 i ricercatori di Google pubblicarono sulla rivista Nature un importante studio in cui spiegavano come Google fosse in grado di prevedere la diffusione dell'influenza invernale negli Stati Uniti sia a livello nazionale che regionale e locale. Ciò sulla base delle domande post dagli utenti al motore di ricerca. Un progetto simile, denominato "Project Premonition" è sviluppato da Microsoft per il contrasto alle epidemie di malattie quali Zika, Ebola, la febbre Dengue, trasmesse da animali e insetti attraverso l'utilizzo di avanzati droni capaci di viaggiare all'interno di ambienti complessi e identificare possibili fonti di contagio.

[103] PHILLIPPA BIGGS (ITU), JOHN GARRITY (CISCO), CONNIE LASALLE (CISCO) AND ANNA POLOMSKA (ITU), UNDER THE SUPERVISION OF DR. ROBERT PEPPER (CISCO), *Harnessing the Internet of Things for Global Development*, Report presentato alla ITU/ UNESCO Broadband Commission for Sustainable Development, consultabile all'indirizzo https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf

richieste per accedervi, ha favorito l'accesso ad un numero sempre maggiore di persone al cyberspace.

Ciò pone problemi di duplice natura.

Da un punto di vista securitario le principali problematiche riguardano le azioni malevole che i diversi attori, i singoli utenti della rete, possono porre in essere. Si tratta di uno spettro di azioni molto ampio che va da azioni di terrorismo ad azioni meramente criminali e illecite che possono coinvolgere singoli utenti più deboli così come soggetti economici di grande rilevanza. Particolarmente interessanti sono inoltre le forme di attivismo orientato da finalità politiche che possono incidere sull'attività delle istituzioni pubbliche.

Allo stesso tempo gli aspetti positivi legati all'utilizzo delle tecnologie ITC pongono problemi legati al digital divide e alla libertà di accesso alla rete internet. Libertà che viene posta in discussione tanto rispetto all'azione di controllo che la tecnologia permette ai poteri pubblici quanto rispetto ai rapporti tra utenti e grandi fruitori di servizi on line. Problemi questi che costituiscono aspetti diversi della più ampia questione della tutela della privacy delle persone. Tale problematica richiede di comprendere in che modo la pervasività delle tecnologie nella vita delle persone può portare alla realizzazione di strumenti tecnici suscettibili di determinare dall'esterno la libertà dell'individuo trasformandolo in un mero strumento per il perseguimento di fini determinati da grandi attori politici o economici.

4.4 Dual-Use.

La duplicità dei problemi legati alla tutela delle persone nel cyberspace è una caratteristica che può essere estesa anche alle infrastrutture e alle supply chain che basano il loro funzionamento sulle tecnologie ITC.

L'ulteriore carattere di tali tecnologie è infatti il loro essere intrinsecamente dual use. Le tecnologie ITC, data la loro integrazione e pervasività, sorreggono azioni volte al perseguimento dei fini più disparati rispetto ai quali è spesso difficile il confine tra ciò che è lecito e ciò che non lo è indipendentemente dagli effetti diretti che esse determinano.

È questo un carattere che rispecchia l'interdisciplinarietà che abbiamo visto esser la cifra di una cultura scientifica e più in generale di un'idea di progresso dell'uomo sviluppatasi a partire dai conflitti

mondiali del secolo scorso e che con l'affermarsi del processo di globalizzazione a acquisito un carattere universale.

Entro questa prospettiva si pone dunque il problema di delineare il limes dello sviluppo tecnologico determinando principi e valori in base ai quali orientare e governare lo sviluppo di tali tecnologie e dunque il progresso umano.

Il problema si pone, come evidenziato da Weiner ai cui studi si deve la fondazione della disciplina della cibernetica alla base della costruzione del cyberspace, in termini di *"uso umano dell'essere umano"*[104].

4.5 Anarchia.

In termini giuridici tale problematica attiene all'individuazione di principi e valori che possano delineare i confini degli interessi perseguiti attraverso l'utilizzo della informazione così come favorito dalle tecnologie ITC e di analisi e manipolazione dei dati.

La disciplina giuridica del cyberspace, tuttavia, risente dei caratteri precedentemente visti.

L'integrazione delle diverse tecnologie non permette la definizione di una disciplina giuridica unitaria favorendo viceversa la frammentazione dei soggetti regolatori e delle regole. Allo stesso tempo la pervasività e il carattere dual use delle tecnologie possono determinare l'esistenza di più regimi giuridici per una stessa fattispecie.

In questo contesto emerge l'ultima caratteristica del cyberspace, il suo essere uno spazio di interazione e un fattore di progresso rispetto al quale, tanto la dinamica degli attori che vi agiscono quanto il suo stesso sviluppo, avvengono in contesto sostanzialmente anarchico.

Sono gli stessi caratteri del cyberspace, così come l'idea di progresso che vi sottende, a determinare, da un lato, la difficolta a definire un quadro normativo unitario e, dall'altro, far emergere nuovi punti di frizione tra gli attori internazionali rispetto all'interpretazione di questo nuovo fenomeno e, di conseguenza, rispetto alla sua regolamentazione.

---

[104] N. WIENER, *Cybernetics, or control and communication in the animal and the machine*, prima edizione: The MIT Press, Cambridge (MA), 1948; seconda edizione: Wiley, New York, 1961 (trad. italiana: *La Cibernetica - Controllo e Comunicazione nell'animale e nella macchina*, Il Saggiatore, Milano, 1968)

Capitolo II

L'influenza del Cyberspace sulle relazioni internazionali.

Introduzione; 1. L'influenza dei caratteri del Cyberspace sui fattori delle relazioni internazionali; 1.1 Il Cyberpower; 1.2 La geopolitica nel cyberspace; 1.3 Strumenti e forme di esercizio della Potenza; 2. L'influenza dei caratteri del cyberspace sul progresso dell'Uomo; 2.1 Le innovazioni scientifiche e tecniche quali fattori economici; 2.2 Le problematiche economiche della società dell'informazione.

Introduzione.

A partire dalle osservazioni svolte sulle caratteristiche del Cyberspace, il presente capitolo si propone di osservare l'influenza che esse esercitano sul piano delle relazioni internazionali.

La prima parte intende rilevare l'influenza del progresso tecnologico sulle relazioni tra Stati. In particolare, verranno presi in considerazione l'emergere di nuovi fattori e strumenti della potenza e della geopolitica che orientano l'azione degli Stati.

Nella seconda parte viene presa in considerazione l'influenza che il progresso tecnologico esercita sulle dinamiche economiche e le principali problematiche che esso determina. Le innovazioni introdotte sul piano economico dal processo di affermazione del cyberspace trovano la loro rilevanza in quanto legate, da una parte, all'emergere di attori non statali e, dall'altra, in quanto si pongono alla base di problematiche sociali aventi natura globale.

1. *L'influenza dei caratteri del cyberspace sui fattori delle relazioni internazionali.*

I caratteri del cyberspace individuati nel primo capitolo possono essere sintetizzati riconducendo, tra gli elementi strutturali, la suddivisione del cyberspace nei livelli logico, sintattico, semantico e, tra gli elementi funzionali, l'interdipendenza e la pervasività delle tecnologie dai quali derivano i due ulteriori caratteri dell'istantaneità e della globalizzazione delle azioni.

Ciò determina in primo luogo un mutamento dei riferimenti spaziali rilevanti nei rapporti geopolitici. Alle caratteristiche fisiche e ai fattori geopolitici[105] degli spazi terrestri, marini, aerei e spaziali, vengono ad aggiungersi le caratteristiche e la collocazione delle infrastrutture tecnologiche che sorreggono il funzionamento del cyberspace[106] di cui ne diviene centrale il controllo e la sicurezza.

In secondo luogo, assumono rilevanza geopolitica le risorse logiche, ovvero i protocolli e i software di funzionamento delle tecnologie ITC che permettono la connessione tra i diversi elementi e i diversi settori del cyberspace, il cui controllo, in termini di progettazione e processi di standardizzazione, rappresenta uno dei fattori costituenti il Cyberpower.

Infine, diviene strumento di geopolitica il contenuto semantico, l'informazione che viene prodotta elaborata e trasmessa nel cyberspace, attraverso cui si può incidere sulla percezione che i diversi attori hanno della realtà e del contesto entro cui agiscono, così esercitando una delle forme del Cyberpower.

Sul piano funzionale, l'interdipendenza e la pervasività delle tecnologie ITC determinano, in primo luogo, il carattere complesso e globale delle azioni condotte nel cyberspace il cui design tecnico incide, inoltre, sulla dimensione temporale dei processi decisionali, politici, economici e militari, riducendoli sostanzialmente all'istantaneità.

Rilevano, in secondo luogo, l'apertura dello spazio cyber che ne permette la fruizione generalizzata moltiplicando il numero e la natura degli attori internazionali così come degli interessi perseguiti all'interno delle relazioni globali. Aspetti che determinano l'esponenziale aumento dei fattori rilevanti nei processi decisionali.

La funzionalità dual use delle tecnologie ITC è l'ulteriore carattere del cyberspace che determina all'interno delle relazioni internazionali la sostanziale sovrapposizione tra la dimensione civile e quella militare. Inoltre, differentemente dal passato, ove si aveva uno spin-off tecnologico dal militare al civile si registra attualmente un inverso fenomeno di spin-in per cui le tecnologie elaborate in ambito civile trovano applicazione in ambito militare[107]. Ciò determinando una

---

[105] CARLO JEAN, *Manuale di Geopolitica*, Laterza, 2006; dello stesso Autore, *Geopolitica del mondo contemporaneo*, Laterza, 2012; MARCO GIACONI, *Spazio e potere. Modelli di geopolitica*, FrancoAngeli, 2003

[106] LUIGI MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, Politica&Società, Il Mulino, 2018, vol. VII, p. 61-76

[107] CARLO JEAN e GIULIO TREMONTI, *Guerre stellari. Società ed economia nel cyberspazio*, Franco Angeli editore, Milano 2000, p. 7.

sempre maggiore importanza nelle relazioni tra Stati di attori privati operanti nei settori connessi alle tecnologie delle telecomunicazioni.

Infine, rileva il carattere anarchico del cyberspace espressione dell'idea di libertà nell'accesso e nella creazione e condivisione della conoscenza che ha sorretto lo sviluppo delle diverse tecnologie ed in particolare della rete Internet[108]. L'assenza di una disciplina giuridica definita, così come la pluralità di soggetti regolatori chiamati ad amministrare la pluralità delle attività interne al cyberspace, lascia ai diversi attori un margine di azione estremamente ampio, suscettibile di produrre punti di frizione e quindi di insicurezza, nei diversi settori in cui le nuove tecnologie trovano applicazione.

Nel complesso, dunque, il cyberspace si pone non solo come *"V dominio della conflittualità dopo terra, mare aria e spazio"*, come è stato definito nel 2010 dal Vice Segretario della Difesa americano, Wiliam J. Lynn III[109], bensì come fattore dinamico in grado di informare dei propri caratteri le relazioni all'interno della Comunità Internazionale.

Rispetto ad essa il cyberspace solleva alcune questioni in merito al mantenimento della sicurezza e della pace internazionali, affrontate nei successivi paragrafi, intorno alle quali si articolerà l'azione multilaterale delle Nazioni Unite, come descritto nel capitolo successivo.

Esse attengono, in primo luogo, alla definizione del concetto di Cyberpower, e dei soggetti che ne detengono l'esercizio, non più identificabili con i soli Stati.

In secondo luogo, si pone la questione dell'impatto del cyberspace sui criteri geopolitici e geostrategici che hanno finora informato i conflitti internazionali.

Tale questione è legata al successivo problema di delineare una definizione di guerra cibernetica e dei suoi strumenti, le armi cibernetiche e del processo decisionale legato ad un attacco cibernetico.

Le questioni indicate sono inoltre funzionali ad affrontare, nello sviluppo della tesi, la tematica dei cambiamenti che il cyberspace determina nella dottrina della guerra e nella disciplina giuridica della stessa.

---

[108] TIM BERNERS-LEE, *Weaving the web. The original ultimate destiny of the world wide web*, HarperCollins Publisher, New York, 2000

[109] WILLIAM J. LYNN III, *Defending e new domain. The Pentagon's cyber strategy*, Foreign Affairs, September/October 2010, p. 97

1.1 Il Cyberpower.

Il Cyberspace si presenta come un fattore delle relazioni internazionali affermatosi in tempi relativamente brevi e al contempo soggetto a continue evoluzioni in ragione della sua natura sostanzialmente artificiale. Ciò determina una generale difficoltà nel delineare, in questo nuovo dominio, i caratteri dei principali fattori sui quali poggiano le relazioni tra Stati.

Il problema si pone anzitutto con riferimento al concetto di *Potenza*, più precisamente di *Cyberpower*. Comunemente usato in diversi ambiti il concetto stesso di *"potere"* appare sfuggente e soggetto alla prospettiva di chi vi fa riferimento, così come al contesto in cui esso viene adoperato. In termini generali viene inteso come *"capacità, possibilità oggettiva di agire, di fare qualcosa"* o come *"capacità di influire sul comportamento altrui, di influenzarne le opinioni, le decisioni, le azioni, i pensieri"*[110].

Rispetto alle forme di esercizio del potere si distingue, lungo uno spettro che va dal comando al comportamento coattivo, tra hard power e soft power. Il primo consiste nella capacità di usare minacce o ricompense per indurre altre entità a fare ciò che altrimenti non farebbero, mentre il secondo è la capacità di raggiungere gli obiettivi attraverso l'attrazione piuttosto che la coercizione.

Tanto la possibilità quanto le modalità di esercizio del potere sono determinate dalla disponibilità di alcune risorse strategiche che vengono variamente individuate nelle strutture militari, nel territorio e nelle risorse naturali, nella popolazione, nelle dimensioni economiche e nella stabilità politica[111]. La misura del potere che gli attori possono esercitare è infine determinata dalla disponibilità delle risorse e della capacità nell'esercitare influenza su altri attori attraverso gli strumenti, definiti a partire dalla Pace di Westfalia[112], della diplomazia, della cultura, dell'economia e delle forze armate.

---

[110] Cfr. la voce POTERE in vocabolario Treccani, consultabile all'indirizzo web http://www.treccani.it/vocabolario/potere1 In termini più propriamente strategici tale concetto è stato variamente definito dagli studiosi della materia. Alcuni definiscono il potere come la capacità di un'entità (di solito uno stato) di influenzare il comportamento di altre entità in base ai propri obiettivi. Altri lo descrivono come la capacità di un attore di far fare ad un altro attore qualcosa che altrimenti non farebbe (A. ORGANSKI, *World Politics*, Knopf, New York, 1968)

[111] D. NOLTE, *How to compare regional powers: analytical concepts and research topics*, Rev. Int. Stud., 36 (4) (2010), pp. 881-901

[112] WOLFGANG REINHARD, *Storia del potere politico in Europa*, Il Mulino, 2001

Tuttavia, rispetto al contesto attuale è significativo notare, nella prospettiva della presente tesi, come il fattore culturale venga oggi declinato in termini di *"informational power"*[113].

Trasfuso nel contesto del cyberspace e delle relazioni che in esso si svolgono, il potere assume infatti caratteri più complessi che possono essere delineati, da una parte, sulla base delle definizioni che esso trova nei domini marittimo[114] e aereo, generalmente presi a riferimento nello studio del cyberspace e delle sue dinamiche; dall'altra, con riferimento alle teorie del potere elaborate dalla sociologia del Novecento.

Il concetto di potere marittimo viene ripreso nella principale definizione di Cyberpower secondo la quale l'esercizio del potere nello spazio informatico consiste nella capacità di utilizzare il cyberspazio

[113] Tale declinazione può essere ricondotta alla Direttiva del Presidente statunitense Carter del 1977 (Cfr documento NATIONAL SECURITY COUNCIL, Presidential Directive/NSC-18, U.S. National Strategy, The White House, Washington, DC, 1977, Homeland Security Digital Library, https://www.hsdl.org/?view&did=458946) con la quale si identificano nella tecnologia, nel sistema economico, nel sistema politico e militare, gli elementi che avrebbero permesso di affermare la potenza statunitense rispetto all'Unione Sovietica. Successivamente nel 1982 il presidente Reagan (Cfr documento NATIONAL SECURITY COUNCIL, National Security Decision Directive 32, U.S. National Security Strategy, The White House, Washington, DC, 1982, Homeland Security Digital Library, https://www.hsdl.org/?view&did=462986), stabiliva la necessità per la sicurezza nazionale di sviluppare e integrare una serie di strategie sulla base delle componenti del potere nazionale identificate nella diplomazia, nell'informazione, nel sistema economico e politico e nelle forze armate, costituenti il noto modello DIME (Diplomacy Information Military Economy) che costituisce il riferimento all'interno dell'attuale teoria del potere. Le direttive indicate vengono emanate entro il quadro strategico proprio della contrapposizione bipolare che caratterizza il secondo dopoguerra. In questo contesto la tecnologia ha rappresentato un fattore di profonda innovazione determinando l'emergere del dominio spaziale affianco ai tradizionali domini della conflittualità rappresentati da terra, mare e aria. Dominio spaziale caratterizzato proprio dalla sua funzionalità rispetto alla rilevazione e trasmissione delle informazioni attraverso strutture di tipo satellitare. Il ruolo della tecnologia è, in realtà, da sempre centrale nelle dinamiche evolutive dei conflitti, tuttavia è solo con l'affermarsi del cyberspace che determina mutamenti radicali nell'esercizio del potere, nei suoi fattori costituenti, nella manifestazione di potenza e di conseguenza nella condotta delle relazioni internazionali e, in ultimo, nella loro disciplina giuridica.

[114] Una definizione di potere marittimo è stata proposta da alcuni professori della U.S. Naval Accademy subito dopo la I° guerra mondiale. Secondo tale definizione, che si colloca sulla scia delle teorie dell'Ammiraglio Mahan, che per primo delineò i fattori che determinano la supremazia navale e le modalità con cui le autorità di governo possono sfruttarli, il potere marittimo consiste, nei suoi tratti generali, nella capacità di un attore di imporre la sua volontà sul mare. Allo stesso modo le prime elaborazioni del concetto di potere aereo non ne fornivano una definizione puntuale così che questo finiva per essere inteso come la capacità di agire nello spazio aereo. Le due prospettive indicate pongono l'accento sulla capacità degli attori di utilizzare e sfruttare per i propri scopi l'ambiente naturale.

per creare vantaggi e influenzare gli eventi in tutti gli ambienti operativi e attraverso gli strumenti del potere[115].

Allo stesso tempo, tuttavia, tale definizione amplia le precedenti nella misura in cui evidenzia il collegamento con le altre forme di potere politico, informazionale, militare ed economico (Diplomacy, Information, Military, Economy - DIME model) che caratterizza in via principale il Cyberpower. Entro questa prospettiva la potenza nel cyberspace diviene la misura dell'abilità degli attori di utilizzare l'ambiente informatico quale fattore funzionale ad incidere sui molteplici piani delle relazioni internazionali, la cui integrazione è determinata dai caratteri propri delle tecnologie dell'informazione e delle telecomunicazioni.

Per quanto riguarda le dinamiche in cui si sviluppa l'esercizio del Cyberpower, da parte tanto di attori statali quanto di attori non statali, queste possono essere osservate a partire dalle teorie del potere elaborate dalla sociologia della seconda metà del secolo scorso secondo cui il potere consiste: nella capacità di un attore di indurre un altro attore a fare ciò che non avrebbe voluto fare; nel precludere le scelte di un altro attore attraverso l'esclusione delle strategie di quest'ultimo, c.d. agenda control; infine nella capacità di un attore di determinare le preferenze di un altro agendo senza prendere in considerazione le strategie di quest'ultimo.

Nello svolgimento di tali azioni acquisiscono un ruolo centrale le caratteristiche proprie dell'ambiente cyber viste nel primo capitolo in quanto determinano le condizioni e le modalità, in altri termini le risorse e gli strumenti, per l'esercizio del potere stesso[116].

---

[115] DANIEL T. KUEHL, *From Cyberspace to Cyberpower: Defining the Problem*, in FRANKLIN D. KRAMER, STUART STARR, AND LARRY K. WENTZ, *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009), p. 38

[116] Come è stato osservato il potere dipende dal contesto, e il Cyberpower dipende dalla risorsa che caratterizza il dominio del cyberspazio. Rilevano qui, in primo luogo, la stratigrafia del cyberspace che, sulla base dei livelli fisico, logico e sintattico, permettono di individuare il contesto e gli strumenti di base delle diverse attività che si svolgono all'interno dello spazio informatico. Le dinamiche legate al livello fisico, ovvero alle infrastrutture del cyberspace, seguono sul piano economico i principi che regolano l'utilizzo di risorse rivali caratterizzate da costi marginali crescenti. Sul piano politico esse sono invece legate ai principi di sovranità e giurisdizione degli Stati. Diversamente i livelli logico e sintattico sono caratterizzati da guadagni marginali crescenti e sfuggono, al contempo, ad un efficace controllo giurisdizionale. Gli ulteriori caratteri del cyberspace, l'interconnessione e la pervasività, la plasticità e la vulnerabilità così come il principio di anarchia, influiscono anch'essi sull'articolazione e sull'esercizio del Cyberpower. Esso diviene il risultato dell'esercizio del controllo sui nodi strategici dei diversi strati del cyberspace influenzato da una distribuzione asimmetrica delle capacità tecniche a ciò atte così come dei vincoli giuridici. Le capacità tecniche a loro volta

Nel complesso le caratteristiche del cyberspace concorrono, come è stato osservato, ad una riduzione dei differenziali di potere tra i diversi attori, secondo uno schema di diffusione del potere tipico della politica globale di questo secolo che determina, in particolare, l'emergere di attori non statali. Allo stesso tempo, tuttavia, gli sviluppi tecnologici che costantemente modificano il cyberspace sembrano determinare un fenomeno di concentrazione del potere a favore degli attori, in primo luogo non statali, che riescono a determinare tali progressi. I dati e la capacità di elaborazione degli stessi sono stati indicati, nel primo capitolo, come gli elementi che determinano l'unitarietà del cyberspace qualificandolo come fattore di progresso della Società Umana. Ed è proprio l'acquisizione di tali capacità da parte di determinati soggetti privati che porta ad osservare un fenomeno di accentramento del potere, sicuramente economico anche se non ancora pienamente politico, in capo ai grandi operatori del settore dell'analisi dei Big Data e dei servizi informatici.

Entro questo quadro generale l'esercizio del potere, nella sua triplice sfumatura sopra indicata, si manifesta attraverso diverse tipologie di azione determinate dalle risorse e dagli strumenti di cui gli attori dispongono[117]. Attori che, inoltre, non coincidono più con le sole

---

sono determinate da una forte integrazione tra dimensione civile ed ambito militare a cui è legata, tra l'altro, la crescente attenzione, da una parte, ai profili della sicurezza nazionale e, dall'altra, alla tutela dei diritti umani e delle libertà fondamentali posti in discussione dalle sempre più ampie e pervasive attività di sorveglianza e intercettazione poste in essere per fini di natura securitaria. Vi è poi una correlazione diretta tra esercizio effettuale del potere e capacità di innovazione tecnologica esplicata in un contesto di rilevanti concentrazioni di potere di mercato e di competizione non concorrenziale associata ai bassi costi di ingresso che determinano l'emergere di rilevanti attori non statali. Un contesto in cui, infine, si registra un'estrema fragilità della dimensione multilaterale che lascia spazio all'affermazione, seppur limitata, di vincoli legislativi nazionali, caratterizzati da un alto grado di difformità, espressione di poteri esercitati in funzione cautelativa ed escludente rispetto alle azioni degli altri attori internazionali, in sostanziale contrasto con la natura globale e multilaterale del cyberspace e delle sue problematiche.

[117] Il potere, quale abilità di un attore di indurre altri a fare qualcosa contrario alle loro iniziali preferenze e strategie, può manifestarsi, nella forma di hard power, ad esempio, in un attacco DOS, come nel caso dell'Estonia e della Georgia (KENNET J. BOYTE, *A comparative analysis of the cyberattacks against Estonia, the United States, and Ukraine: Exemplifyng the evolution on internet-supported warfare*, International Journal of Cyberwarfare and Terrorism, Volume 7, Issue 2 april-June 2017). Altro esempio può essere rintracciato nell'azione volta a bloccare i messaggi di blogger dissidenti posta in essere ad esempio dal Governo cinese nei confronti di blogger dissidenti (ROBERTA MADDALENA, Un'altra bocca messa a tacere: il caso wu gan e la censura in Cina, ilcaffègeopolitico.org, 23/01/2018; ALESSANDRO IACUELLI, La censura cinese, Altrenotizie.org., 13/01/2006.). In termini di soft power, un individuo o un'organizzazione possono spingere altri a modificare i propri comportamenti come avviene nell'azione di proselitismo svolta da gruppi terroristici o nelle attività di profilazione a fini commerciali svolte

organizzazioni statali alle quali occorre affiancare le grandi imprese private del settore ITC, i gruppi privati e singoli privati volti al perseguimento dei fini più disparati, leciti e non, favoriti dal basso costo di accesso e uscita così come dall'anonimato che il cyberspace offre.

In conclusione, si può rilevare come la contrapposizione tra poteri che caratterizza le relazioni internazionali subisca nel contesto del cyberspace una particolare evoluzione che ne aumenta la complessità. Ciò in ragione dei bassi costi di ingresso nell'arena cyber, dell'anonimato e delle asimmetrie nella distribuzione del potere che permettono ad attori minori, statali e non, di esercitare azioni di hard power e di soft power più facilmente rispetto ai tradizionali domini politici. Si registra dunque un fenomeno di diffusione del potere che, tuttavia, non esclude la concentrazione dello stesso in capo ad attori maggiori, di natura statale e non, dotati di maggiori capacità di governo dei network di potere, ovvero dei legami tra i diversi settori ed elementi del cyberspace, così come dei diversi ambiti di manifestazione del potere sintetizzati nel modello DIME.

Infine, le diverse forme di manifestazione del potere impongono di valutare secondo nuovi paradigmi le azioni dei diversi attori al fine di definirne correttamente il valore giuridico.

Quest'ultimo può essere rilevato prendendo in considerazione una caratteristica che accomuna le diverse manifestazioni del Cyberpower e che consiste nella centralità che i dati hanno nelle attività informatiche e nel loro stretto legame con le persone e con la loro vita privata.

---

dai fornitori di servizi di social network o di e-commerce. La seconda espressione del potere, ovvero la capacità di determinare o frammentare le strategie di un altro attore assume i caratteri di hard power se tale azione non è accettata da quest'ultimo, diversamente assume i caratteri di soft power. L'azione volta a rendere difficoltosa la diffusione di materiale video on line nel 2010 durante l'anniversario della rivoluzione iraniana può essere indicato come esempio del primo tipo (NICOLO BRUNO, Iran, i Green in piazza. Mistero sulla foto di Neda, articolo pubblicato il 10/02/2010 su SkyTg24 consultabile all'indirizzo web https://tg24.sky.it/mondo/2010/02/10/iran_proteste_neda_foto_errore.html). Rientrano nella seconda tipologia i filtri che vengono posti alle comunicazioni on line, generalmente noti e accettati dagli utenti per ragioni di sicurezza, senza tuttavia che essi possano controllare la reale ampiezza e funzionalità di tali filtri. La terza manifestazione dell'esercizio del potere nel contesto cyber può manifestarsi nell'adozione, da parte di imprese tecnologiche, di protocolli e prodotti software che si impongono sulle strategie degli altri attori modificandole radicalmente. I governi possono delegittimare determinate idee, come nel caso del movimento religioso Falun Gong rispetto al quale il governo cinese impedisce la diffusione di informazioni impedendone la conoscenza tra i cittadini. Allo stesso modo i governi di Francia e Germania impediscono la diffusione di idee di matrice nazista su internet, mentre il governo degli stati uniti si preoccupa di limitare in vario modo i servizi di scommesse on line.

Entro questa prospettiva si comprende la centralità attribuita dai lavori svolti in seno alle Nazioni Unite ad alcuni particolari aspetti quali lo sviluppo di processi multistakeholder (volti a favorire la partecipazione di rilevanti attori privati nell'ambito dell'accademia, della ricerca scientifica e tecnica, dell'industria e del settore civile), e alla tutela del diritto alla vita privata e delle libertà di opinione, espressione e partecipazione politica che ad esso sono legate.

1.2 La geopolitica nel cyberspace.

I caratteri e le dinamiche del Cyberpower hanno un profondo impatto sulla politica internazionale incidendo sui classici riferimenti geografici ai quali si aggiungono ora le infrastrutture dello strato fisico del cyberspace quali punti di snodo fondamentali e, al contempo, vulnerabili ad attacchi malevoli tanto di natura cyber quanto cinetica. Inoltre, la militarizzazione del cyberspace determina il superamento del concetto di localizzazione della minaccia in ragione della de-territorializzazione del potere da cui derivano profonde modifiche nei concetti di luogo, tempo e spazio geografico.

La rilevanza geopolitica dei caratteri del cyberspace è, inoltre, legata all'intangibilità delle attività ivi svolte che determina sia una diffusione del potere a favore di attori minori sia l'accesso alle informazioni ad attori in precedenza soggetti alle censure degli Stati[118].

Sembra dunque, come è stato osservato, che lo sviluppo del cyberspace *"will tend to eliminate geopolitics through its influence on military security, rather than (or at Ieast in addition to) its influence on international politics"*[119].Una prospettiva questa che muove dall'impatto delle innovazioni tecnologiche sulle relazioni umane e che ricorre ad ogni nuovo progresso tecnico[120].

---

[118] Luigi MARTINO, *La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica*, CSSII – Centro studi Strategici, Internazionali e Imprenditoriali, 2012, consultabile https://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf

[119] MARTIN LIBICKI, *A debate on geopolitics. The emerging primacy of information*, Orbis Vol. 40, Issue 2, Spring 1996

[120] Già in passato McKinder indicava l'avvento della ferrovia come fattore determinante il potenziale dell'Heartland a danno delle Potenze marittime, allo stesso modo in cui De Seversky, negli anni Cinquanta, sosteneva che la nuova geopolitica del Potere aereo avrebbe eliminato i limiti geografici imposti alla strategia. Quanti sostengono l'effetto dirompente del cyberspace sulle forze armate e sulla strategia ritengono, in sintesi, sorpassate i criteri geopolitici elaborati

È tuttavia possibile osservare come le attuali tecnologie costituiscano strumenti in grado di sostituire i paradigmi tradizionali della geopolitica, spazio, posizione e distanza determinando nuovi schemi di interpretazione delle questioni geopolitiche[121] senza che l'era dell'informazione, pur comportando un sostanziale ridimensionamento del tempo e dello spazio, determini il superamento del valore del territorio[122]. Questo resta, infatti, il principale elemento di organizzazione delle relazioni umane e dell'azione militare. Ne consegue che il cyberspace rimane soggetto alle dinamiche di esercizio del potere proprie della politica internazionale[123] costituendone in definitiva un medium.

Centrale in questa prospettiva, come è stato osservato, è il *sense of location*[124] che caratterizza il livello fisico del cyberspace. Tanto le infrastrutture[125] quanto le imprese che operano nel settore ITC sono infatti fisicamente collocabili all'interno di giurisdizioni nazionali a cui sono soggette. Conseguentemente, la centralità e la parallela vulnerabilità agli attacchi di tali infrastrutture concorrono a trasporre sul piano geopolitico le dinamiche del cyberspace[126].

---

nei vari settori da Mahan, MacKinder, Spykman, Kissinger e Brzezinsky. Sulle diverse teorie geopolitiche si veda CARLO JEAN, *Manuale di geopolitica*, Editori Laterza, 2010.

[121] CARLO JEAN e GIULIO TREMONTI, *Guerre stellari. Società ed economia nel cyberspazio*, Franco Angeli editore, Milano 2000.

[122] UMBERTO GORI, *Cyberspazio e relazioni internazionali: implicazioni geopolitiche e geostrategiche*, in a cura di UMBERTO GORI E SERENA LISI, *Information Warfare 2012. Armi cibernetiche e processo decisionale*, Franco Angeli, Milano, 2013

[123] CARLO JEAN, *Geopolitica del XXI secolo*, Laterza, 2014

[124] DAVID CLARK, *Characterizing cyberspace: past, present and future*, MIT CSAIL, Version 1.2 of March 12, 2010

[125] Tra le infrastrutture ITC assumono una particolare rilevanza i data center, strutture di stoccaggio e elaborazione dei dati. La capacità di raccolta e di analisi dei big data costituiscono, come visto nel primo capitolo, uno degli elementi portanti lo sviluppo del cyberspace. L'acquisizione e lo sviluppo di tali capacità rappresentano dunque risorse di potere fondamentali. Risorse di natura informatica legate tuttavia, ad una dimensione territoriale determinata dalla loro collocazione entro il territorio, e l'ordinamento, di uno Stato.

[126] Un aspetto questo, messo in evidenza nella relazione sulla politica della sicurezza del 2010 redatta dai servizi di intelligence italiani nella quale si sottolinea che la minaccia *cyber "sebbene riferita al mondo intangibile del cyberspace, presenta ormai tratti di estrema concretezza. Il settore ITC ha infatti assunto negli anni un peso crescente per l'economia e la società, registrando una crescita esponenziale sia delle apparecchiature fisse e mobili che si connettono ora alla rete wireless, sia del volume e della sensibilità delle informazioni scambiate. Tale settore ha la peculiare caratteristica di costituire un'infrastruttura critica in sé e di rappresentare, il nervo portante delle altre infrastrutture critiche"* (Cfr. *Relazione al Parlamento sulla politica dell'informazione per la sicurezza 2010*, p. 30, consultabile all'indirizzo web https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html).

Il cyberspace, dunque, non rende privi di rilevanza i tradizionali criteri geopolitici. Ne muta piuttosto i fattori e vi affianca nuovi elementi quali appunto, tra gli altri, le infrastrutture ITC, i dati e la capacità di elaborarli. Si parla, da questo punto di vista di geopolitica dei dati espressione di una forma di potere più profonda e sottile consistente appunto nel controllo dei dati[127] o, più precisamente, nella capacità di estrapolare, immagazzinare, elaborare dati e comunicare le informazioni ottenute al fine di determinare nel ricevente, che sia uno Stato, una comunità o un singolo individuo, gli effetti desiderati.

Entro questa prospettiva si può osservare il ruolo dominante ricoperto dagli Stati Uniti dove risiede il maggior numero di data center. Ruolo che tuttavia è messo in discussione dall'emergere nel settore di operatori europei e soprattutto del mondo asiatico[128].

Essendo i dati raccolti, in primo luogo, anche se non esclusivamente, rispetto alle attività delle persone, la demografia muta la sua rilevanza nelle dinamiche di potere del cyberspace. All'alto tasso demografico dei paesi asiatici corrisponde una elevata quantità di dati e di conseguenza di possibilità di elaborazione e fruizione. In questa prospettiva le persone, i cittadini, divengono una risorsa geopolitica non più confinata alla dimensione economico-militare del potere ponendo, da tale prospettiva, nuove problematiche rispetto alla tutela dei diritti umani e delle libertà fondamentali.

In conclusione, lo sviluppo del cyberspace non rende di colpo obsoleti i tradizionali riferimenti geopolitici trasponendo il confronto di potenza entro uno spazio virtuale. La dimensione reale rimane centrale nell'esercizio della potenza. Di essa tuttavia, mutano, da una parte, le logiche di sviluppo, legate all'istantaneità e alla delocalizzazione degli eventi; dall'altra acquisiscono rilevanza nuovi elementi come le infrastrutture ITC che si affiancano, ad esempio, ai tradizionali colli di bottiglia del dominio marino, mentre altri fattori, quali quello demografico, acquisiscono un nuovo significato determinato dal ruolo che le persone rivestono all'interno del generale fenomeno della rivoluzione dell'Informazione e di affermazione di una Società della Conoscenza.

---

[127] F. VITALI, *La geopolitica economica dei dati e il futuro del dominio. Dal controllo alla previsione. Il potere tra social media e manipolazione dell'azione sociale*, in *Nomos & Khaos*. *Rapporto Nomisma 2011-2012 sulle prospettive economico-strategiche*, Osservatorio Scenari Strategici e di Sicurezza, Nomisma Spa, A.G.R.A., Roma, 2012, pp. 207-231

[128] FABIO RUGGE, *Confronting an "Axis of Cyberspace"? China, Iran, North Korea, Russia in Cyberspace*, ISPI, Ledizioni LediPublishing, Milano, 2018.

1.3 Strumenti e forme di esercizio della Potenza.

Conseguenza diretta dei mutamenti illustrati è l'evoluzione degli strumenti e delle forme di esercizio della forza. La rivoluzione dell'Informazione trova una sua espressione sul piano dei rapporti internazionali conflittuali nella militarizzazione del cyberspace, nello sviluppo di metodologie di cyberwarfare, così come nello sviluppo di strutture decisionali nazionali caratterizzate da un elevato grado di accentramento e di segretezza e, infine, nello sviluppo di armi tecnologicamente avanzate[129].

Sono questi, infatti, i principali aspetti dell'evoluzione dei conflitti determinati dai progressi tecnologici del cyberspace suscettibili di porre, sul piano del diritto, problematiche differenti in ragione dei fattori che singolarmente li caratterizzano. Come per la maggior parte degli elementi costituenti lo spazio informatico, l'incertezza resta il principale aspetto problematico.

Incertezza che si registra anzitutto riguardo il concetto di "guerra cibernetica" di cui non esiste una definizione condivisa in ragione, da un lato, della relativa novità rappresentata da questo campo di ricerca[130]

---

[129] Entrambe le tendenze indicate prendono avvio dalla ridefinizione delle dottrine militari operate dagli Stati Uniti attraverso "un continuum strategico di lungo respiro"129 che impegna le amministrazioni dei presidenti Clinton, Bush jr., e Obama, muovendo dall'analisi dei conflitti avvenuti nel periodo immediatamente successivo alla definizione del confronto bipolare.
In particolare, rileva la "Joint Vision 2010" del 1996 redatta dal Ministero della Difesa dove viene indicato l'obiettivo di rinnovare la conduzione di operazioni interforze facendo affidamento non sulla concentrazione delle forze e su una struttura sequenziale delle operazioni, ma realizzando la concentrazione degli effetti con altri mezzi resi disponibili dallo sviluppo della tecnologia e in particolare dalle novità introdotte dalla Information Technology. Queste sono alla base dell'elaborazione della teoria Network Centric Warfare, traducibile con guerra netcentrica o meglio digitalizzazione dello spazio di manovra. Il fulcro della teoria netcentrica risiede nell'interconnessione in rete di sensori, cioè elementi tecnici o umani che percepiscono e rilevano attività naturali e umane; decisori, cioè elementi che, sulla base delle informazioni disponibili, assumono una decisione e attuatori, cioè elementi che mettono in pratica la decisione, di solito si tratta di sistemi d'arma UAV e LAWS piuttosto che agenti umani. Tutti gli elementi sono integrati in un'unica struttura, per sfruttare sinergicamente informazioni e capacità operative allo scopo di conseguire effetti coerenti con gli obiettivi desiderati. Solo tramite il collegamento in rete e mediante la conseguente possibilità di accesso e condivisione delle informazioni si ottiene la conoscenza condivisa della situazione (Situational Awareness), vero moltiplicatore di forza. Una forza net centrica, di conseguenza, è in grado di operare in un'area geografica più ampia, con risorse quantitativamente inferiori e distribuite nello spazio, con maggiore precisione, portata e capacità di sopravvivenza, in modo sincronizzato e con un ciclo decisionale estremamente ridotto rispetto a una forza tradizionale, accrescendo proporzionalmente l'efficienza della propria azione e le probabilità di successo.
[130] In particolare, rispetto allo studio delle dinamiche conflittuali consolidatesi attraverso eventi di cui è ricca la storia dell'uomo

e, dall'altro, della confusione che si è generata rispetto alla classificazione dei singoli eventi cyber finora registrati.

È tuttavia possibile giungere all'individuazione di categorie e tipologie di conflitti cyber entro cui collocare i singoli accadimenti[131].

In particolare, si può evidenziare come la Information Warfare costituisca la categoria principale all'interno della quale la Cyber Warfare ne costituisce una sua manifestazione[132].

Il concetto di Information warfare trova applicazione nella dottrina NATO delle Information Operation[133] elaborate per rispondere alla crescente complessità delle relazioni internazionali, all'asimmetria dei conflitti moderni e all'affermarsi del cyberspace quale spazio di interazione internazionale in cui tali problemi acquisiscono un ulteriore grado di complessità.

In tale contesto alla persistenza delle minacce classiche derivanti dal terrorismo e dalle armi di distruzioni di massa si sono affiancati due fenomeni ulteriori. Da una parte, l'aumento della copertura mediatica dei fenomeni globali ha fatto sorgere l'aspettativa che le azioni volte alla tutela dell'ordine e della sicurezza internazionale siano condotte

---

[131] Martin C. Libicky, uno dei più accreditati esperti in materia distingue sette forme di Information Warfare, intesa come conflitto che coinvolge la protezione, la manipolazione, la degradazione e la negazione dell'informazione (MARTIN C. LIBICKI, *What is Information warfare?*, Center for Advanced Concepts and Tecnology Istitute for National Strategic Studies, National Defense University, August 1995). Queste vengono individuate nelle forme del: i) comand and control warfare attraverso cui colpire i centri decisionali, la testa, dell'avversario; ii) intelligence-based warfare il cui scopo è quello di progettare e proteggere i propri sistemi informatici e ingannare e inquinare quelli dell'avversario; iii) electronic warfare, basata sull'utilizzo di strumentazioni radio, elettroniche e di crittografia; iv) psychological warfare dove l'informazione è usata per modificare le opinioni e le percezioni di singoli soggetti ed opinioni pubbliche la cui rilevanza strategica risulta accresciuto nel contesto della società dell'informazione; v) hacker warfare volta ad attaccare computer, reti e sistemi di elaborazione dei dati; vi) economic information warfare che blocca o manipola informazioni ai fini di una supremazia economica; vii) cyberwarfare che *"costituisce la summa delle operazioni più avanzate con l'utilizzo delle più recenti tecnologie informatiche, satellitari, ecc."* (UMBERTO GORI e SERENA LISI, *Information Warfare 2012. Ari cibernetiche e processo decisionale*, Franco Angeli, Milano, 2013). Essa in particolare può essere divisa in difensiva, nell'accezione di difesa attiva, volta cioè a costruire e programmare i propri sistemi in modo che siano resistenti e resilienti rispetto agli attacchi subiti; e in offensiva, mirante a comprendere come i sistemi-bersaglio possano essere vulnerabili.

[132] A titolo di esempio si può indicare nell'attacco subito dall'Estonia condotto attraverso sistemi di Distributed Denial of Service (DDoS) un primo esempio di Information Warfare mentre un primo acclarato atto di Cyber warfare può essere individuato nell'attacco portato all'Iran attraverso il virus Stuxnet (NICOLAS FALLIERE, LIAM O MURCHU, ERIC CHIEN, *W32.Stuxnet Dossier Version 1.4*. Symantec Corporation, February 2011, 7 consultabile all'indirizzo web www.symantec.com).

[133] NATO *Allied Joint Doctrine For Information Operation*, AJP-3.10, Novembre 2009 cunsultabile all'indirirzzo web https://info.publicintelligence.net/NATO-IO.pdf

entro un quadro morale e giuridico sempre più vincolante. Dall'altro, la rivoluzione dell'informazione ha modificato la dinamica dei fenomeni e dei processi decisionali ponendo al centro la ricerca e l'elaborazione computerizzata delle informazioni funzionali all'adozione delle decisioni stesse.

In termini di esercizio del potere diviene dunque centrale il raggiungimento di un livello di superiorità rispetto alla capacità di informazione e di acquisizione e sfruttamento della conoscenza. Obiettivi questi che possono essere ottenuti attraverso mezzi letali a cui tuttavia si ricorre sempre meno preferendo il ricorso a mezzi non letali sulla base del principio del Effect-Based Approach che pone attenzione alle relazioni di causa effetto piuttosto che ai risultati degli attacchi diretti. Si tratta di un principio la cui operatività coinvolge ogni livello decisionale lungo tutto l'arco della conflittualità così come tutti i fattori sintetizzati nel modello DIME.

Entro questo paradigma le *InfoOps* sono definite come una funzione militare mirante a creare effetti desiderati sulla volontà, comprensione e capacità dell'avversario.

L'obiettivo di tali operazioni è dunque quello di influenzare la volontà, la cognizione, l'interpretazione della realtà da parte dell'avversario e, differentemente dal passato, solo in secondo luogo le *capabilities* che condizionano i processi decisionali della controparte.

Le tipologie di Information Warfare indicate in precedenza rientrano quasi tutte tra le Info Operations.

Se ne differenziano in parte le operazioni di Cyber Warfare. Queste sono strettamente legate allo sviluppo delle tecnologie ITC e possono essere descritte come un insieme di attività da parte di uno stato tese ad introdursi nei computer o nelle reti di un altro Stato al fine di danneggiare o bloccare gli uni e le altre. Attività che possono essere svolte, si ricorda, anche da attori non statali dotati di rilevanti risorse e capacità tecniche. Si tratta in via principale di attacchi di natura cyber contro infrastrutture critiche e sistemi militari o nel furto e nell'alterazione di dati aventi rilevanza politico ed economica. Il loro tratto distintivo consiste nella potenziale letalità o capacità distruttiva di cose e persone attraverso operazioni condotte attraverso lo spazio cyber.

L'ampia tipologia di azioni riconducibili alle generale categoria dell'Information Warfare si riflette nelle incertezze che caratterizzano la definizione di cyber war. Un termine che, come è stato notato *"is often inaccurately used as synonym for information operation: while*

the latter can occur both in times o peace and of war, the former refers exclusively to information operations occurring during peace time"[134].

Inoltre, ai fini del diritto internazionale, i termini *cyberwar*, *cyberwarfare*, *cyberhostilities* e *cyberconflict*, non hanno trovato una definizione formale in atti internazionali[135]. A livello convenzionale si registra nell'ambito della Shangai Cooperation Organization una definizione di information war secondo cui essa può essere definita *"as confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, and underminig political, economic and social systems, processes and resources, and undermining political, economic and social system, mass brainwashing to destabilize society and state, as well as forcing the state to take decisions in the interest of an opposing party"*[136]

Diversamente, appaiono particolarmente utili le ricostruzioni volte ad individuare i fattori che determinano la rilevanza di un attacco quale atto di guerra. In questa prospettiva diviene dunque centrale l'analisi strategico-situazionale del contesto in cui si sviluppa l'attacco cyber. Secondo lo studioso italiano Umberto Gori occorre individuare la fonte dell'attacco, ovvero valutare: i) se dietro l'attacco non ci sia uno Stato; ii) le conseguenze (tipo dei danni, quanto gravi, per quanto tempo); iii) la motivazione (ovvero se l'attacco risponde a logiche di realpolitik); iv) la complessità di pianificazione ed esecuzione[137].

Si tratta di una posizione, condivisa da altri studiosi[138] e, come vedremo, dal *Group of Governamental Expert* istituito dall'Assemblea Generale delle Nazioni Unite, che pone al centro la valutazione di alcuni fattori oggettivi quali: l'elemento razionale dell'attacco, l'obiettivo perseguito; l'elemento violento rappresentato dalla complessità e letalità che caratterizzano gli attacchi di natura militare; infine, l'elemento coercitivo, ovvero l'incisività rispetto al target individuato.

---

134 MICHAEL SCHMITT, *Computer network attack and the use of force in international law: thoughts on a normative framework*, Columbia Journal of Transnational Law, vol 37, 1999.

135 NILS MELZER, *Cyber operations and Jus in bello*, in, a cura di KERSTIN VIGNARD, *Confronting cyberconflict*, United Nations Institute for Disarmament Research, Disarmement Forum, four 2011

136 SHANGAI COOPERATION ORGANIZATION, *Annex I to the agreement between the governaments of the member states of Shangai Cooperation Organization on cooperation in the field of international information security*, 16 June 2009, una traduzione non ufficiale è reperibile all'indirizzo https://ccdcoe.org/organisations/sco/

137 UMBERTO GORI, *Information warfare 2012*, Franco Angeli Editore, milano, 2013 pag 23

138 P. CORNISH, D. LIVINGSTONE, D. CLEMENTE, C.YORKE, *On Cyber Warfare*. A Chatham House Report,2010.

Tali problematiche assumono un rilievo centrale entro le attuali relazioni internazionali in considerazione dei mutamenti che gli Stati apportano alle loro dottrine militari e difensive in ragione del potenziale bellico che caratterizza il cyberspace quale V dominio della conflittualità.

Entro questa prospettiva il cyberspace appare infatti uno spazio di interazione in cui è particolarmente rilevante la componente militare la quale presenta un duplice profilo. Da un lato si manifesta nell'affermazione di rinnovate dottrine di impiego della forza militare. Dall'altra essa determina la creazione di strutture decisionali ad hoc dotate di ampie competenze e spesso sottratte al controllo pubblico.

Inoltre, il carattere dual-use delle tecnologie ITC e lo spin-in con il settore militare determinano la sempre maggiore rilevanza dei nuovi attori privati. La loro affermazione è legata allo sviluppo di nuovi principi economici in grado di sorreggere il processo economico legato alla valorizzazione dei dati in quanto risorsa principale del cyberspace.

La dinamica economica che caratterizza il cyberspace costituisce l'oggetto dei successivi paragrafi.

2. *L'influenza dei caratteri del Cyberspace sul progresso dell'Uomo.*

Le innovazioni tecnologiche si pongono alla base dei momenti di più marcato progresso della società umana in ragione della loro capacità di implementare l'agire dell'uomo permettendogli di soddisfare antichi e fondamentali bisogni favorendo, inoltre, un processo di definizione di nuovi e vari interessi il cui soddisfacimento si pone alla base del mutare dei sistemi economici e sociali.

L'affermarsi delle tecnologie delle telecomunicazioni e con esse del cyberspace presentano, tuttavia, intensità e caratteri differenti rispetto ai precedenti momenti di innovazione tecnica in quanto in grado non solo di implementare l'agire dell'uomo ma di indirizzarlo verso il raggiungimento di scopi predeterminati.

Come è stato osservato *"siamo abituati a considerare le ITC come strumenti mediante i quali interagiamo con il mondo e tra noi. In realtà tali tecnologie sono divenute forze ambientali, antropologiche, sociali interpretative. Esse creano e forgiano la nostra realtà fisica e intellettuale, modificano la nostra comprensione, cambiano il modo in cui ci relazioniamo con gli altri e con noi stessi, aggiornano la nostra interpretazione del mondo e fanno tutto ciò in maniera pervasiva, profonda e incessante"*[139].

I fattori su cui poggia tale processo rivoluzionario legato ai progressi scientifici e tecnologici consistono nell'esponenziale aumento delle informazioni la cui rilevanza è correlata allo sviluppo di tecnologie informatiche le cui funzionalità ridefiniscono i caratteri dell'ambiente umano. Trova dunque affermazione un'ulteriore dimensione esperienziale dell'individuo, determinando, a sua volta una nuova prospettiva circa la comprensione che l'uomo ha di sé e del suo rapporto con il mondo. In termini generali è stato rilevato come la rivoluzione dell'informazione sia alla base di talune significative trasformazioni nella nostra storia (che diviene iperstoria), nel nostro ambiente (che diviene l'infosfera) e nello sviluppo dei nostri se (l'esperienza on life). Alla luce della quarta rivoluzione, inoltre, comprendiamo noi stessi come organismi informazionali tra altri organismi informazionali[140].

---

[139] LUCIANO FLORIDI, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Raffaele Cortina Editore, Milano, 2017, pag. IX

[140] LUCIANO FLORIDI, La rivoluzione dell'informazione, Codice Edizioni, Torino 2012

La rivoluzione dell'informazione si caratterizza dunque, per essere al contempo una rivoluzione scientifica e una rivoluzione tecnologica i cui effetti si riverberano sul piano economico, culturale, politico, militare influenzando i rapporti tra gli attori internazionali secondo schemi e modalità non ancora compiutamente definiti.

Entrambe le dimensioni rappresentano lo stato attuale del progresso raggiunto nell'età moderna. Al contempo costituiscono i fondamenti di un nuovo processo di sviluppo volto all'edificazione di una Società dell'Informazione. Come è stato osservato: *"until now the human race has undergone two great waves of change, each one largely obliterating earlier cultures or civilizations and replacing them with ways of life inconceivable to those who came before"*[141]. Al millenario processo di sviluppo della rivoluzione agricola è seguito l'impetuoso affermarsi della rivoluzione industriale che nell'arco di appena 300 anni trova compimento e nuovi caratteri nella Terza Ondata rivoluzionaria animata dal progresso scientifico e tecnologico.

Lungo il dipanarsi dei tre momenti, l'intensità con cui le innovazioni tecnologiche hanno inciso sul livello di vita dell'uomo è stata progressivamente maggiore a partire dall'affermarsi dell'era moderna. Il lento tasso di progresso che caratterizza i momenti precedenti è ricondotto dall'economista *John Maynard Keynes* a *"l'assenza vistosa di miglioramenti tecnici di rilievo, e la mancata accumulazione di capitale"*[142]

A partire dal XVI secolo, a cui l'Autore riconduce l'avvio di un processo di accumulazione secondo l'interesse composto, *"è incominciata, proseguendo con un crescendo ininterrotto nel XVIII secolo, la grande era delle invenzioni scientifiche e tecniche che, dall'inizio del secolo XIX, ha avuto sviluppi incredibili: carbone, vapore, elettricità, petrolio, acciaio, gomma, cotone, industrie chimiche, macchine automatiche e sistemi di produzione di massa, telegrafo, stampa, Newton, Darwin, Einstein e migliaia di altre cose e uomini troppo famosi e troppo noti per essere ricordati"*.

A tale processo è dovuto il sostanziale sviluppo del tenore di vita in Europa e negli Stati Uniti la cui rapidità tuttavia pone, sul piano economico, *"problemi di difficile soluzione"* quali, in primo luogo, la

---

[141] ALVIN TOFFLER, The Third Wave, William Morrow and Comp. inc., New York, 1980, p.26
[142] JOHN MAYNARD KEYNES, *Economic Possibilities four our Grandchildren*, Conferenza tenuta da Keynes a Madrid nel giugno del 1930. Ora nel nono volume dei suoi Collected Writings intitolato Essay in Persuasion, traduzione itliana, La fine del laissez faire ed altri scritti, Bollati Boringhieri, Torino 1991.

disoccupazione tecnologica dovuta alla scoperta di strumenti economizzatori di manodopera e alla conseguente necessità di trovare nuovi impieghi.

Un problema che in prospettiva, tuttavia, significa per l'Autore *"che l'umanità sta procedendo alla soluzione del suo problema economico"* verso il raggiungimento del *"momento in cui* [i bisogni assoluti] *risultano soddisfatti nel senso che preferiamo dedicare le restanti energie a scopi non economici"*.

Momento al quale viene ricondotto l'emergere del vero e costante problema dell'uomo: *"Come impiegare la sua libertà dalle cure economiche più pesanti, come impiegare il tempo libero che la scienza e l'interesse composto gli avranno guadagnato, per vivere bene, piacevolmente e con saggezza"*.

Affianco al controllo demografico e al mantenimento della pace e della sicurezza internazionali lo sviluppo di questa nuova e dirompente fase di progresso dell'uomo è infine determinata dai due ulteriori fattori della *"nostra volontà di affidare alla scienza la direzione delle questioni che sono di sua stretta pertinenza, e il tasso di accumulazione in quanto determinato dal margine fra produzione e consumo"*. Con l'ulteriore avvertenza che *"una volta conseguiti i primi tre punti il quarto verrà da sé"*.

I successivi eventi bellici che originarono in Europa negli anni sancirono il passaggio del potere economico e politico da Lombard Street a Wall Street[143]. Ed è proprio nel nuovo modello sociale ed economico espresso dagli Stati Uniti e affermato nell'ordine mondiale post-bellico che origina e trova alimento un'ulteriore momento di sviluppo dei sistemi produttivi ed economici. Influenzato dallo sviluppo delle tecnologie dell'informazione e della comunicazione tale momento di sviluppo si caratterizza per l'automazione del processo produttivo e la creazione di un mercato globale di beni capitali e idee.

Tale processo di innovazione tecnologica viene ricostruito in termini di Terza Ondata[144] e il suo momento iniziale viene comunemente ricondotto alla metà degli anni 50 quando si registra il sorpasso del numero dei lavoratori impiegati negli uffici e nei servizi rispetto al numero degli operai impiegati nella produzione industriale di tipo fordista. Nel decennio successivo i progressi scientifici resero disponibili prodotti medici per il controllo delle nascite mentre sul

[143] PAUL KENNEDY, *Il parlamento dell'uomo. Le Nazioni Unite e la ricerca di un governo mondiale*, Garzanti, 2007.
[144] ALVIN TOFFLER, The Third Wave, William Morrow and Company, inc., New York, 1980

piano tecnologico iniziano a diffondersi le macchine computazionali general pourpouse così come l'aviazione commerciale spinta dai nuovi motori a reazione che implementarono le potenzialità degli aeromobili. Queste e altre rilevanti innovazioni trovarono nell'ordine mondiale emerso dai conflitti bellici gli stimoli e le garanzie necessarie alla loro affermazione. Il processo di globalizzazione avviatosi nel dopoguerra trova un rinnovato slancio con la fine della contrapposizione bipolare che rese possibile l'estensione del principio universalistico anche alle organizzazioni internazionali di tipo economico fino ad allora informate al principio dell'esclusione di modelli economici non improntati al libero mercato.

2.1 Le innovazioni scientifiche e tecniche quali fattori economici.

Da un punto di vista prettamente economico, nel 1987 il noto *"Paradosso di Solow"* evidenziava come *"l'era dei computer poteva vedersi ovunque tranne che nelle statistiche sulla produttività"*. Tuttavia, lo sviluppo delle tecnologie ITC ha contribuito in maniera fondamentale all'accelerazione della crescita della produttività[145] registrata a partire dalla metà degli anni '90. Si tratta di un contributo secondo alcuni contingente che una volta esauritosi lascerà spazio ad una nuova fase di stagnazione[146]. Ciononostante, prevale l'idea che l'accelerazione del progresso tecnologico costituisca un processo esponenziale ormai irreversibile il cui momento di accelerazione, implementazione, viene collocato nei primi anni 2000[147]. Tale andamento viene ricondotto alla nota legge di Moore secondo la quale il numero dei transistor aumenta ogni due anni. Ad essa, tuttavia, segue un corollario, comunemente noto come Seconda Legge di Moore, secondo cui *"cresce in maniera esponenziale con il tempo anche l'investimento necessario per realizzare una fabbrica che produca una nuova tecnologia di microprocessori"*. Richiamando ancora le riflessioni di Keynes *"non sarebbe fuori luogo prendere in*

---

[145] VALERIO INTRALIGI, PAOLO NATICCHIONI, *Cambiamento tecnologico e mercato del lavoro: una survey*, Università degli Studi di Roma Tre.

[146] FERNALD J. G., *Productivity and potential output before, during and after the great recession*, NBER Working Paper No 20248, 2014.

[147] E. BRYNJOLFSSON, A. MCAFEE, *Race against the machine: how the digital revolution is accelerating innovation, driving productivity, and irreversibly trasforming employment nd the economy*, Digital Frontier Press, 2011; degli stessi Autori, *the second machine age: work, progress and prosperity in a time of brilliant technologies*, W. W. Northon & Co. Press, 2014

considerazione la possibilità di progressi anche superiori"[148], e tali sono quelli che ci si attende dallo sviluppo della Società dell'Informazione. Tali progressi sono tuttavia legati alla dinamica economica determinata dal rapporto tra i due fattori dei progressi scientifici e tecnologici rispetto alla produzione (prima legge di Moore) e del processo di accumulazione del capitale (seconda legge di Moore).

La pervasività del cyberspace informa dei suoi caratteri i sistemi produttivi determinandone un ulteriore sviluppo. Alla meccanizzazione dei processi industriali e alla produzione di massa fordista, segue la Terza Rivoluzione Industriale nella quale l'utilizzo delle tecnologie ITC ha portato all'automazione del processo produttivo.

Dal punto di vista dei sistemi produttivi, la fase attuale rappresenta la Quarta Rivoluzione la cui caratteristica principale piano industriale *"è costituita dalla connessione in rete intelligente dei prodotti e dei processi, della produzione industriale, della tecnologia di automazione, informazione e comunicazione, che consentirà di generare catene di creazione del valore industriale integrate"*[149].

In altri termini la rivoluzione dell'informazione determina lo sviluppo di un'economia basata su beni immateriali[150]. Nella dimensione immateriale i costi di produzione sono generalmente più bassi. Allo stesso tempo i costi marginali sono tendenti allo zero per le attività di riproduzione, archiviazione o immagazzinamento, e, infine, per le attività di trasferimento che avvengono istantaneamente. Allo stesso tempo l'attività di manipolazione è svolta dai computer e dalle macchine dalla quale deriva l'ulteriore caratteristica propria di tali sistemi di produzione rappresentata dall'assenza di vincoli derivanti dai turni di lavoro. Inoltre, i beni prodotti nell'economia immateriale presentano caratteri peculiari: non sono rivali, non sono escludibili, non deperiscono, sono tendenzialmente interconnessi. Infine, tale sistema di produzione presenta ricavi di tipo crescente. In questo contesto l'informazione costituisce al contempo i beni di input e i beni di output la cui riproduzione consente costi nulli. L'assenza di costi variabili

---

148 JOHN MAYNARD KEYNES, *Economic Possibilities four our Grandchildren*, Conferenza tenuta da Keynes a Madrid nel giugno del 1930. Ora nel nono volume dei suoi Collected Writings intitolato Essay in Persuasion, traduzione itliana, La fine del laissez faire ed altri scritti, Bollati Boringhieri, Torino 1991.

149 WOLFGANG SHROEDER, *La strategia tedesca per un'industria 4.0*, in, a cura di, ALBERTO CIPRIANI, ALESSIO GRAMOLATI, GIOVANNI MARI, *Il lavoro 4.0. La quarta Rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018, p. 697

150 STEFANO QUINTARELLI, *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Bollati Boringhieri, Torino 2019

determina, di conseguenza, l'accelerazione esponenziale della produzione di beni immateriali.

Tale sistema di produzione si pone alla base dei processi di creazione di ricchezza che informano la dinamica del cyberspace quale fattore di progresso della società. Un modello che acquista sempre più rilevanza a fronte di un processo di declino del sistema economico attuale. Rispetto ai sistemi produttivi attuali, volti alla trasformazione di materie prime in prodotti, l'economia immateriale trova la sua risorsa prima nei dati rilevati e sfruttati attraverso le tecnologie ITC.

Tuttavia, il carattere integrato proprio di tali tecnologie e la capacità di apprendimento computazionale che le caratterizza, sorreggono un'attività volta all'elaborazione sulla base dei dati rilevati di un nuovo contenuto informativo, di una nuova conoscenza che sorregga la definizione e la realizzazione, per il tramite della tecnologia, di effetti reali nella sostanziale totalità delle attività in cui l'uomo manifesta le sue attitudini.

La dinamica tratteggiata evidenzia un'ulteriore caratteristica del cyberspace. Come è stato notato il cyberspace produce ciò che consuma, ovvero i dati. La centralità da essi acquisita nel cyberspace caratterizza inoltre il processo di creazione della ricchezza su cui poggiano le attuali dinamiche del progresso. Occorre dunque considerare a fianco dei sistemi di produzione immateriale i meccanismi propri del capitalismo dell'informazione.

Tale processo di accumulazione del capitale muove dal contenuto informativo che è possibile estrapolare dai dati relativi alle interazioni degli utenti. È questa la materia prima che attraverso sistemi computazionali avanzati viene trasformata in prodotti informativi di tipo predittivo. Un surplus comportamentale che in parte contribuisce al miglioramento di prodotti e servizi e, in altra parte, fornisce ai sistemi computazionali la risorsa essenziale per il loro sviluppo e per la produzione di nuovi prodotti predittivi così alimentando la richiesta dei mercati specializzati. Tuttavia, le tecnologie della telecomunicazione permettono di informare la società dei caratteri del messaggio inviato. In altri termini, *"i processi automatizzati non solo conoscono i nostri comportamenti ma li formano"*[151] creando ulteriore ricchezza.

[151] SHOSHANA ZUBOF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, 2019, pag.18

2.2 Le problematiche economiche della società dell'informazione.

Quanto sopra permette di osservare come la dinamica del progresso della Società dell'Informazione sia determinata da un originale rapporto tra i sistemi di produzione e i sistemi di capitalizzazione. Una dinamica, ancora indefinita, che, tuttavia, presenta un marcato carattere asimmetrico nell'accesso e nella fruizione delle informazioni, dal quale derivano problematiche in ordine alla costruzione della stessa idea di dignità dell'uomo.

Entro il contesto del cyberspace, infatti, la persona costituisce nella sua dimensione datizzata la risorsa essenziale alla dinamica del progresso scientifico e tecnologico e, al contempo, l'oggetto dell'azione delle tecnologie dell'informazione.

Dal punto di vista economico le innovazioni introdotte nei sistemi produttivi e nelle dinamiche di creazione della ricchezza sembrano riproporre problematiche note legate alla disoccupazione tecnologica e alla concentrazione di ricchezza. Tuttavia, i peculiari caratteri del cyberspace ne mutano i termini e le dinamiche determinando nei domini sociali mutamenti sostanziali e incerti.

Sul piano della produzione occorre considerare l'impatto delle innovazioni tecnologiche sui livelli occupazionali, sulla composizione dell'occupazione, sui salari. Si ripropone, in altri termini, il problema dell'impatto negativo delle innovazioni tecnologiche sulla domanda di lavoro e i suoi caratteri. Un tema affrontato dalla scienza economica a partire dai due diversi paradigmi delle teorie della sostituzione e della compensazione[152]. Nonostante i dati storici permettano di associare ai progressi tecnici una dinamica di aumento della domanda di lavoro[153], i caratteri propri delle attuali innovazioni tecnologiche, mutando il rapporto di base tra la tecnologia e i lavoratori, esprimono risultati incerti rispetto ai quali occorre sviluppare nuove prospettive di analisi.

Differentemente dalla prima rivoluzione tecnologica, nella quale l'offerta di lavoro si riallocò in altri settori, e dalla seconda,

[152] La teoria della sostituzione sostiene che l'innovazione dei processi produttivi dovuto ai progressi tecnologici, aumentando la produttività del lavoro, riduca, ceteris paribus, la domanda di lavoro rispetto a quella di capitale necessario agli investimenti in tecnologia, in tal modo determinando una riduzione dei livelli di occupazione. La teoria della compensazione evidenzia il ruolo dei meccanismi di mercato in grado di neutralizzare l'effetto sostituzione. I principali mecanismi atraverso cui opera la compensazione l'innovazione del prodotto, la diminuzione dei prezzi e incrementi del reddito.

[153] VALERIO INTRALIGI, PAOLO NATICCHIONI, *Cambiamento tecnologico e mercato del lavoro: una survey*, Università degli Studi di Roma Tre.

caratterizzata da dinamiche di ricollocamento legate alle mansioni, uno scenario plausibile è che le tecnologie attuali e i loro sviluppi possano progressivamente ridurre la domanda di lavoro a zero nella maggior parte dei settori industriali indifferentemente dalle qualifiche del lavoratore[154]. Le innovazioni tecnologiche nel campo dei robot permettono a tali macchine di sostituire l'uomo in tutte le tipologie di lavoro, svolgendo le stesse mansioni con maggior produttività, precisione e qualità del prodotto ad un minor costo. Nei precedenti processi di sviluppo tecnologico tale dinamica non era possibile, né immaginabile.

Come è stato osservato: "*the old theoretical models were capable of taking into account the old process of technological progress, within which machine cooperate with humans in production and increase labor productivity. But these models are incapable of systematizing the new process of technological progress, within which robot can totally substitute for human worker, while neither cooperate with the other nor increase their productivity. In such a framework, mass unemployment, or even full unemployment, will be a realistic outcome"*[155].

Le parole di Keynes possono essere nuovamente richiamate per descrivere il processo di accumulazione del capitale nel contesto del cyberspace. L'economista inglese, nel suo testo qui utilizzato quale canovaccio per lo sviluppo dell'analisi, descrive il momento in cui il sistema economico garantirà alle persone il soddisfacimento dei bisogni essenziali sostenendo che *"gli indefessi, decisi creatori di ricchezza potranno portarvi tutti, al loro seguito, in seno all'abbondanza economica. Ma saranno solo coloro che sanno tenere viva, e portare a perfezione l'arte stessa della vita, e che non si vendono in cambio dei mezzi di vita, a poter godere dell'abbondanza, quando verrà"*.

Le due preposizioni descrivono i termini delle problematiche sottese alla dinamica economica del cyberspace rappresentate dall'accentramento delle ricchezze e dalla loro redistribuzione. Problematiche che, in termini generali, possono essere osservate

[154] DARRELL M. WEST, *What appens if robots take the job? The impact of emerging technologies on employment and pubblic policy*, Center for Technology Innovation at Brookings, Octtober 2015; in senso contrario BEN MILLER, ROBERT D. ATKINSON, *Are robot taking our jobs, or making them?*, ITIF – The Information Technology & Innovation Foundation, september 2013.
[155] FABIO D'ORLANDO, *Problem, solutions and new problems whit the third wave of technological unemployment*, CreaM Working Papers Series Nr. 2/2018.

attraverso le teorie della sociologia[156] e dell'economia[157] comportamentale in quanto volte ad organizzare la società e a massimizzare i profitti delle attività economiche. Teorie che trovano nelle attuali tecnologie utili strumenti per la loro applicazione e realizzazione.

Entrambi i termini del problema trovano fondamento nei dati e nella loro funzionalità.

La struttura e la dinamica del cyberspace così come il valore e la funzionalità dell'informazione sono state descritte nel capitolo iniziale. Sul piano economico il fattore rilevante è rappresentato dal processo di accentramento in un numero ristretto di attori, principalmente privati, della disponibilità dei fattori tecnici costituenti il cyberspace e la sua dinamica.

Gli indefessi creatori di ricchezza sono, nel contesto economico del cyberspace, coloro che dispongono della tecnologia e delle risorse economiche necessarie alle attività, da un lato, di rilevazione, memorizzazione ed elaborazione dei dati. Alle attività, dall'altro lato, necessarie allo sviluppo di prodotti e servizi per la persona.

Il fattore dinamico è qui costituito dalla produzione e dall'utilizzo di prodotti informativi di tipo predittivo[158].

Questi costituiscono la risorsa essenziale per lo sviluppo di servizi in grado di massimizzare i profitti incidendo sul contesto economico e relazionale delle persone attraverso attività, permesse dalle nuove

---

[156] BURRHUS FREDERIC SKINNER, *About Behaviorism*, Vintage Books, 1974, vedi, per una sintesi della teoria, GIUSEPPE MUCCIARELLI, *La psicologia nel sentiero contemporaneo*, G. D'Anna, Messina-Firenze, 1981, pagg. 60-68, secondo l'Autore, Skinner "*sostiene che il comportamento deve essere oggetto di una indagine scientifica che ne individui le cause. Dare una spiegazione del comportamento presupponendo che a provocarlo siano sentimenti, sensazioni, stati d'animo e, in genere, "eventi mentali", non può rispondere a criteri scientifici e oggettivi perché questi fattori non sono osservabili e non possono essere oggetto di verifica sperimentale. È necessario allora evitare il "mentalismo" e considerare solo i dati osservabili, dirigendo l'attenzione sul ruolo dell'ambiente. È questo il piano del "behaviorismo metodologico", il quale però ha lasciato aperto il problema della effettiva esistenza di processi mentali che non possono essere studiati oggettivamente ma che non per questo possono essere ignorati: il "behaviorismo radicale" di Skinner cerca di dare anche a questi eventi una spiegazione alternativa a quella mentalistica riconducendo anch'essi a "comportamenti" da porre in relazione con l'ambiente: Diverrà così possibile estendere anche a questi aspetti l'indagine sperimentale, il controllo e la previsione che sono propri della scienza.*

[157] RICHARD H. THALER, *Misbehaving. La nascita dell'economia comportamentale*, Giulio Einaudi Editore, Torino 2018,

[158] SHOSHANA ZUBOF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, 2019

tecnologie, di re-indirizzamento dei comportamenti e dei bisogni delle persone.

Tali prodotti, tuttavia, vengono creati a partire dai dati forniti o ricavati dalle persone che in tale dinamica sono relegate al duplice ruolo di fornitori di una risorsa essenziale, i dati grezzi, e fruitori di prodotti e servizi volti a influenzarne il contesto sociale e i comportamenti al fine di massimizzare i profitti economici.

Entro tale sistema, informato a peculiari principi economici dell'economia comportamentale sorretti dalle potenzialità offerte dal progresso tecnologico e scientifico, la distribuzione della ricchezza tende ad orientarsi a favore di quanti svolgono le attività produttive indicate.

Trattandosi di attività particolari, generalmente estranee alla funzione e alle capacità di attori aventi natura pubblica, emerge la sempre più ampia e pervasiva rilevanza acquisita dall'azione di un numero ristretto e qualificato di soggetti privati, la cui attività si fonda sulla capacità di sviluppare strumenti e prodotti informativi innovativi in pressoché tutti gli ambiti di attività delle persone.

Tale sistema economico favorisce un processo di redistribuzione della ricchezza complessivamente generata marcatamente orientato a favore di un élite di attori "tecnologici" determinando la progressiva irrilevanza della "classe media"[159].

Un processo che appare sorretto dallo sviluppo di un più ampio pensiero volto ad evidenziare da una parte la funzione pubblicistica dell'azione privata[160] e dall'altra, a ridefinire il concetto di proprietà[161].

---

[159] JARON LANIER, *La dignità ai tempi di internet. Per un'economia digitale equa*, Il Saggiatore, Milano 2014; JERRY KAPLAN, *Le persone non servono. Lavoro e ricchezza nell'epoca dell'Intelligenza Artificiale*, LUISS University Press, Roma, 2016

[160] ANDREA VENEZIANI, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, Rivista Italiana di Informatica e Diritto, Fascicolo 1-2020; GUNTHER TEUBNER, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Armando Editore, Roma, 2005

[161] THOMAS PIKETTY, *Capitale e ideologia*, La nave di Teseo editore, Milano, 2020

Capitolo III

Le Nazioni Unite e il processo di rilevazione e definizione delle problematiche del cyberspace

Introduzione; 1. I progressi della teleinformatica nel contesto della sicurezza internazionale; 1.1 I lavori del Group of Governamental Expert; 1.2 La rilevazione delle problematiche internazionali; 1.3 La ricognizione delle norme di comportamento responsabile degli Stati; 1.4 L'uso delle tecnologie ITC nei conflitti armati; 1.5 Problemi irrisolti rispetto all'applicazione del diritto internazionale; 1.6 Le iniziative avviate dall'Assemblea Generale nel 20018; 1.7 I sistemi d'arma letali autonomi nel quadro della Convenzione sugli Armamenti; 1.7.1 L'attività di rilevazione delle problematiche operata nell'Informal Meeting of Expert; 1.7.2 I lavori del Group of Governamental Expert; 1.7.3 Il Report del Gruppo di Esperti del 2019; 2. La sicurezza delle tecnologie della comunicazione; 2.1 L'azione di contrasto allo sfruttamento criminale delle tecnologie ITC; 2.2 Gli strumenti di contrasto alla criminalità informatica; 2.3 L'attività di rilevazione e precisazione del fenomeno criminale nel Cyberspace; 2.4 Sviluppo di una cultura globale della sicurezza informatica; 2.5 la sicurezza delle infrastrutture informatiche critiche; 2.6 Internet Governance Forum; 3. Promozione e tutela dei Diritti Umani nel cyberspace; 3.1 I primi rapporti tematici; 3.2 L'attività del Consiglio dei Diritti Umani delle Nazioni Unite.

Introduzione.

L'ampiezza e la complessità del lavoro volto alla comprensione e alla regolamentazione dei fenomeni connessi allo sviluppo del cyberspace, si impongono nelle relazioni internazionali a partire dai lavori della Cinquantatreesima Assemblea Generale delle Nazioni Unite tenutasi nel 1998.

La Risoluzione n° 53/70 già nella sua intitolazione, *"Les progrès de la téléinformatique dans le contexte de la sécurité internationale"*, pone in rilievo il rapporto tra il progresso tecnologico e la sicurezza e la pace internazionale delineato a partire dalla considerazione *"que le réalisations scientifiques et techniques pouvaient se preter à des applications civiles aussi bien que militaires etqu'il fallait poursuivre et encourager les progrés de la science et de la technique à des fin civiles"*.

I rilevanti progressi che, si riconosce, sono stati realizzati nell'ambito delle tecnologie dell'informazione, sembrano infatti offrire, nei loro sviluppi, *"de très vastes perspectives puor le progrès de la civilisation, la multiplication des possibilités de cooperation pour le bien commun de tous les Etats, le renforcement du potentiel créateur de l'Humanité et l'amelioration de la circulation de l'information dans*

la societè mondiale". Ciononostante, l'Assemblea Generale *"se déclarant préoccupée par le fait que la teleinformatique risque d'etre utilisée à des fins incompatibles avec le maintenement de la stabilité et de la sécurité internationales et de nuire à la securité des Etats"*. Conseguentemente viene rivolto un invito agli Stati membri a collaborare sul piano multilaterale all'esame delle problematiche e dei rischi emergenti comunicando al Segretario Generale i loro punti di vista e le loro osservazioni su una serie di questioni.

La Risoluzione 53/70 costituisce dunque il punto iniziale dell'azione finora condotta dell'Assemblea Generale volta ad affrontare le diverse problematiche emergenti nel cyberspace. Un'azione che si svilupperà entro i riferimenti fissati in questa prima risoluzione: la cooperazione tra stati a livello multilaterale, lo studio delle problematiche e delle possibilità di risoluzione e contrasto, la definizione di principi internazionali volti a determinare la sicurezza dello spazio informatico e delle relazioni internazionali.

Entro questo quadro generale l'Assemblea Generale orienterà i suoi lavori rispetto ad alcune tematiche principali declinandole nel tempo coerentemente all'evoluzione complessiva del cyberspace.

Il tema principale, fissato nella indicata risoluzione, relativo a *"Le progrès del la téléinformatique dans le contexte de la securité internazionale"* sarà oggetto costante dell'attenzione dell'Assemblea[162] ed intorno ad esso si svilupperanno da una parte, il dialogo tra gli Stati Membri e l'Assemblea Generale tramite il Segretario Generale delle Nazioni Unite e, dall'altro, il processo di analisi delle problematiche e di definizione di principi e norme internazionali svolto attraverso la costituzione nel tempo di sei Gruppi di esperti intergovernativi (Group of Governamental Expert – GGE) e recentemente di un Open-Ended Working Group.

Nell'ambito della tematica indicata presenta un particolare interesse la questione legata allo sviluppo di sistemi d'arma autonomi letali (Letal Autonomous Weapon Sistem - LAWS). Le problematiche sollevate dall'applicazione delle nuove tecnologie e dall'utilizzo dei peculiari sistemi di elaborazione informatica sviluppati nell'ambito dell'Intelligenza Artificiale, vengono affrontate nell'ambito della Convenzione promossa dalle Nazioni Unite nel 1982 sulla proibizione

[162] ASSEMBLEA GENERALE, *Risoluzioni* 53/70 del 1998; 54/49 del 1999; 55/28 del 2000; 56/19 del 2001; 57/53 del 2002; 58/32 del 2003; 59/61 del 2004; 60/45 del 2005; 61/54 del 2006; 62/17 del 2007; 63/37 del 2008; 64/25 del 2009; 65/41 del 2010; 66/24 del 2011; 67/27 del 2012; 68/243 del 2013; 69/28 del 2014; 70/237 del 2015; 73/27 e 73/266 del 2018.

o la limitazione dell'uso di alcune armi convenzionali che possono essere considerate dannose o avere effetti discriminatori (Convention on Certain Weapons – CCW). Le Alte Parti Contraenti della Convenzione sviluppano la loro azione, in un primo momento attraverso lo strumento degli Informa Meeting of Expert[163] e, successivamente, attraverso i Gruppi di Esperti a Intergovernativi[164] indicati dagli Stati Parti. La stessa attività delle Alte Parti Contraenti costituisce, come vedremo in seguito, un elemento di interesse rispetto alla composizione e articolazione del quadro istituzionale generale.

Sulla base della Risoluzione 55/28 del 2000, appartenente alla serie indicata, l'Assemblea Generale svilupperà un ulteriore indirizzo tematico relativo alla *"Lutte contre l'exploitation des tecnologies de l'information à des fin criminelles"*. Tale problematica sarà oggetto di risoluzione durante le sessioni dell'Assemblea Generale del 2000 e del 2001[165]. Con le successive risoluzioni del 2002 e del 2003[166] la tematica verrà declinata in termini di *"Creation of global culture of cybersecurity"*, per poi essere ulteriormente ampliato nel 2009[167] quando l'Assemblea Generale lo interpreta in termini di *"Creation d'une culture mondiale de la cybersécurité et evaluation des efforts nationaux visant à protegér les infrastructures essentielles"*.

Nell'ambito delle Nazione Unite una particolare attenzione è stata posta dall'Assemblea Generale e dal Consiglio per i Diritti Umani ai temi relativi alla promozione e alla tutela dei diritti e delle libertà fondamentali rispetto alle problematiche poste dagli sviluppi delle tecnologie delle telecomunicazioni e dell'informazione.

Un'attenzione che si è sviluppata con particolare intensità nell'ultimo decennio attraverso i report presentati dagli Special Rapporteur i cui lavori sono stati avviati o indirizzati dalle risoluzioni dei due organi. I confini della problematica dell'affermazione e della tutela dei diritti umani nel cyberspace iniziano a delinearsi nel corso del 2011 attraverso i due report presentati dallo Special Raporteur Frank la Rue[168]. I risultati di questo lavoro vengono ripresi dalla risoluzione 68/197 con la quale l'Assemblea Generale richiede all'Alto

---

163 CCW, INFORMAL MEETING OF EXPERT, *Documenti* CCW/MSP/2014/3; CCW/MSP/2015/3; CCW/CONF.V/2 del 2016

164 CCW, GROUP OF GOVERNAMENTAL EXPERT, *Report* CCW/GGE.1/2017/CRP.1; CCW/GGE.1/2018/3; CCW/GGE.1/2019/CRP.1/Rev.2

165 ASSEMBLEA GENERALE, *Risoluzioni* 55/63 del 2000; 56/199 del 2001*;*

166 ASSEMBLEA GENERALE, *Risoluzioni* 57/239 del 2002; 58/199 del 2003.

167 ASSEMBLEA GENERALE, *Risoluzione* 64/211 del 2009

168 CONSIGLIO DEI DIRITTI DELL'UOMO, *Documenti* A/HRC/17/27; A/69/290; A/HRC/23/40

Commissario per i Diritti Umani di sviluppare il tema della protezione e promozione del diritto alla privacy nel contesto della sorveglianza e dell'intercettazione delle comunicazioni digitali e della raccolta di dati personali sul territorio nazionale e all'estero[169].

Le conclusioni e le raccomandazioni elaborate nel report presentato all'Assemblea Generale confluiscono nella risoluzione 69/166, intitolata Le droit a la viè privèe à l'ère numerique, con la quale il Consiglio dei Diritti Umani viene incaricato di sviluppare lo studio delle questioni finora emerse.

La prima parte del suo lavoro muove dalla risoluzione A/HRC/RES/25, che il Consiglio adotta nel marzo del 2014, con la quale delinea il mandato dello Special Rapporteur David Kaye avente ad oggetto la promozione del diritto alla libertà di espressione il cui lavoro si articola in tre report[170] presentati al Consiglio dei Diritti Umani nel corso del triennio previsto dal mandato.

La seconda parte dell'attività si sviluppa a partire dalla risoluzione A/HRC/RES/28/16, adottata dal Consiglio nell'aprile del 2015, con la quale, dando seguito alla risoluzione 69/166 dell'Assemblea Generale, viene incaricato un ulteriore Special Rapporteur il cui mandato prevede una maggiore articolazione delle questioni da sviluppare. Il lavoro svolto confluisce in una serie di rapporti presentati annualmente sia al Consiglio dei Diritti Umani[171] sia all'Assemblea Generale[172].

Il quadro generale dell'azione delle Nazioni Unite, ed in particolare dell'attività condotta in seno all'Assemblea Generale e al Consiglio dei diritti umani, si presenta dunque particolarmente articolato.

Muovendo dall'analisi del rapporto tra i progressi tecnologici e la sicurezza internazionale, a cui si affianca la tematica dei sistemi d'arma LAWS sviluppata dalle Alte Parti Contraenti della Convenzione CCW, i due organi estendono la loro azione rispetto a due problematiche specifiche. Da una parte il contrasto alle attività criminali e terroristiche che verrà ampliato nel tempo nel più generale problema dello sviluppo di una cultura della sicurezza informatica che permetta di tutelare le infrastrutture essenziali che sorreggono lo sviluppo della società dell'informazione, tanto a livello nazionale quanto globale. Dall'altro,

---

[169] REPORT GGE A/HRC/27/37

[170] CONSIGLIO DEI DIRITTI DELL'UOMO, *Documenti* A/HRC/29/39; A/HRC/32/38; A/HRC/35/22

[171] CONSIGLIO DEI DIRITTI DELL'UOMO, *Documenti* A/HRC/31/64 (2016); A/HRC/34/60 (2017); A/HRC/3762 (2018)

[172] ASSEMBLEA GENERALE, *Documenti* A/71/368 (2016); A/72/43103(2017); A/73/45712 (2018)

la tutela dei diritti umani e delle libertà fondamentali rispetto ai mutamenti determinati dalle nuove tecnologie ed in particolare rispetto alle modalità di esercizio dei poteri pubblici e dell'influenza esercitata dai soggetti privati, che, ora più ampie e meno trasparenti, pongono in discussione l'effettività dei diritti umani e delle libertà fondamentali in particolare rispetto alla tutela del diritto alla vita privata.

1. I progressi della teleinformatica nel contesto della sicurezza internazionale.

La prima di tali aree tematiche, come detto, riguarda il rapporto tra il progresso tecnologico e la sicurezza internazionale, mentre l'azione di ricognizione dell'Assemblea Generale svolta in questo settore muove dalla Risoluzione 53/70 del 1998.

Azione che si conclude con le Risoluzioni 73/27 e 73/266 del 2018 che chiudono il percorso seguito formalizzandone i risultati e aprendo ad una nuova fase volta a rendere *"le processus de négociation de l'Organisation des Nation Unies sur la sécurité d'utilisation du numérique plus démocratique, inclusif et trasparent"* [173] coinvolgendo il settore privato, le organizzazioni non governative, le università così come le organizzazioni regionali[174] quali l'Unione Africana, l'Unione Europea, l'Organizzazione degli Stati Americani, l'OSCE e l'ASEAN.

La risoluzione 53/70 delinea i presupposti, le modalità e le finalità dell'azione delle Nazioni Unite e degli Stati Membri, richiamandosi alle metodologie e ai principi individuati nella Conferenza su la società dell'informazione tenutasi a Midrand (Sud Africa) nel 1996 per assicurare la realizzazione di un progresso tecnologico equo per tutti i membri della società internazionale e ai risultati e alle raccomandazioni formulate nella Conferenza ministeriale sul terrorismo tenutasi a Parigi nel 1996.

Tali riferimenti saranno costanti lungo tutta la serie delle raccomandazioni durante la quale vi si aggiungerà, a partire dalla successiva risoluzione 54/49 del 1999, il richiamo alla Conferenza sul tema *"Les progrès de la téléinformatique dans le contexte de la sécurité internationale"* organizzata a Ginevra nel 1999 dal Segretario Generale

[173] Cfr. ASSEMBLEA GENERALE, *Risoluzione* A/RES/73/27, par. 5
[174] Cfr. ASSEMBLEA GENERALE, *Risoluzione* A/RES/73/266, par. 4

delle Nazioni Unite e dall'Istituto di ricerca delle Nazioni Unite sul disarmo.

Le diverse risoluzioni indicate inoltre, contengono tutte un richiamo iniziale alle precedenti e ai contributi che gli Stati Membri hanno nel tempo fornito all'Assemblea tramite il Segretario Generale.

Questi, sulla base di tali risoluzioni, sono chiamati a fornire il proprio contributo, in primo luogo, per quanto riguarda la rilevazione dei problemi generali in materia di sicurezza dell'informazione e, in secondo luogo rispetto alla definizione dei concetti fondamentali in materia di sicurezza dell'informazione e in particolare riguardo le interferenze illecite nei sistemi informatici e il loro utilizzo a fini illeciti. Infine, gli Stati Membri sono invitati ad esprimersi in merito all'opportunità di elaborare dei principi internazionali suscettibili di rafforzare la sicurezza del sistema informatico mondiale e di contribuire a contrastare il terrorismo e la criminalità nel dominio informatico. A partire dalla risoluzione 60/45 del 2005 si aggiunge l'invito a comunicare le misure adottate a livello nazionale per garantire la sicurezza dell'informazione e le attività di cooperazione internazionale in questo settore.

Le risoluzioni relative al rapporto tra i progressi delle tecnologie di telecomunicazione e la sicurezza internazionale costituiscono in particolare, il fondamento del lavoro dei Gruppi Intergovernativi di Esperti (GGEs) che si sono susseguiti e ne delineano l'ampiezza e l'oggetto dei lavori.

1.1 I lavori del Group of Governmental Expert.

L'Assemblea Generale delle Nazioni Unite ha incaricato nel 2002 il Segretario Generale di istituire un Group of Governanmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of Interntional Security. Successivamente sono stati convenuti ulteriori cinque GGEs nel 2005, nel 2011, nel 2013, nel 2015 e l'ultimo, i cui lavori non sono ancora conclusi, nel 2018.

I diversi report presentati all'Assemblea Generale hanno contribuito, in termini generali, a definire l'agenda dei negoziati in materia di cyber security, lo sviluppo di competenze e fiducia tra gli Stati Membri e l'evoluzione del quadro politico della cooperazione multilaterale, in particolare riconoscendo in essa la centralità della

Carta delle Nazioni Unite, del diritto internazionale e della sovranità nazionale nelle questioni relative al cyberspace. Tuttavia, resta irrisolto il problema dell'esatta definizione di come le norme e i principi di diritto internazionale si applichino esattamente rispetto all'utilizzo delle tecnologie dell'informazione.

I documenti rilasciati dal GGE sono il risultato di complessi negoziati nei quali occorre bilanciare problematiche riconducibili ad alcuni argomenti centrali, quali il rapporto tra la libertà di espressione e le esigenze di sicurezza, la natura e la legittimità delle azioni poste in essere nel cyberspace e le tensioni tra i rilevanti interessi internazionali e i valori universali che i singoli problemi richiamano.

Un quadro generale delle tematiche fondamentali affrontate dal GGE è stato ricostruito durante i lavori di tre workshops di esperti organizzati nel 2016 dal UN Institute for Disarmament Research (UNIDIR) e dal Center for Strategic and International Studies (CSIS)[175]. Queste sono state individuate nell'applicabilità del diritto internazionale, nell'identificazione di nuove specifiche norme internazionali e nella definizione delle modalità di gestione degli strumenti cyber suscettibili di avere un'applicazione malevola.

L'oggetto e la durata dei lavori del GGE è tuttavia delineato dalle risoluzioni con le quali l'Assemblea Generale di volta in volta richiede al Segretario Generale di procedere allo studio di determinati problemi avvalendosi dell'ausilio di un gruppo di esperti intergovernativi del quale ne indica i criteri di composizione e i limiti del mandato precedentemente determinati attraverso negoziati e consultazioni, su aspetti politici e amministrativi, svolte in seno al Primo Comitato dell'Assemblea Generale.

Per quanto riguarda la composizione, tutti i GGE devono essere istituiti sulla base di un'equa distribuzione geografica mentre i cinque Membri Permanenti del Consiglio di Sicurezza vi mantengono sempre un rappresentante. Quest'ultimi sono generalmente indicati in ufficiali governativi dotati di specifiche competenze tanto sul piano diplomatico quanto su quello tecnico.

La composizione governativa comporta, in particolare, lo svolgimento di lavori in forma riservata. Non è infatti prevista la pubblicazione dei verbali degli incontri dei GGE ne la presenza di osservatori esterni al fine di favorire una discussione sincera che

[175] A cura di J. LEWIS, K. VIGNARD, *Report of the International Security Cyber Issues Workshop Series*, UNIDIR, Center for strategic and International Studies (CSIS).

diversamente, considerati i rilevanti interessi nazionali coinvolti, sarebbe preclusa con il rischio di impedire la formazione del consenso necessario per affrontare le problematiche di cui il GGE è investito[176].

Il mandato dei GEEs viene delineato, come detto, attraverso le risoluzioni dell'Assemblea Generale le quali, nel loro susseguirsi, recepiscono, da una parte, gli orientamenti espressi dagli Stati Membri in merito alle problematiche del cyberspace, dall'altra, individuano argomenti specifici in ragione della loro incidenza sulla sicurezza internazionale in un dato momento.

1.2 La rilevazione delle problematiche internazionali.

Il primo GGE è stato istituito nel 2003 sulla base della Risoluzione 58/32 con la quale l'Assemblea Generale chiedeva al Segretario Generale *"d'examiner la question des menaces qui existent ou pourraient exister dans le domaine de la sécurité de l'information ainsi que le mesures de coopération qui pourrient etre prise pour y parer, de procéder à une étude sur les principes internationaux susceptible de renforcer la sécurité des systèmes télématiques mondiaux"*[177] con l'ausilio di un gruppo di esperti governativi da istituirsi nel 2004.

Il rapporto del GGE presentato alla sessantesima sessione dell'Assemblea nel 2005 tuttavia, tenuto conto della complessità dei temi esaminati, non ha raggiunto il consenso sulle questioni discusse[178]. L'insuccesso non ha interrotto l'azione dell'Assemblea la quale contestualmente, con la Risoluzione 60/45, rinnova la richiesta al Segretario Generale di costituire un nuovo GGE nel 2009 avente il medesimo mandato del precedente.

Il secondo GGE continua lo studio dei rischi legati alle tecnologie ITC e delle possibili misure di cooperazione e, differentemente dal precedente, giunge alla redazione di un rapporto finale contenente una serie, seppur minimale, di rilievi e raccomandazioni[179].

---

[176] A cura di J. LEWIS, K. VIGNARD, *Report of the International Security Cyber Issues Workshop Series*, UNIDIR, Center for strategic and International Studies (CSIS), pag. 4 e ss.

[177] Cfr. ASSEMBLEA GENERALE, *Risoluzione* A/RES/58/32, par. 4; sul punto vedi anche *Risoluzioni* A/RES/56/19 e A/RES/57/53.

[178] Cfr. ASSEMBLEA GENERALE *Rapporto GGE* A/60/202

[179] Il rapporto presentato dal Segretario Generale nel 2010 riconosce, in primo luogo, l'incidenza che i rischi emergenti nel cyberspace possono avere sulle persone, sulle imprese e sugli Stati. Ciò viene ricondotto alla facilità di accesso alle tecnologie ITC, al loro intrinseco carattere dual-use, alla pluralità di finalità perseguibili tramite il loro utilizzo e, infine,

In particolare, il Rapporto rileva che *"il est de plus en plus souvent signalé que des Etats développent des techniques informatiques comme instruments de guerre et de reinseignement, ainsi que des fins politiques"*[180], sottolineando come i problemi dell'attribuzione e l'assenza di un valori condivisi che permettano di determinare quali comportamenti siano accettabili per gli Stati rischino di creare instabilità e confusione. Problemi su cui gravano inoltre, la disparità di sviluppo tecnologico e legislativo tra i vari paesi che, in ragione dell'interconnessione propria delle tecnologie ITC, determinano ripercussioni sulla Comunità Internazionale nel suo complesso[181].

Conseguentemente, il rapporto del GGE prende in considerazione, in terzo luogo, la necessità di sviluppare misure di cooperazione internazionale di cui ne viene evidenziata l'importanza affianco al coinvolgimento degli attori privati al fine di rafforzare la sicurezza delle ITC a livello mondiale con particolare attenzione ai paesi in via di sviluppo[182].

Sulla base di tali rilievi il Rapporto presenta, infine, alcune raccomandazioni, il cui contenuto è tuttavia mantenuto su un piano generico[183].

---

all'anonimato che esse garantiscono ai loro utilizzatori che possono essere sia attori Statali sia soggetti privati.
In secondo luogo evidenzia come tali tecnologie possano essere utilizzate da soggetti che perseguono finalità di natura terroristica e criminale (ASSEMBLEA GENERALE *Rapporto GGE* A/65/201).

[180] Cfr. ASSEMBLEA GENERALE *Rapporto GGE* A/65/201 par. 7

[181] Cfr. ASSEMBLEA GENERALE *Rapporto GGE* A/65/201 par. 11

[182] Dopo aver richiamato l'attività svolta dalle principali organizzazioni internazionali a carattere regionale, il rapporto indica l'opportunità di porre attenzione ai domini di interesse transnazionale che non sono legati alla sola criminalità poiché i rischi legati alla confusione determinata dalla divergenza di prospettive circa le norme internazionali volte a disciplinare l'utilizzazione delle tecnologie ITC da parte degli Stati, può compromettere la gestione delle crisi in caso di incidenti gravi (ASSEMBLEA GENERALE *Rapporto GGE* A/65/201 par. 14).

[183] In particolare si raccomanda: i) di proseguire il dialogo tra gli Stati volto a definire norme internazionali per ridurre i rischi collettivi e proteggere le infrastrutture; ii) di adottare misure di confiance, di stabilità e di riduzione dei rischi nei rapporti tra Stati; iii) di favorire lo scambio di informazioni tra Stati sulle legislazioni nazionali e le strategie di sicurezza delle ITC così come sui rischi, le tecnologie, le politiche e le best practices seguite dagli Stati; iv) di definire modalità d'aiuto ai paesi meno sviluppati dal punto di vista tecnologico; v) di mettere in evidenza la possibilità d'elaborare azioni e definizioni comuni sulla base della risoluzione 64/25 dell'Assemblea Generale. (ASSEMBLEA GENERALE *Rapporto GGE* A/65/201 par. 18)

1.3 La ricognizione delle norme di comportamento responsabile degli Stati.

Ciononostante, l'adozione del rapporto spinse l'Assemblea Generale alla costituzione di un terzo GGE con la Risoluzione A/RES/66/24 del 2011 con la quale definì un mandato più specifico chiedendo espressamente di procedere all'esame *"des règle ou principes de comportament responsable des Etat"*[184].

Ribadita la necessità di sviluppare la cooperazione internazionale e di coinvolgere gli attori civili per individuare misure che favoriscano la stabilità e la sicurezza del cyberspace, il Rapporto presentato dal GGE nel 2013, sottolinea la particolare importanza di quelle misure volte all'applicazione di norme, regole e principi per un comportamento responsabile da parte degli Stati, così come ad aumentare la trasparenza e a rafforzare la fiducia tra gli Stati e la loro capacità tecniche.

Rispetto alle prime, il GGE ritiene essenziale, in primo luogo, sviluppare, nel contesto delle Nazioni Unite e con riferimento all'attività di altre organizzazioni internazionali e regionali, un intesa sul diritto internazionale applicabile in materia di principi e norme di comportamento responsabile favorendo la partecipazione anche dei soggetti privati[185]. Prendendo i considerazione le osservazioni presentate dagli Stati Membri all'Assemblea Generale e il progetto di codice di condotta internazionale per la sicurezza dell'informazione elaborato dal Segretario Generale, il GGE ritiene che *"Le droit international et, en particulier, la Charte des Nations Unies sont applicables et essentiels au mantien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique, sur, pacifique et accessible"*[186]. Evidenzia inoltre che tali principi, in primo luogo il principio di sovranità debbano informare la politica degli Stati rispetto alle infrastrutture informatiche presenti sul loro territorio[187]. In particolare, il rispetto dei diritti dell'uomo e delle libertà fondamentali, enunciati dalla Dichiarazione Universale dei Diritti dell'Uomo e dagli altri strumenti internazionali, costituiscono, nella prospettiva del GGE, limiti all'azione che gli stati possono porre in essere in materia di

---

[184] Cfr. ASSEMBLEA GENERALE, *Risoluzione A/RES/66/24 par 4*

[185] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE A/68/98 del 2013* paragrafi da 11 a 15

[186] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE A/68/98 del 2013* par. 19

[187] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE* A/68/98 del 2013 par. 20, "La politique des Etats en matière informatique et leur compétence territoriale pour ce qui est des infrastructures informatiques présentes sur leur territoire relèvent de la souveraineté des Etats et des normes e principes internationaux qui en découlent".

sicurezza informatica[188]. Infine, si ribadisce che gli Stati sono tenuti da una parte, ad onorare le obbligazioni internazionali derivanti da illeciti che possono essere loro imputabili, dall'altro ad astenersi dall'utilizzare i loro agenti per commettere tali atti e garantire che attori non statali non utilizzino il loro territorio per fare uso illegale di strumenti informatici[189].

Rispetto alle necessità di aumentare la trasparenza e a rafforzare la fiducia tra gli Stati e la loro capacità tecniche, il GGE sviluppa alcune osservazioni cui gli Stati sono chiamati a far riferimento nell'elaborazione di tali norme[190].

Tali misure si ritiene possano contribuire all'acquisizione di esperienze e conoscenze utili per il continuo dei lavori in materia di sicurezza informatica i quali dovranno, tra gli altri aspetti, giungere alla definizione comune di *"comportamento responsabile degli stati nel dominio informatico"* e rafforzare ulteriormente la cooperazione internazionale.

La necessità di rafforzare la cooperazione internazionale, sotto l'egida delle Nazioni Unite e attraverso il lavoro di organizzazioni regionali e specializzate, è costantemente ribadita dal GGE il quale la ritiene un presupposto essenziale per la sicurezza dello spazio informatico.

---

[188] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE A/68/98 del 2013 paragrafo 21,* "Les action entreprise par les Etats pour assurer la sécurité informatique doivent se faire dans le respect des droits de l'homme et des libertés fondamentales énoncés dans la Declaration universelle des droits de l'homme et dans les autres instruments internationaux".

[189] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE* A/68/98 del 2013 par. 23 "Les Etats sont tenus d'honorer leurs obbligations internationals quant aux faits intentionalement illicites qui leur sont imputables. Ils s'interdisent d'utliser leurs agents pour commetre de tells actes et veillent à ce que des agents non étatiques n'utilisent pas leur territoire pour faire un usage illegal des outils informatique"

[190] In particolare, si ritiene necessario: sviluppare, a livello bilaterale e multilaterale, lo scambio di informazioni, a titolo facoltativo e nella misura determinata dagli Stati stessi, delle informazioni sulle strategie politiche nazionali, sulle metodologie seguite e sui processi decisionali. L'istituzione di strutture di concertazione, bilaterale, regionale o multilaterale, e lo svolgimento di attività di approfondimento e di esercitazione congiunta rispetto alle diverse problematiche. L'ottimizzazione dei canali di comunicazione esistenti e la creazione di nuovi adeguati a ricevere, analizzare e utilizzare le informazioni sugli incidenti informatici e predisporre risposte immediate, con riferimento, in particolare, agli incidenti che possono coinvolgere le infrastrutture informatici di controllo dei grandi sistemi industriali. Lo scambio di informazioni e il dialogo tra le strutture tecniche così come il potenziamento della cooperazione di polizia e giudiziaria (ASSEMBLEA GENERALE, *Rapporto GGE* A/68/98 del 2013 par. 26).

Cooperazione che tuttavia è determinata dallo sviluppo diffuso di capacità tecniche che, diversamente, mancano ad alcuni Stati in ragione del diverso livello di sviluppo tecnologico e che possono comunque determinare rischi per le infrastrutture ITC, globalmente diffuse e interconnesse.

Il GGE ritiene dunque che gli Stati, lavorando con le organizzazioni internazionali, con gli organismi delle Nazioni Unite e il settore privato, *"doivent déterminer les milleurs moyen de fournir une aide tecnique ou autre aux pays ayant besoin de renforcer leurs capacités en matière de sécurité informatique, notamment aux pays en développment"*[191]. A tal fine gli Stati sono invitati, con riferimento anche alla Risoluzione dell'Assemblea Generale 64/211, ad adottare alcune misure[192] volte a sostenere a livello bilaterale, regionale, multilaterale e internazionale, il rafforzamento della cooperazione di polizia e del quadro giuridico, delle capacità di intervento in caso di incidente, della formazione politica in materia informatica, della conoscenza incoraggiando le ricerche universitarie.

Si può rilevare dunque, come il rapporto presentato nel 2013 dal GGE, dopo aver rilevato l'importanza della cooperazione internazionale e dell'aiuto ai paesi in via di sviluppo, ponga al centro della discussione internazionale in materia di sicurezza del cyberspazio la necessità di individuare norme e principi internazionali per l'azione degli stati nel cyberspace.

In particolare, viene riconosciuta l'applicabilità dei principi e delle norme di diritto internazionale così come dei diritti umani e delle libertà fondamentali al dominio informatico.

Una posizione questa che recepisce le posizioni dei principali Stati Membri, Stati Uniti e Federazione Russa, e che trova un riscontro nell'attività di altre organizzazioni internazionali quali la NATO.

Allo stesso tempo esprime i dubbi espressi da altri Stati Membri, quali la Cina, nella misura in cui lascia irrisolto il problema centrale rappresentato dalla definizione delle modalità concrete in cui il diritto internazionale attuale deve essere interpretato e applicato rispetto alle peculiarità del cyberspace.

In altri termini, la questione si pone non tanto rispetto all'applicabilità del diritto internazionale attuale quanto rispetto al come applicarlo.

---

[191] Cfr. ASSEMBLEA GENERALE A/68/98 del 2013 par. 31
[192] Cfr. ASSEMBLEA GENERALE A/68/98 del 2013 par. 32

Questione che costituirà a partire da questo momento l'aspetto più rilevante della discussione internazionale in materia di sicurezza nel cyberspazio alla quale contribuiranno i lavori di due ulteriori GGE istituiti nel 2013 e nel 2015.

1.4 L'uso delle tecnologie ITC nei conflitti armati.

Con la Risoluzione 68/243 l'Assemblea Generale definiva il mandato del primo di due GGE da ultimo indicati.

Questi veniva investito del compito di continuare lo studio dei rischi emergenti nel dominio informatico, delle misure collettive che possono essere prese e delle norme e principi internazionali che possono trovare applicazione in questo contesto. La risoluzione inoltre ampliava l'oggetto dei lavori del GGE rispetto ai mandati precedenti includendovi *"l'examen des questions de l'utilisation des technologies de l'information et des communications dans les conflits et de l'applicabilité de droit international à l'utilisation de ces technologies par les Etats"*[193].

Il rapporto del GGE[194], presentato alla settantesima sessione dell'Assemblea Generale del 2015, da una parte, richiama e rinnova alcuni contenuti dei precedenti report, relativamente alla necessità di sviluppare la cooperazione internazionale ai diversi livelli, di determinare misure e azioni che rafforzino sia la fiducia tra gli attori, sia lo sviluppo delle competenze tecniche degli Stati, in particolare di quelli tecnologicamente meno avanzati[195].

Dall'altra approfondisce nettamente lo studio dei principi e delle norme internazionali applicabili nel cyberspace ponendo particolare attenzione alle questioni legate alla giurisdizione degli Stati sulle

---

[193] Cfr. ASSEMBLEA GENERALE, *Risoluzione A/RES/68/243* del 2013 par. 4

[194] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE*, A/70/174

[195] La cooperazione e l'assistenza internazionale in materia di sicurezza informatica e di sviluppo delle capacità tecniche sono ritenuti aspetti essenziali per la sicurezza dello spazio informatico in considerazione che i rischi e gli incidenti che vi si possono manifestare sfuggono alle capacità di gestione dei singoli stati, nonostante essi restino i primi responsabili della sicurezza nazionale e dei loro cittadini (Assemblea Generale, *Rapporto GGE A/70/174 del 2015* par. 19). Il GGE richiamati i precedenti rapporti del 2010 e del 2013, con i quali era stato raccomandato agli Stati di definire le modalità per sostenere lo sviluppo dei paesi tecnologicamente meno avanzati e le strategie, le azioni e le norme a ciò necessarie, procede ad una precisazione del contenuto e della funzione della cooperazione e dell'assistenza internazionale.

infrastrutture ICT collocate nei loro territori; ai principi di sovranità e non intervento negli affari interni di altri Stati; al rispetto dei diritti umani e delle libertà fondamentali.

Il report inoltre afferma che la Carta delle Nazioni Unite trova piena applicazione e che gli Stati hanno diritto di adottare misure di carattere interno che non siano confliggenti con essa e con il diritto internazionale. Prende in considerazione, infine, l'applicabilità dei principi di umanità, necessità, proporzionalità e distinzione oltre agli obblighi per gli Stati di non ricorrere ad esecutori per la commissione di azioni illecite e di assicurare che il loro territorio non sia usato per tali attività da attori non statali.

Il report si presenta dunque, più articolato rispetto ai precedenti in ciò rispecchiando i progressi finora realizzati nell'approfondimento delle principali questioni problematiche così come l'attenzione che l'Assemblea Generale e gli Stati Membri pongono rispetto agli sviluppi del cyberspace e della capacità di azioni dei diversi attori al suo interno.

Aspetti questi che si ritrovano nell'analisi puntuale delle tematiche indicate svolta dal GGE.

Sul piano della cooperazione internazionale le misure individuate non si risolvono nel mero trasferimento di conoscenze e competenze verso i paesi tecnologicamente meno avanzati trovando piena realizzazione nel quadro del più ampio lavoro svolto dalle Nazioni Unite. Esse costituiscono infatti un prolungamento dei rapporti e delle risoluzioni finora adottate ed in particolare della Risoluzione 64/211 dell'Assemblea Generale intitolata *"Création d'une culture mondiale de la cybersécurité et evaluation des efforts nationaux visant a protéger les infrastructures essentielles"*[196].

Entro questo quadro specifico il GGE ritiene che gli stati dovrebbero riflettere sull'adozione di una serie di misure volontarie puntualmente indicate nel rapporto[197].

---

[196] Cfr. ASSEMBLEA GENERALE, *Risoluzione A/RES/64/211*

[197] In base a tali indicazioni gli stati dovrebbero: contribuire a rafforzare i meccanismi di cooperazione attraverso le équipe nazionali di intervento informatico di emergenza e di altri organismi competenti; fornire assistenza e formazione volte a migliorare la sicurezza nell'utilizzo delle tecnologie ITC compresi gli aspetti relativi alle infrastrutture essenziali oltre che condividere le best practices legislative e amministrative; aiutare ad espandere l'accesso alle tecnologie ritenute essenziali per la sicurezza informatica; elaborare procedure di assistenza e intervento rapido; facilitare la cooperazione transfrontaliera rispetto ai problemi che possono verificarsi sulle infrastrutture transnazionali; attribuire alle diverse azioni congrue risorse economiche (Assemblea Generale, *Rapporto GGE A/70/174 del 2015* par. 21). Viene infine sottolineato l'importanza di elaborare le diverse attività tenendo conto degli aspetti culturali,

Le azioni di cooperazione e assistenza internazionale sono inoltre legate all'adozione di misure volte a sviluppare la fiducia nei rapporti internazionali favorendo la trasparenza, la prevedibilità e la stabilità nelle relazioni tra stati. Il rapporto del GGE da una parte richiama i principi direttivi per l'elaborazione di effettive misure di confiance adottati dalla Commissione sul disarmo nel 1988 e approvati per consenso dall'Assemblea Generale[198], dall'altra indica una serie di misure specifiche[199].

Una necessità, quella di giungere alla definizione di una prospettiva comune sulle problematiche del cyberspace, che appare ancor più essenziale rispetto alla definizione di norme regole e principi di comportamento responsabile degli Stati e dell'applicabilità del diritto internazionale all'utilizzo delle tecnologie ITC da parte degli Stati.

Sono questi i due aspetti che maggiormente caratterizzano il lavoro svolto dal GGE nel 2015.

Rispetto al primo tema, il rapporto risponde all'obiettivo di definire *"nouvelles normes facultatives et non contraignantes de comportament responsable des Etats"*[200] e di giungere a definire una visione comune sul tema al fine di rinforzare la stabilità e la sicurezza dell'ambiente

---

geografici, politici, economici o sociali che caratterizzano gli stati (Assemblea Generale, *Rapporto GGE A/70/174 del 2015* par. 22)

[198] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE A/RES/43/78 (punto H)*

[199] Tali misure sono: l'individuazione di punti di contatto appropriati a livello decisionale e tecnico per affrontare gli incidenti informatici; lo sviluppo di procedure di concertazione, bilaterale, regionale e multilaterale, per aumentare la fiducia nei rapporti e diminuire i rischi di incomprensione rispetto agli incidenti informatici; le azioni volte a favorire, a titolo volontario e nella misura ritenuta opportuna, la trasparenza e lo scambio di informazioni sui diversi aspetti delle minacce informatiche nazionali e transnazionali; la condivisione volontaria di osservazioni in merito ad aspetti tecnici, legali, amministrativi sulle categorie di infrastrutture critiche ritenute rilevanti per la sicurezza informatica. Misure queste che possono comprendere l'individuazione di specifici referenti istituzionali e di dispositivi di classificazione degli incidenti così come la definizione di procedure di concertazione e meccanismi tecnici, giuridici e diplomatici per rispondere alle domande legate alle tecnologie di informazione e comunicazione. Rispetto ai rapporti di cooperazione bilaterale, regionale e multilaterale, il GGE indica ulteriori misure volte a: rinforzare la cooperazione tecnica, giuridica e diplomatica all'interno degli organismi competenti attraverso lo scambio di personale, l'intervento in caso di incidenti o nell'attività di repressione di attività malevole oltre che incoraggiare i rapporti tra centri di ricerca e università; individuare dei responsabili per lo scambio di informazioni e l'assistenza; costituire équipe di intervento rapido e sviluppare le pratiche di cooperazione tra le stesse; dare seguito, nel rispetto della legislazione nazionale e del diritto internazionale, alle richieste di altri stati volte a indagare su azioni malevole legate ai sistemi informatici e di comunicazione(Assemblea Generale, *Rapporto GGE A/70/174* del 2015 par. 17). Il GGE sottolinea infine la necessità di definire una comune interpretazione su tali temi e di rafforzare a tal fine la cooperazione e il dialogo nel quadro delle Nazioni Unite e di altri fori internazionali. (Assemblea Generale, *Rapporto GGE A/70/174* del 2015 par. 18)

[200] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE A/70/174* del 2015 par. 9

informatico mondiale. Tale tipologia di norme non tende a limitare o a interdire le azioni che rispettano il diritto internazionale quanto, piuttosto, a tradurre le aspettative della comunità internazionale fissando regole di comportamento responsabile degli Stati che permettano alla comunità internazionale di valutare le attività poste in essere dagli Stati e le loro intenzioni[201]. Il GGE in particolare si prefigge di determinare quale area delle norme esistenti può essere oggetto di sviluppo al fine di renderle applicabili all'ambiente informatico, di incoraggiare una migliore accettazione delle norme e di precisare in quale settore può essere necessario elaborare ulteriori norme che tengano conto della complessità e della specificità delle tecnologie dell'informazione e della comunicazione[202].

---

[201] Cfr. ASSEMBLEA GENERALE, *Rapporto GGE A/70/174* del 2015 par. 10

[202] In tale prospettiva il rapporto (ASSEMBLEA GENERALE, *Rapporto* GGE A/70/174 par. 13), prendendo nota del codice di condotta internazionale per la sicurezza informatica presentato da alcuni Stati Membri (ASSEMBLEA GENERALE, D*ocumento A/69/723*. Codice di condotta internazionale per la sicurezza dell'informazione proposto dalla Cina dalla Federazione Russa dal Kazakhistan, dal Kighizistan, dall' Uzbekistan e dal Tagikistan), propone all'esame degli Stati specifiche raccomandazioni riguardanti norme, regole o principi non vincolanti in base alle quali gli Stati: dovranno cooperare all'elaborazione e all'applicazione dei misure volte ad accrescere la stabilità e la sicurezza dell'utilizzo delle ITC e a prevenire le pratiche informatiche giudicate nocive che possono compromettere la pace e la sicurezza internazionale; in caso di incidente informatico dovranno esaminare tutte le informazioni utili, compreso il contesto generale dell'evento, la difficoltà di attribuzione e la natura e l'ampiezza delle conseguenze dell'incidente; dovranno considerare il modo migliore di cooperare per lo scambio di informazioni, aiutarsi a vicenda, perseguire il terrorismo o l'uso criminale delle tecnologie dell'informazione e delle comunicazioni e applicare altre misure collettive per contrastare questi rischi. A questo proposito, gli Stati potrebbero dover determinare se devono essere sviluppate nuove misure. Gli Stati, allo stesso modo, dovranno: rispettare le risoluzioni del Consiglio dei diritti dell'uomo e dell'Assemblea Generale in materia di diritti dell'uomo e di libertà di espressione garantendo il pieno rispetto di tali diritti; prendere le misure appropriate per proteggere le loro infrastrutture essenziali tenendo conto delle risoluzioni dell'Assemblea Generale; rispondere alle domande di aiuto di un altro Stato volte a contrastare e indagare attività malevole perpetrate nei confronti di infrastrutture essenziali; garantire l'integrità della catena logistica e prevenire la proliferazione di tecniche e strumenti informatici malevoli, al fine di tutelare l'utilizzatore finale e aumentarne la fiducia rispetto alla sicurezza dei prodotti informatici; dovranno infine incoraggiare la segnalazione responsabile delle vulnerabilità dei computer e condividere informazioni pertinenti su come correggerle, al fine di limitare ed eventualmente eliminare i rischi per i sistemi ITC e le infrastrutture che li utilizzano. Gli Stati, inoltre, non dovranno: permettere consapevolmente che il loro territorio sia utilizzato per la commissione di fatti internazionalmente illeciti attraverso l'utilizzo di tecnologie ITC; condurre o sostenere consapevolmente attività di natura informatica contrarie agli obblighi internazionali e intenzionalmente volte a danneggiare un'infrastruttura essenziale per la fornitura di servizi pubblici o a comprometterne l'utilizzazione e il funzionamento. Gli Stati, infine, non dovrebbero condurre o sostenere consapevolmente attività volte a danneggiare i sistemi di informazione delle equipe di risposta alle emergenze di un altro Stato ne utilizzare le stesse per svolgere attività internazionalmente dannose.

Rispetto alla seconda tematica affrontata, l'applicabilità del diritto internazionale all'utilizzo delle tecnologie ITC, il rapporto muove dai risultati del GGE del 2013 il quale aveva affermato l'applicabilità della Carta delle Nazioni Unite e la sua essenzialità al fine di mantenere la pace e la stabilità internazionale così come per promuovere lo sviluppo di un ambiente informatico aperto, sicuro, stabile, accessibile e pacifico.

Tale affermazione viene rinnovata sottolineando l'importanza che ricoprono alcuni particolari principi quali: il principio di sovranità che, assieme alle norme e agli ulteriori principi che vi derivano, si applicano all'uso delle tecnologie ITC da parte degli Stati e alla loro giurisdizione territoriale sulle relative infrastrutture[203]. Vengono richiamati inoltre, i principi di risoluzione pacifica delle controversie e di non intervento negli affari interni di altri Stati così come il divieto di minaccia e uso della forza e il rispetto dei diritti umani e delle libertà fondamentali[204].

Il GGE, basandosi sui lavori dei precedenti gruppi oltre che sulla Carta delle Nazioni e sul mandato ad esso conferito dalla risoluzione 68/243 dell'Assemblea Generale, esprime il punto suo punto di vista rispetto all'applicabilità del diritto internazionale all'utilizzo delle tecnologie ITC da parte degli Stati.

Tuttavia, come sottolinea lo stesso rapporto[205], tali rilievi non chiariscono pienamente la questione restando in capo agli Stati il compito di determinare una visione comune in materia di diritto applicabile[206].

---

[203] Cfr. ASSEMBLEA GENERALE, *Rapporto* GGE A/70/174 par. 27

[204] Cfr. ASSEMBLEA GENERALE, *Rapporto* GGE A/70/174 par. 26

[205] Cfr. ASSEMBLEA GENERALE, *Rapporto* GGE A/70/174 par. 28 e 29

[206] Viene dunque affermato che: la competenza territoriale degli Stati si applica alle infrastrutture informatiche situate sul loro territorio; che l'utilizzo delle tecnologie ITC deve rispettare, tra gli altri, i principi di: sovranità, di risoluzione pacifica delle controversie e di non intervento negli affari interni di altri Stati. Inoltre gli obblighi esistenti ai sensi del diritto internazionale sono applicabili all'uso delle ITC da parte degli Stati i quali devono, infine, adempiere agli obblighi previsti dal diritto internazionale di rispettare e proteggere i diritti umani e le libertà fondamentali; Sottolineando le aspirazioni della comunità internazionale per l'uso pacifico delle ITC per il bene comune dell'umanità e ricordando che la Carta si applica nella sua interezza, il GGE osserva che gli Stati hanno un diritto implicito a adottare misure conformi al diritto internazionale e alla Carta delle Nazioni Unite, ritenendo comunque necessario che sul punto sia svolto un approfondimento. Particolarmente rilevante, per la sua specificità, è il richiamo che il GGE svolge in merito all'applicabilità dei principi di umanità, necessità, proporzionalità e differenziazione. Infine, nel rapporto si afferma che gli Stati non dovrebbero ricorrere ad agenti esecutori per commettere atti illeciti a livello internazionale tramite tecnologie ITC mentre dovrebbero garantire che gli attori non statali non utilizzino il proprio territorio per commettere tali atti. Essi sono infatti tenuti a ad adempiere ai propri obblighi internazionali in relazione ad atti internazionalmente illeciti. Sul punto il GGE

Il rapporto presentato dal GGE nel 2015 si conclude delineando una prospettiva per lo sviluppo delle successive azioni. Questa acquisisce rilevanza in ragione, da una parte, delle difficoltà registrate nel successivo GGE che hanno impedito l'adozione di un rapporto condiviso e, dall'altra, delle azioni delineate dall'Assemblea Generale con le ultime risoluzioni del 2018[207] che sembrano dar seguito alle indicazioni conclusive del report del GGE del 2015.

1.5 Problemi irrisolti rispetto all'applicazione del diritto internazionale.

L'ultimo GGE finora svolto è stato istituito nel dicembre del 2015 con la Risoluzione 70/237.

Con tale risoluzione l'Assemblea Generale fa propri i risultati del precedente GGE in particolare rispetto all'applicabilità del diritto internazionale, della Carta delle Nazioni Unite e alla definizione di una disciplina facoltativa e non vincolante sul comportamento responsabile degli Stati.

Allo stesso tempo domanda agli Stati Membri di ispirarsi al rapporto del 2015 per ciò che riguarda l'utilizzazione dell'informazione e delle tecnologie di comunicazione, e di continuare a promuovere a livello multilaterale l'esame dei diversi aspetti rilevanti per la sicurezza dello spazio informatico e della stabilità delle relazioni internazionali.

---

puntualizza che il segno che un'attività informatica è stata lanciata dal territorio o dall'infrastruttura informatica di uno Stato o ivi trova la sua origine, può essere di per sé insufficiente per imputare l'attività in questione a quello Stato; il Gruppo ritiene che le accuse di organizzazione e esecuzione di atti illeciti contro gli Stati dovrebbero essere motivate.

[207] Le risoluzioni del 2018, come vedremo successivamente, evidenziando la necessità di giungere, attraverso la cooperazione internazionale, alla definizione degli elementi fondamentali per garantire la pace e la sicurezza internazionale nell'utilizzo delle tecnologie dell'informazione e della comunicazione e riaffermando, al contempo, come la responsabilità di garantire un ambiente informatico sicuro e pacifico sia primariamente posta in capo agli Stati, rilevano l'importanza dei contributi che possono essere forniti da attori privati. Viene dunque proposto di delineare dei meccanismi di partecipazione del settore privato e delle migliori università e della società civile avvalendosi, ad esempio, del lavoro dell'Istituto per la ricerca sul disarmo delle Nazioni Unite. Quest'ultime, a cui viene attribuito un ruolo motrice del dialogo internazionale in materia, si ritiene potranno lanciare un dialogo internazionale che dia spazio al lavoro delle diverse organizzazioni internazionali e alle diverse istanze che emergono sul piano internazionale rispetto alle problematiche della sicurezza determinate dall'azione dei diversi attori nello spazio cyber.

Infine delinea il mandato di un nuovo GGE da istituirsi nel 2016 attribuendo ad esso il compito di continuare l'esame delle questioni già affrontate in precedenza ampliandolo allo studio *"de la manière dont le droit international s'applique à l'utilisation de l'informatique et des technologies des communications par les États"*.

Il Gruppo di Esperti è dunque chiamato ad affrontare la questione sostanziale lasciata irrisolta dai precedenti report relativa alla definizione del modo in cui le norme e principi di diritto internazionale possano trovare applicazione rispetto alle azioni poste in essere nel cyberspace.

Su tale aspetto, tuttavia, gli Stati Membri esprimono posizioni differenti che impediscono al GGE del 2016 di giungere alla definizione di un rapporto finale.

Nonostante l'assenza di verbali delle riunioni del GGE e del contenuto meramente procedurale proprio dei report su cui non si è formato un consenso tra gli Stati Membri partecipanti, la differenza tra le diverse visioni espresse può, in questo caso, essere desunta da alcune dichiarazioni rilasciate dagli Stati su alcuni temi specifici.

Come è stato rilevato[208], l'insuccesso del GGE sembra possa essere ricondotto alle posizioni assunte da Cuba, Cina e Federazione Russa relativamente all'interpretazione del concetto di self-defence.

Secondo quanto espresso dal rappresentante di Cuba in una dichiarazione[209] successiva ai lavori del GGE, il problema riguardava *"the pretension of some, reflected in paragraph 34 of the draft final report, to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs"*.

Tale formulazione contenuta nel draft report veniva intesa come un'inaccettabile tentativo di *"establish equivalence between the malicious use of ICTs and the concept of "armed attack", as provided for in Article 51 of the Charter, which attempts to justify the alleged applicability in this context of the right to self-defense"*.

---

[208] ANDERS HENRIKSEN, *The end of the road for the UN GGE process: The future regulation of cyberspace*, Journal of Cybersecurity, 2019, p. 1-9.

[209] Cfr. Declaration by MIGUEL RODRIGUE, representative of Cuba, at the final session of Group of Governamental Expert on Developments in the Field of Information and Telecommunications in the Context of International Security. New York, June 23, 2017, citata in ANDERS HENRIKSEN, *The end of the road for the UN GGE process: The future regulation of cyberspace*, cit., consultabbile all'indirizzo web https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

Inoltre ritiene che *"To establish as a precedent this dangerous reinterpretation of the norms of international law and the Charter of the United Nations would be a fatal blow to the collective security and peacekeeping architecture established in the Charter of the United Nations. The "Law of the Jungle" cannot be imposed, in which the interests of the most powerful States would always prevail to the detriment of the most vulnerable"*.

La dichiarazione del rappresentante di Cuba evidenzia un ulteriore punto di frizione tra le posizioni espresse dagli Stati Membri relative all'applicazione del diritto umanitario al contesto ITC ritenuta inaccettabile in quanto *"it would legitimize a scenario of war and military actions in the context of ICT"*.

Le obiezioni mosse da Cuba rispetto all'applicabilità delle norme internazionali sul diritto all'auto difesa sembrano contrastare con quanto previsto dal precedente GGE Report del 2015 nel quale, come visto, da una parte, era stata affermata l'applicabilità della Carta delle Nazioni Unite, dall'altra era stato riconosciuto il diritto degli Stati di adottare misure non confliggenti con il diritto internazionale e con la Carta delle Nazioni Unite di cui il diritto alla self-defence fa certamente parte.

Autodifesa cui, diversamente, fanno esplicito riferimento, le dichiarazioni del G20, del novembre 2015[210], e del G7 dell'aprile 2017[211].

Meno sorprendenti appaiono le obiezioni relative all'applicabilità del diritto umanitario rispetto all'azione degli Stati nel cyberspace.

Da una parte occorre infatti notare che nel Report del 2015 non vi è un esplicito riferimento all'applicabilità del diritto umanitario. Dall'altra rilevano le posizioni espresse da alcuni Stati Membri, in particolare la Cina, la quale sostiene una visione pacifista dell'utilizzo del cyberspace contrastando l'applicazione a tale dominio di un paradigma militare per l'interpretazione degli attacchi cyber nella convinzione che ciò determini l'intensificarsi di una corsa agli armamenti e della militarizzazione del cyberspace[212]. Ciò comporta,

[210]Cfr.G20 *Communique´ Antalya Summit, 15–16 November 2015*. https:// www.consilium.europa.eu/en/press/press-releases/2015/11/16/g20-sum mit-antalya-communique/

[211]Cfr.G7 *Declaration on Responsible States Behavior in Cyberspace*, Lucca, 11 April 2017. https://www.mofa.go.jp/files/000246367.pdf

[212] M. XINMIN, *Key issues and future development of international cyberspace law*, CQISS 2016; 2:119–33. Citato in ANDERS HENRIKSEN, *The end of the road for the UN GGE process: The future regulation of cyberspace*, Journal of Cybersecurity, 2019, 1-9

nella visione ufficiale della Cina che *"application of existing law of armed conflict to cyberspace requires further scrutiny"*[213].

Posizione non del tutto differente da quella espressa dall'International Committee of Red Cross (ICRC) in una dichiarazione rilasciata alle Nazioni Unite nel novembre del 2017 secondo cui, pur affermando l'applicabilità del diritto internazionale umanitario quale strumento e metodo volti a limitare le attività di warfare durante i conflitti bellici, ciò *"is no way condoning cyber warfare, nor is condoning th militarization of cyberspace"*[214].

Le differenti visioni registrate sui temi della self-defense e dell'applicazione del diritto internazionale umanitario sono espressione delle difficoltà di determinare una visione comune all'interno della Comunità Internazionale sulle modalità di applicazione del diritto internazionale e della Carta delle Nazioni Unite alla disciplina dell'azione degli attori nel cyberspace.

Il lavoro svolto dai diversi Gruppi di Esperti ha permesso di affermare l'applicabilità di tale insieme normativo lasciando tuttavia insoluta tale ulteriore questione la cui risoluzione richiederà lo sviluppo di un intenso lavoro di discussione sul piano multilaterale così come ai diversi livelli tecnici, regionali e bilaterali.

1.6 Le iniziative avviate dall'Assemblea Generale nel 2018.

In tale direzione, sul piano multilaterale, l'Assemblea Generale delle Nazioni Unite nella sua ultima sessione del 2018 ha predisposto l'avvio di particolari iniziative, alcune delle quali nel solco del lavoro svolto dai Gruppi di Esperti, altre volte ad aprire un nuovo percorso entro cui sviluppare la cooperazione multilaterale e che sembrano rispondere alle indicazioni conclusive del GGE Report del 2015.

Tra le prime si inserisce il conferimento, con la Risoluzione 73/266 del 22 dicembre 2018[215], di un nuovo mandato al Gruppo di Esperti per il triennio 2019-2021.

---

[213] K. MACAK, *From cyber norms to cyber rules: re-engaging states as lawmakers*, Leiden J Int L (published online 18 July 2017), citato in ANDERS HENRIKSEN, *The end of the road for the UN GGE process: The future regulation of cyberspace*, Journal of Cybersecurity, 2019, 1-9

[214] Cfr. ICRC, *Weapons: Statement of the ICRC to the United Nations, 2017*, cunsultabile all'indirizzo web https://www.icrc.org/en/document/weapons-statement-icrc-united-nations-unag-2017

[215] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/73/266

Con essa l'assemblea rinnova il mandato per la costituzione di un nuovo GGE costruito sulla base dei precedenti e con la specificazione del compito di procedere all'esame *"de la manière dont le droit international s'applique à l'utilisation des technologies de l'information et des communications par le Etats, en vue de définir une vision commune et de l'applique efficacement"*[216].

Inoltre, l'Ufficio per gli affari sul disarmo del Segretariato viene incaricato di collaborare, a nome dei membri del gruppo di esperti governativi, con le pertinenti organizzazioni regionali, tra cui l'Unione africana, l'Unione europea , l'Organizzazione degli Stati americani, l'Organizzazione per la sicurezza e la cooperazione in Europa e il Forum regionale dell'Associazione delle nazioni del Sud-Est asiatico, per tenere una serie di consultazioni su mandato del gruppo prima delle sue sessioni[217].

Infine, chiede al presidente del gruppo di esperti governativi di tenere due riunioni consultive aperte informali di due giorni ciascuna, in modo che tutti gli Stati membri possano partecipare al dibattito interattivo e condividere le loro opinioni. Opinioni, che saranno comunicate dal presidente al gruppo di esperti governativi per il suo esame[218].

Queste due ultime disposizioni incidono sulle procedure che informano il lavoro del Gruppo di Esperti determinando una maggiore apertura rispetto al passato rispecchiando in ciò le indicazioni conclusive del Report del 2015.

A tali indicazioni, volte a favorire una maggiore trasparenza, apertura e il coinvolgimento degli attori privati, della società civile e del mondo della ricerca e delle università, sembra rispondere in maniera più puntuale la seconda iniziativa avviata dall'Assemblea Generale nella sua ultima sessione.

Con la Risoluzione 73/27 del 2018 viene infatti dato avvio ad un ampio processo negoziale attraverso la creazione di un "Gruppo di lavoro a composizione non limitata" il cui scopo è di rendere tale processo *"plus déocratique, inclusif et trasparent"*[219].

Rispetto alle precedenti, tale risoluzione svolge una duplice funzione recependo, da una parte, i punti fondamentali finora fissati e,

[216] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/73/266 par. 3
[217] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/73/266 par. 4
[218] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/73/266 par. 5
[219] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/73/27 par. 5

dall'altra, delineando un'azione multilaterale più ampia nelle finalità perseguite così come negli attori coinvolti.

Sotto il primo profilo rileva anzitutto il richiamo iniziale non solo alla serie completa delle precedenti risoluzioni in materia di progresso delle tecnologie ITC e di sicurezza internazionale ma anche a due specifiche risoluzioni, la 36/103 del 1981 e la 43/78 H del 1988 attraverso le quali vengono richiamati il principio di non ingerenza e una serie di norme volte ad aumentare la fiducia nei rapporti interstatali[220]. Tale attenzione è determinata dalla rilevanza assunta dalle problematiche del cyberspace così come dai caratteri di quest'ultimo[221].

Sulla base di queste osservazioni l'Assemblea sottolinea il comune interesse di tutti gli Stati alla promozione e all'utilizzo della tecnologia informatica per fini pacifici e per il progresso dell'umanità e ad evitare l'insorgere di conflitti condotti attraverso l'utilizzo di tali tecnologie.

Conseguentemente viene affermato che le Nazioni Unite dovranno svolgere un ruolo di primo piano nella promozione del dialogo tra gli Stati Membri volto alla definizione di una posizione comune sulle questioni legate alla sicurezza informatica e all'utilizzo delle tecnologie ITC così come alla definizione di una comune interpretazione della disciplina giuridica applicabile e dei principi e regole per un comportamento responsabile degli Stati, incoraggiando gli sforzi regionali e favorendo le misure di trasparenza e diffusione dei progressi raggiunti. In quest'ultima prospettiva vengono singolarmente richiamati e riaffermati i principi, le norme e le regole internazionali per

[220] La prima contiene la *"Déclaration sur l'inadmissibilité de l'intervention et de l'ingérence dans les affaires intérieures des Etats"* mentre la seconda fa specifico riferimento ai *"Principes directeurs puor l'elaboration de mesures de confiance"*. Si tratta di richiami che non sono presenti nelle precedenti e che denotano l'intenzione dell'Assemblea Generale di avviare un percorso che sulla base delle analisi, valutazioni, osservazioni, proposte e affermazioni finora svolte, porti alla definizione di un consenso internazionale sulle diverse problematiche legate allo sviluppo e all'utilizzo delle tecnologie ITC da parte degli Stati nel loro agire all'interno del cyberspace.

[221] Nonostante siano riconosciti i considerevoli progressi fatti nella concezione e nell'utilizzo delle tecnologie ITC, e l'aspirazione della Comunità Internazionale ad un loro utilizzo pacifico per il progresso comune dell'umanità, l'Assemblea Generale, tenendo presente sia l'essenzialità per la sicurezza internazionale di rafforzare le capacità, in particolare dei paesi meno sviluppati, in materia di sicurezza informatica attraverso il rafforzamento della cooperazione e dell'aiuto tra Stati, sia la rilevanza dei rischi derivanti dal carattere dual-use delle tecnologie ITC, esprime la sua preoccupazione nel rilevare che "plusieurs États mettent au point des technologies numériques à des fins militaires et que la probabilité que ces technologies soient utilisées dans des conflits futurs entre États augmente"

un comportamento responsabili degli Stati elaborati nei rapporti del 2013 e del 2015, e già riaffermati nella Risoluzione 71/28.

L'Assemblea, infine, sottolinea l'importanza del rispetto dei diritti dell'uomo e delle libertà fondamentali oltre che della Carta delle Nazioni Unite e dei principi e norme internazionali rilevati nel Rapporto presentato dal Gruppo di Esperti Intergovernativo nel 2015. Gli Stati sono quindi chiamati a farvi riferimento nel loro agire, così come a continuare a fornire i loro contributi al Segretario e a sviluppare i rapporti multilaterali, favorendo, rispetto al passato il coinvolgimento del settore privato, della società civile e del mondo della ricerca e delle università.

La risoluzione 73/27 sintetizza dunque, i principali aspetti su cui finora si è determinata una visione comune tra gli Stati Membri ponendoli a fondamento di un nuovo percorso.

Il processo negoziale, a cui tale risoluzione da avvio conferendo il mandato ad un Gruppo di lavoro a composizione non limitata, intende rispondere alle questioni finora delineate, e tuttavia irrisolte, anche attraverso l'attribuzione di un ruolo e di un valore ad attori ed istanze non statali, il cui apporto si ritiene possa contribuire a superare le differenze tra le prospettive espresse dagli Stati Membri durante i lavori dei precedenti gruppi di esperti intergovernativi.

A tal fine il Gruppo di Lavoro viene incaricato di studiare la possibilità di stabilire il più ampio dialogo istituzionale regolare sotto l'egida delle Nazioni Unite e di considerare, nei suoi lavori e nell'ambito dei contributi disponibili, la possibilità di tenere riunioni consultive intersessionali con attori privati quali le imprese, le organizzazioni non governative e la comunità accademica, al fine condividere le rispettive opinioni in merito alle diverse questioni che rientrano nel mandato.

Quest'ultimo prevede gli ulteriori incarichi di: approfondire la discussione relativa al modo in cui il diritto internazionale si applica all'utilizzo della tecnologia da parte degli Stati; di proseguire l'elaborazione dei principi e delle norme di comportamento responsabile degli Stati[222] e delle misure volte a rafforzare la fiducia[223], individuandone le modalità di applicazione apportando modifiche o stabilendone di nuove; di continuare a esaminare i rischi attuali o che

[222] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/73/27 par. 1
[223] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/73/27 par. 3

possono insorgere nel campo della sicurezza digitale e le misure che possono essere adottate per affrontarli;

I risultati e le implicazioni dell'avvio di questa nuova fase potranno essere valutati successivamente alla presentazione del report prevista per il 2020, nel corso della settantacinquesima sessione dell'Assemblea Generale.

1.7 I sistemi d'arma letali autonomi nel quadro della Convenzione sugli Armamenti.

La descritta attività svolta nell'ambito delle Nazioni Unite pone attenzione alle dinamiche relazionali tra gli attori internazionali al fine di delinearne i limiti in funzione dei mutamenti e delle problematiche determinate dall'affermarsi di un nuovo e peculiare fattore delle relazioni internazionali.

Nei successivi paragrafi l'attenzione verrà posta all'azione multilaterale volta ad affrontare le problematiche che il progresso tecnologico solleva rispetto agli strumenti attraverso cui agiscono gli attori del cyberspace. Tra la pluralità delle questioni emergenti in materia, l'interesse principale si è posto rispetto alla regolamentazione dell'uso di sistemi d'arma letali autonomi (Lethal Autonomous Weapons Sistems – LAWS).

L'azione multilaterale di rilevazione delle problematiche e degli strumenti giuridici inerenti il settore degli armamenti, trova la sede entro cui svolgersi nel sistema della Convenzione del 1980 sulla proibizione o la limitazione dell'uso di alcune armi convenzionali che possono essere considerate dannose o aventi effetti discriminanti (CCW – Convention on Certain Weapons).

Le Alte Parti Contraenti la Convenzione CCW hanno sostenuto la realizzazione di diverse iniziative volte all'approfondimento delle relazioni tra armamenti autonomi e la disciplina giuridica posta dalla Convenzione CCW. A partire dal 2013 e fino al 2016, la discussione si è svolta attraverso i lavori di Informal Meeting of Expert chiamati a sviluppare il dibattito in merito alle questioni correlate alle teconologie emergenti nell'area dei sistemi d'arma letali autonomi in relazione agli obiettivi e agli scopi della Convenzione CCW.

1.7.1 La ricognizione delle problematiche svolta dal Gruppo di Esperti Informale.

Nella Riunione tenuta a Ginevra nel 2013[224] è stato definito il mandato del primo di tali gruppi di esperti individuando i temi in merito ai quali raccogliere le diverse posizione dei partecipanti rispetto alle problematiche emergenti, declinate secondo le diverse prospettive tecniche, etiche e sociologiche, giuridiche e militari[225].

Nel dettaglio, la discussione tecnica ha preso in considerazione le questioni legate, in primo luogo, alla nozione di autonomia. Rispetto ad essa è stata evidenziata l'esistenza di differenti gradazioni determinate dal diverso livello di controllo esercitato dall'uomo sul sistema informatico dell'arma. Viene rilevata, in secondo luogo, la necessità di approfondire la fondamentale nozione di controllo umano così come di definire una serie di criteri oggettivi per determinare il livello di autonomia degli armamenti. Infine, considerata la natura dual-use delle tecnologiche adottate nei sistemi d'arma autonomi, si sottolinea la necessità di non incidere negativamente sulla loro applicazione nel dominio civile. In generale viene comunque rilevata la necessità di approfondire l'analisi delle tematiche data la novità della materia e lo stato delle attuali tecnologie in rapido sviluppo.

Aspetti quest'ultimi che hanno informato anche le discussioni di natura etica e sociologica.

Da questo punto di vista è stato posto in luce come le attuali tecnologie agiscano ancora sulla base delle istruzioni fornite alla macchina dall'operatore ponendo in discussione la possibilità per un sistema robotico di acquisire le capacità di ragionamento morale e di valutazione operativa e militare. Rispetto a tali capacità sono state sottolineate le difficoltà di natura etiche in particolare riguardo alla possibilità per i sistemi d'arma letali autonomi di eguagliare il giudizio umano, fattore che si pone alla base del rispetto dei principi di diritto internazionale umanitario. Al riguardo si è posto il problema di integrare la logica che informa i sistemi robotizzati con i valori che informano il ragionamento umano. Infine, è stato discusso l'impatto di tali tecnologie sulla società ed in particolare dell'accettabilità della delega ad una macchina del diritto di decidere di lasciar vivere o di uccidere.

---

[224] Cfr. ALTE PARTI CONTRAENTI CONVENZIONE CCW, *Documento finale della Riunione delle Alte Parti Contraenti, Genera 14-15 novembre 2013, Documento* CCW/MSP/2013/10, par. 32

[225] Cfr. ALTE PARTI CONTRAENTI CONVENZIONE CCW, *Report* CCW/MSP/2014/3 par. 10

Sul piano giuridico la discussione ha affrontato, in primo luogo, la questione della compatibilità delle armi autonome con il diritto internazionale attuale e in particolare i principi di distinzione, proporzionalità e precauzione, propri del diritto internazionale umanitario oltre che la compatibilità con le Convenzioni di Ginevra (1949), la clausola di Martens e il diritto consuetudinario. Sia le Delegazioni che gli esperti hanno riaffermato la necessità che gli sviluppi e l'utilizzazione di tali sistemi d'arma siano conformi al diritto internazionale umanitario mentre diversi punti vista sono stati espressi riguardo alla possibilità che tali sistemi saranno in grado di rispettare le norme internazionali.

Viene preso in considerazione, in secondo luogo, il tema dell'adeguamento del diritto internazionale attuale rispetto al quale sono emerse posizioni differenti, volte ad evidenziare, da un lato, l'utilità di giungere ad una definizione dei sistemi d'arma letali autonomi così come dei concetti di autonomia e prevedibilità di tali sistemi e, dall'altro, la necessità di disciplinare gli sviluppi tecnologici e di aumentarne la trasparenza e la condivisione.

Sono state affrontate, in terzo luogo, le questioni legate al regime di responsabilità nell'utilizzo di armi autonome rispetto alle quali è emersa la necessità di svolgere ulteriori studi in merito alla possibilità di attribuire la responsabilità agli Stati e, a livello individuale, agli operatori, ai programmatori o ai produttori dei sistemi d'arma autonomi.

Allo stesso modo, le questioni emergenti nell'ambito dei diritti umani sono state oggetto di discussione rispetto ai profili inerenti il diritto alla vita, la dignità umana, il diritto di essere protetti contro tutti i trattamenti inumani e il diritto ad un equo processo.

Infine, l'attenzione è stata rivolta all'eventuale impatto dello sviluppo e dell'utilizzo di armi autonome sulle norme dello jus ad bellum e, in particolare, rispetto alla questione se tali armi possano modificare la soglia alla quale è possibile il ricorso alla forza.

Da ultimo, sul piano militare, sono emerse posizioni opposte circa l'effettiva capacità dei nuovi armamenti di incidere o meno sulla condotta militare e sulla sicurezza e la pace internazionali.

Le questioni indicate sono state progressivamente approfondite nei report redatti al termine dei due successivi incontri del 2015 e del

2016[226] e hanno costituito la base per la successiva azione delle Alte Parti Contraenti sviluppata attraverso Group of Governamental Expert istituiti nel 2017, 2018 e 2019.

1.7.2 I lavori del Group of Governamental Expert del 2017 e 2018.

Nel Report[227] del 2017 il GGE delinea una serie di conclusioni e raccomandazioni rispetto ad alcune delle tematiche indicate rinviando per altre ai successivi lavori.

Si riconosce anzitutto che la CCW offre un contesto ottimale per il confronto sulla materia e che il carattere modulare ed evolutivo della Convenzione favorisce il bilanciamento tra le considerazioni umanitarie e le necessità militari così come il coinvolgimento di differenti stakeholder.

Viene affermata l'integrale applicabilità del diritto umanitario a tutti i sistemi d'arma inclusi i potenziali sviluppi ed usi dei sistemi LAWS.

Conseguentemente si riconosce che la responsabilità per l'utilizzo di qualsiasi sistema d'arma durante i conflitti rimane in capo agli Stati, i quali sono tenuti a rispondere sulla base del diritto internazione e umanitario delle azioni letali condotte, durante un conflitto armato, con l'utilizzo di qualsiasi sistema d'arma ivi compresi i sistemi LAWS.

Diversamente, vengono rinviate ai successivi lavori le questioni legate da un lato, alla duplice natura, civile e militare, delle tecnologie che sono alla base dei sistemi d'arma autonomi e, dall'altro la definizione dei caratteri tecnici, etici, sociali legali e militari delle tecnologie autonome.

Il successivo report del 2018[228] presenta, conseguentemente, una maggiore articolazione svolgendo specifiche conclusioni in relazione ai diversi aspetti: i) dei principi di riferimento della materia; ii) della caratterizzazione dei sistemi d'arma in esame al fine di delineare una definizione comune dei loro principali aspetti; iii) della rilevanza della componente umana nell'utilizzo di armi autonome.

---

[226] Cfr. ALTE PARTI CONTRAENTI CONVENZIONE CCW, *Report* CCW/MSP/2015/3; CCW/CONF.V/2 (2016)

[227] Cfr. ALTE PARTI CONTRAENTI CONVENZIONE CCW, *Report* CCW/GGE.1/2017/CRP.1 (2017)

[228] Cfr. ALTE PARTI CONTRAENTI CONVENZIONE CCW, *Report CCW*/GGE.1/2018/3 del 2018

In merito al primo punto, il Report conclude affermando la necessità di orientare lo sviluppo dei lavori alla luce del diritto internazionale e, in particolare, della Carta delle Nazioni Unite e del diritto umanitario e delle pertinenti considerazioni etiche. Inoltre, considerate le questioni problematiche che i sistemi d'arma autonomi pongono rispetto alla concreta applicabilità del diritto umanitario, il GGE sviluppa una serie di rilievi nei quali si chiariscono alcuni aspetti fondamentali.

Viene ribadita anzitutto, l'applicabilità del diritto umanitario anche ai sistemi LAWS e la responsabilità degli Stati per le decisioni relative al loro utilizzo, non potendosi trasferire alle macchine l'obbligo di risponderne. Principio del quale si afferma la validità per tutta la durata di vita dei sistemi d'arma considerati e dal quale deriva l'obbligo di garantire la conformità al diritto internazionale applicabile rispetto alla realizzazione, allo sviluppo e all'utilizzo di tutti i sistema d'arma rilevanti per la Convenzione, svolgendo una preventiva valutazione volta a determinare se l'utilizzo di una data arma, dei suoi vettori o delle metodologie di impiego, può essere, in alcune o tutte le circostanze, interdetta dal diritto internazionale.

Viene evidenziata l'opportunità di predisporre appropriate misure di sicurezza, fisiche e non, al fine di evitare l'acquisizione da parti di gruppi terroristici di tali sistemi d'arma così come il rischio di proliferazione. La valutazione e le misure di attenuazione dei rischi dovranno inoltre costituire una parte integrante della progettazione, realizzazione, sviluppo a utilizzo delle tecnologie emergenti adottate nei nuovi sistemi d'arma.

Sul piano giuridico viene infine affermato che la promozione del rispetto del diritto internazionale umanitario e delle altre obbligazioni giuridiche internazionali applicabili, dovrà prendere in considerazione l'utilizzo delle nuove tecnologie all'interno del dominio dei sistemi di arma letali autonomi sviluppando misure che non attribuiscano loro attributi umani. Tuttavia, le discussioni e le eventuali misure adottate nel contesto della Convenzione non dovranno costituire un ostacolo al progresso e all'utilizzo pacifico delle tecnologie intelligenti autonome né all'accesso e al loro utilizzo.

Rispetto ai caratteri dei sistemi d'arma e alla loro definizione il GGE esamina i diversi approcci concettuali alle loro caratteristiche e peculiarità rispetto alla Convenzione, delineando una serie di affermazioni conclusive. Vengono rilevate le diverse posizioni favorevoli e non all'elaborazione di una definizione la quale,

comunque, si ritiene non debba predeterminare le valutazioni politiche rispetto alle diverse scelte sottese allo sviluppo e utilizzo di tali sistemi d'arma. Le caratteristiche puramente tecniche possono costituire parametri per l'elaborazione di una definizione, mentre le caratteristiche tecniche relative alle capacità di auto apprendimento delle macchine dovranno essere studiate più approfonditamente in quanto suscettibili di determinare una pluralità di tipologie di armamenti autonomi. Viene riaffermato inoltre che il carattere letale di tali tecnologie non pregiudica l'applicazione e il rispetto della disciplina giuridica relativa alla conduzione delle ostilità. Allo stesso tempo si ritiene necessario approfondire lo studio dell'autonomia del processo di funzionamento e utilizzo dei sistemi d'arma in oggetto e in particolare alle caratteristiche legate al ruolo della componente umana al fine di chiarire le ulteriori questioni legate al regime di responsabilità.

Quest'ultimo aspetto è stato approfondito nel prosieguo del Report che, nella sezione C, nota l'importanza della natura e della qualità dell'interazione uomo-macchina al fine di rispondere alle preoccupazioni relative alla realizzazione, sviluppo e utilizzo di tali sistemi d'arma. Rapporto uomo macchina che pone problemi in ordine: 0) agli orientamenti politici che possono incidere sulla fase di pre-sviluppo; 1) allo svolgimento delle fasi di ricerca e sviluppo; 2) alla messa in funzione, valutazione e certificazione; 3 e 4) all'utilizzo, al controllo e all'abbandono di tali sistemi d'arma e 5) alla valutazione successiva il loro utilizzo.

Entro questa prospettiva il GGE svolge una serie di osservazioni in merito ad aspetti di particolare interesse. Viene anzitutto chiarito la rilevanza del tema della responsabilità rispetto alla Convenzione e che, di conseguenza, conformemente al diritto internazionale, l'uomo dovrà poter incidere sulle decisioni relative al ricorso alla forza durante tutto l'arco di utilizzo dei sistemi d'arma autonomi. Si rileva conseguentemente la necessità di adottare un sistema di valutazione indipendente basato su di un approccio multidisciplinare che tenga conto delle implicazioni di natura etica collegate allo viluppo e alle modifiche di tali armamenti pur nel rispetto delle istanze di sicurezza nazionale e delle norme sulla tutela dei brevetti e della proprietà industriale. In secondo luogo, il diritto internazionale umanitario viene individuato quale parametro di conformità per la valutazione dei sistemi d'arma esistenti o in corso di sviluppo. Conseguentemente si ritiene necessario sviluppare procedure di verifica e certificazione che coprano l'intero scenario delle possibilità d'uso, tenendo conto degli imperativi

di sicurezza nazionale e delle restrizioni alla divulgazione poste dalla disciplina di tutela della proprietà industriale e commerciale. Infine viene rilevato come l'obbligo di rispondere dell'uso di tali sistemi d'arma con riferimento all'uso della forza durante un conflitto armato, dovrà essere garantito secondo il diritto internazionale applicabile, in particolare assicurando che l'utilizzo di tutti i nuovi sistemi d'arma siano integrati in una catena di responsabilità, di comando e di controllo. Ciò al fine di conservare la responsabilità dell'uomo per il ricorso alla forza e potrà essere estesa alle azioni legate al funzionamento di un'arma se ciò sarà necessario ad assicurare il rispetto delle disposizioni del diritto internazionale umanitario. Il GGE conclude le osservazioni relative al rapporto uomo macchina osservando come il grado di autorità e responsabilità degli Stati in questa materia, richieda di approfondire l'esame al fine di giungere ad una definizione comune dell'ampiezza e dei caratteri dell'interazione uomo macchina e di classificare i livelli di responsabilità rispetto alle differenti fasi del ciclo di vita di un sistema d'arma.

L'ultimo punto trattato dal Report del 2018 riguarda l'esame delle applicazioni militari delle tecnologie d'arma in oggetto che si ritiene siano suscettibili di determinare alcune specifiche problematiche: la violazione dei diritti umani riconosciuti ai civili e ai combattenti in tempo di guerra; l'aumento delle tensioni regionali e internazionali legate alla corsa agli armamenti a all'abbassamento della soglia del ricorso alla forza; i rischi di proliferazione e di acquisizione e utilizzazione da parte di soggetti terroristici; la loro vulnerabilità informatica e la possibilità che ciò mini la fiducia nell'utilizzo civile delle tecnologie che compongono i sistemi d'arma autonomi.

Rispetto a tali problematiche le delegazioni hanno proposto soluzioni tra loro differenti rispetto al valore vincolante degli strumenti giuridici indicati e all'oggetto della relativa disciplina.

Alcuni Stati Membri ritengono sia necessario giungere alla definizione di strumenti giuridici vincolanti relativi alla definizione, da un lato, di divieti e regolamenti applicabili ai sistemi d'arma letale autonomi e, dall'altro, del principio del controllo umano sulle funzioni critiche dei sistemi d'arma letale autonomi.

Altri, diversamente, propongono l'adozione di una dichiarazione politica volta a stabilire i principi fondamentali, quali il principio del controllo umano sull'uso della forza e il principio di responsabilità dell'uomo, oltre che la definizione di elementi di trasparenza e di valutazione tecnologica.

Infine, nella convinzione che non siano necessarie ulteriori misure giuridiche, in ragione dell'applicabilità ai sistemi LAWS del diritto umanitario internazionale, si è proposto di proseguire le discussioni sugli aspetti relativi all'interazione uomo-macchina e all'attuazione degli obblighi giuridici internazionali esistenti, così come rispetto alla condivisione delle informazioni e all'individuazione di misure concrete e *best practices* per migliorare il rispetto del diritto internazionale.

I partecipanti concordano tuttavia sul fatto che queste diverse opzioni non si escludono necessariamente a vicenda e che il lavoro svolto finora dal gruppo di esperti governativi sui principi, la caratterizzazione, l'interazione uomo-macchina e lo studio delle potenziali applicazioni militari delle tecnologie emergenti nel campo dei sistemi d'arma letale autonomi e delle relative tecnologie hanno fornito una base utile per i lavori futuri che dovranno ampliare le definizioni esistenti, chiarire le questioni in sospeso e sviluppare i punti di convergenza sulla base del consenso.

1.7.3 Il Report del Gruppo di Esperti del 2019.

Le ultime due sessioni del GGE si sono tenute nel marzo e nell'agosto del 2019 e la discussione svolta è confluita in un ultimo Report che muove le sue considerazioni sulla base dei principi precedentemente elaborati.

In merito al rapporto tra le tecnologie emergenti nel settore delle armi letali autonome e il diritto internazionale umanitario il GGE sintetizza, nelle sue conclusioni, i punti principali del dibattito svolto.

Viene ribadita l'applicabilità del diritto internazionale e in particolare del diritto internazionale umanitario e i suoi requisiti e principi, tra cui distinzione, proporzionalità e precazione. L'uso dei sistemi d'arma letali deve essere dunque condotto conformemente al quadro giuridico indicato il quale, viene sottolineato, impone obblighi agli Stati, alle parti di un conflitto armato e alle persone, non alle macchine. Essi, di conseguenza, restano in ogni momento responsabili del rispetto degli obblighi giuridici internazionali.

Gli Stati devono inoltre garantire la responsabilità individuale per l'impiego di mezzi o metodi bellici che comportano l'uso potenziale di sistemi d'arma basati su tecnologie emergenti nel settore dei sistemi d'arma autonomi letali. In particolare, il GGE evidenzia che i requisiti e i principi del diritto internazionale umanitario, compresi, tra l'altro, i

principi di distinzione, proporzionalità e precauzione, devono essere applicati attraverso una catena di comando e controllo di cui siano responsabili operatori e comandanti umani. In merito viene chiaramente affermata da un lato, l'essenzialità del giudizio umano al fine di garantire la conformità dell'uso dei sistemi LAWS al quadro giuridico internazionale, dall'altro che esso presuppone che la persona possa fare in buone fede affidamento sul processo di elaborazione delle informazioni sottese alla decisione.

Vengono presi in considerazione i casi che riguardino sistemi d'arma LAWS non contemplati dalla CCW e dai protocolli allegati o da altri accordi internazionali, chiarendo che la popolazione civile e i combattenti restano in ogni momento sotto la protezione e l'autorità dei principi del diritto internazionale derivati da usi consolidati, dai principi dell'umanità e dai dettami della coscienza pubblica. Da tali principi deriva inoltre che un sistema d'arma LAWS non deve essere utilizzato se è di natura tale da causare lesioni superflue o sofferenze inutili, o se è intrinsecamente indiscriminato, o se non è altrimenti in grado di essere utilizzato conformemente ai requisiti e ai principi del diritto internazionale umanitario.

Infine il Gruppo di Esperti nota l'utilità delle attività nazionali finalizzate a verificare la conformità al diritto internazionale delle attività di progettazione, sviluppo, acquisizione o adozione di una nuova arma, mezzo o metodo di guerra.

2. La sicurezza delle tecnologie della comunicazione.

Tra le problematiche connesse all'azione degli attori nel cyberspace rientrano le attività poste in essere per finalità criminali suscettibili di incidere su interessi e valori fondamentali della Comunità Internazionale.

L'Assemblea Generale delle Nazioni Unite riconosce che la libera circolazione dell'informazione favorisce lo sviluppo economico e sociale, l'educazione e la governance democratica[229], mentre gli importanti progressi realizzati nella messa a punto e nell'utilizzo delle tecnologie dell'informazione[230] ne comportano una sempre maggiore dipendenza[231] dei governi, delle imprese, delle altre organizzazioni e degli utenti individuali per la promozione dello sviluppo socioeconomico e la fornitura di beni e servizi essenziali[232].

Allo stesso tempo ne evidenzia i rischi connessi.

Le preoccupazioni muovono dalla constatazione da una parte, che il progresso tecnologico crea nuovi strumenti e possibilità per le attività illecite[233] e, dall'altra, che il ricorso a tali tecnologie ha determinato la necessità di accrescere la cooperazione e il coordinamento a livello mondiale con la conseguenza che in tale ambito le azioni criminali possono avere ripercussioni su tutti gli Stati[234] in ragione dei legami sempre più stretti che esistono tra le infrastrutture essenziali della maggior parte dei paesi e le infrastrutture ITC, pervasive e tra esse integrate, che, ogni giorno, sorreggono le diverse attività[235].

Entro questo quadro generale l'azione di contrasto alle problematiche di natura criminale emergenti nel cyberspace posta in essere in seno alle Nazioni Unite, si sviluppa lungo tre direttrici, delineate dall'Assemblea Generale e sviluppate attraverso l'attività di altri organi ONU e la promozione di Conferenze Internazionale su specifici temi.

La prima area di intervento, definita con le Risoluzioni 55/63 del 2000 e 56/121 del 2001, attiene alla *"Lutte contre l'exploitation des technologies de l'information à des fins criminelles"* e si sviluppa nell'ambito dell'attività della Commissione per la prevenzione del

[229] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/55/63 del 2000
[230] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/56/121 del 2001
[231] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/57/239 del 2002
[232] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/58/199 del 2003
[233] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/55/63 del 2000
[234] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/56/121 del 2001
[235] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/58/199 del 2003

crimine e la giustizia penale avente come oggetto le leggi e i procedimenti giurisdizionali nazionali e, come finalità, la loro armonizzazione.

La seconda area di intervento, delineata a partire dalla Risoluzione 57/239 del 2002, presenta una vocazione più ampia essendo volta al coinvolgimento non solo degli attori Statali ma anche degli attori privati e sociali nella *"Création d'une culture mondiale de la cybersécurité"* e si sviluppa attraverso la promozione di conferenze internazionali a partire dal World Summit on the Information Society tenutosi a Ginevra nel 2003 e a Tunisi nel 2005 sotto l'egida dell'ITU.

Nel contesto delle grandi conferenze internazionali si realizza anche la terza linea di azione promossa dall'Assemblea Generale con la Risoluzione 58/199 del 2003 "Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information" che trova, con la Risoluzione 64/211 del 2009, un'ulteriore spazio entro cui svolgere il confronto e l'armonizzazione tra le azioni realizzate a livello nazionale nel Forum sur la gouvernance d'Internet.

2.1 L'azione di contrasto allo sfruttamento criminale delle tecnologie ITC.

Il lavoro svolto dall'Assemblea Generale muove dunque, dalla Risoluzione 55/63 del 2001[236] volta al contrasto dell'uso delle tecnologie ITC per finalità criminali, la quale delinea anzitutto il quadro generale entro cui l'Assemblea costruisce la sua azione indicandone i riferimenti nella più ampia azione condotta dalle Nazione Unite nel settore della lotta alla criminalità e dello sviluppo dei sistemi giudiziari nazionali e dei reciproci rapporti per il contrasto della criminalità transnazionale[237].

[236] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/55/63

[237] Questi vengono individuati nella Dichiarazione del Millennio e nella Dichiarazione ministeriale adottata dal Consiglio economico e sociale nella sessione del 2000. Viene inoltre richiamata la Risoluzione 45/121 del 1990 con la quale vengono approvate le raccomandazioni dell'ottavo Congresso delle Nazioni Unite sulla prevenzione del crimine e il trattamento dei delinquenti, della quale rileva, in particolare, la sezione dedicata alla risoluzione sulla criminalità legata alle tecnologie informatiche con la quale si invitano gli Stati Membri ad aumentare gli sforzi nel contrastare tale tipo d criminalità.

Azione rispetto alla quale la Risoluzione delinea il ruolo centrale che può essere svolto dalle Nazioni Unite e in particolare dalla Commissione per la prevenzione del Crimine. Differentemente dal lavoro condotto in tema di sicurezza internazionale precedentemente analizzato, il ruolo delle Nazione Unite è fin dall'inizio posto al centro dell'azione internazionale di contrasto alla criminalità informatica così come il contributo che può essere fornito dalle imprese private operanti in questo settore.

Azione che, inoltre, muove dalle stesse preoccupazioni determinate dalla integrazione e pervasività del complesso delle tecnologie ITC oltre che dall'affermazione della necessità che essa si svolga sul piano multilaterale nonostante le differenti prospettive degli Stati e i diversi livelli di sviluppo tecnologico che gli Stati Membri sono chiamati a sostenere.

L'assemblea Generale infine pone il suo lavoro in collegamento con quello svolto da altre organizzazioni internazionali richiamando, già in questa prima risoluzione, il lavoro realizzato in diversi contesti internazionali. Anzitutto viene richiamato il lavoro del Comitato di Esperti sulla criminalità nel cyberspazio del Consiglio d'Europa relativo ad un progetto di Convenzione sulla Cyber criminalità. In secondo luogo, si fa riferimento ai principi fissati nel corso dei lavori dei Ministri della giustizia e degli interni del Gruppo degli Otto, così come al lavoro della Conferenza del Gruppo degli Otto sul dialogo tra i governi e l'industria privata concernente la sicurezza e la fiducia nel cyberspazio tenutasi a Parigi nel 2000. Infine, vengono richiamate le raccomandazioni approvate nello stesso anno dalla terza Riunione dei Ministri della giustizia delle Americhe, tenutasi in Costa Rica nel quadro dell'azione dell'Organizzazione per gli Stati Americani.

Affermando in tal modo la sua centralità rispetto all'azione multilaterale volta al contrasto della criminalità nel cyberspazio, l'Assemblea Generale ribadisce l'importanza che gli Stati Membri tengano conto di tali misure nella loro azione nazionale evidenziando, tra le altre, alcune specifiche misure alla luce delle quali gli Stati, attraverso i loro sistemi legali e giudiziari, dovrebbero238: i) garantire l'effettività delle leggi e delle procedure così che i criminali informatici non possano godere di impunità; ii) coordinare le indagini e i procedimenti giudiziari; iii) sviluppare lo scambio di informazioni e la formazione del personale; iv) proteggere la riservatezza e l'integrità

[238] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/55/63 Punto 1

delle rete informatiche e procedere alla sanzione dei reati che le compromettano; v) conservare i dati relativi a particolari indagini e garantirne l'accesso così come la rapida apertura di procedimenti di mutua assistenza per la raccolta e lo scambio di prove sui crimini informatici.

Tali misure prevedono inoltre che i cittadini vengano informati della necessità di prevenire e combattere l'utilizzo criminale delle tecnologie informatiche che, a loro volta, dovrebbero essere progettate per prevenire e rilevare qualsiasi loro sfruttamento illecito.

Viene infine ribadito che la lotta contro lo sfruttamento delle tecnologie dell'informazione nel campo del diritto penale richiede soluzioni che tengano conto della necessità di proteggere le libertà individuali e la privacy, preservando al contempo i poteri di autorità pubbliche per combattere questo tipo di sfruttamento.

2.2 Gli strumenti di contrasto alla criminalità informatica.

L'invito rivolto agli Stati Membri di prendere in considerazioni tali indicazioni nella loro azione interna e internazionale viene rinnovato nella successiva Risoluzione 56/121 del 2001[239] con la quale l'Assemblea Generale sostanzialmente riafferma il contenuto della risoluzione sopra indicata e, in particolare, l'importanza del lavoro svolto all'interno della Commissione per la prevenzione del crimine e della giustizia penale cui gli Stati Membri sono chiamati a contribuire.

In questo ambito la Commissione promuove lo sviluppo delle capacità necessarie per il contrasto alla criminalità informatica fornendo supporto specialistico in materia di risposta dei sistemi di giustizia penale fornendo assistenza tecnica per lo sviluppo delle capacità, la prevenzione e la sensibilizzazione, la cooperazione internazionale, la raccolta di dati, la ricerca e l'analisi sulla criminalità informatica.

Il cyber crime entra a far parte della sua azione a partire dalla Dichiarazione di San Salvador[240], elaborata nel dodicesimo Congresso delle Nazioni Unite sulla prevenzione del crimine e la giustizia penale

[239] Cfr. ASSEMBLEA GENERALE *Risoluzione* A/RES/56/121

[240]Cfr. Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, Consultabbile all'indirizzo web https://www.unodc.org/documents/crime-congress/12th-Crime Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf

tenutosi nel 2010, la quale riconosce la rilevanza e l'attualità del problema, con riferimento, tra gli altri, alle vulnerabilità dei minori e al contributo che i soggetti privati possono fornire per contrastarle, ed invita la Commissione a collaborare con gli Stati, le altre organizzazioni internazionali e gli attori privati nei settori di sua competenza241.

In particolare la Commissione è invitata a convocare un Gruppo di Esperti Governativi a composizione non limitata allo scopo di realizzare uno studio approfondito sul fenomeno della cyber criminalità e sulle misure prese dagli Stati Membri, dalla Comunità Internazionale e dal settore privato, comprese le legislazioni nazionali, le migliori pratiche, l'assistenza tecnica e la cooperazione internazionale, al fine di valutare le misure da adottare per rafforzare i sistemi giuridici nazionali e internazionali[242].

2.3 L'attività di rilevazione e precisazione del fenomeno criminale nel Cyberspace.

L'Assemblea Generale delle Nazioni Unite da seguito a quanto previsto dalla Dichiarazione di San Salvador con la Risoluzione 65/230 del 2010[243] attribuendo alla Commissione per la prevenzione del crimine e la giustizia penale il compito di formare il Gruppo di Esperti con le modalità e le finalità indicate.

Il primo GGE ha svolto i suoi lavori nel 2011 giungendo alla definizione di una serie di argomenti ritenuti rilevanti e delle metodologie di analisi[244]. Il paragrafo 42 della dichiarazione di san Salvador identificava le diverse questioni di fondo oggetto dello studio del Gruppo di Esperti. Queste venivano individuate nello studio del generale fenomeno della criminalità informatica, delle legislazioni nazionali, delle migliori pratiche, dell'assistenza tecnica e della cooperazione internazionale. Tale studio doveva inoltre essere condotto con riferimento alle misure adottate dagli Stati Membri, dalla Comunità Internazionale e dal settore privato. Infine, l'obbiettivo della ricerca veniva fissato nell'esame delle misure volte a rafforzare il quadro esistente e nell'indicazione di nuove misure nazionali e internazionali,

---

[241] Cfr. Salvador Declaration, parr. 39-41
[242] SALVADOR DECLARATION par. 42
[243] ASSEMBLEA GENERALE *Risoluzione* A/RES/65/230, par. 9
[244] CONSIGLIO ECONOMICO E SOCIALE, *Report* UNODC/CCPCJ/EG.4/2011/3

di natura non solo giuridica, volte a contrastare il nuovo fenomeno criminale.

Tali indicazioni vengono raccolte dal GGE che identifica 12 tematiche rispetto alle quali strutturare il lavoro di cui è incaricato. Il fenomeno della cyber criminalità, la rilevazione statistica e i problemi posti costituiscono le prime tre aree tematiche. Ad esse seguono l'identificazione di approcci legislativi comuni, i temi dell'incriminazione e delle regole di procedure e delle prove di natura informatica, la cooperazione internazionale. Vengono presi inconsiderazione gli ulteriori temi della prevenzione del crimine attraverso i mezzi esistenti nel campo della giustizia penale e le altre forme di risposta al fenomeno criminale. Infine, gli ultimi due temi vengono individuati nell'azione delle organizzazioni internazionali e nell'assistenza tecnica ai paesi tecnologicamente non avanzati.

Sul piano delle metodologie è stato predisposto un questionario, diffuso tra gli Stati Membri, le organizzazioni internazionali, gli attori privati, con lo scopo di raccogliere e analizzare dati rispetto al cyber crime al fine di studiare, come richiesto dall'Assemblea Generale, nuove risposte legali, a livello nazionale ed internazionale, all'emergere del cyber crime.

Il Gruppo di Esperti condurrà la ricerca e la rivelazione statistica con il supporto dell'Ufficio delle Nazioni Unite contro la droga e il crimine (UNODC) il quale elaborerà uno studio[245] che, nella sua complessità, costituisce una fotografia dettagliata del fenomeno e delle risposte sviluppate a livello nazionale e internazionale. In tale studio i temi indicati vengono ulteriormente raccolti in 8 capitoli relativi ai temi: i) della connettività e criminalità informatica; ii) il quadro globale; iii) la legislazione e i quadri normativi; iv) la criminalizzazione; v) l'applicazione della legge e lo svolgimento delle indagini; vi) le prove elettroniche e la giustizia penale; vii) la cooperazione internazionale; viii) e la prevenzione.

Successivamente, con la Risoluzione 67/189 del 2012 l'Assemblea Generale esprime apprezzamento per i lavori del Gruppo di Esperti che viene incaricato di completare il suo lavoro e di presentarne i risultati[246].

Il Gruppo di Esperti ha sviluppato i suoi lavori a partire dallo studio condotto dall'ONUDOC rispetto ai temi e sulla base delle metodologie

[245] UNODC, *Etude détaillée sur la cybercriminalité*, Ebauche – Février 2013 consultabile all'indirizzo web https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_French.pdf

[246] ASSEMBLEA GENERALE *Risoluzione* A/RES/67/189 del 2012 punto 6

indicate nel precedente Rapporto del 2011mettendone in evidenza alcuni punti e notando come durante il loro svolgimento siano emerse tra gli Stati Membri da un lato, prospettive differenti nell'adozione di misure di contrasto alla cyber criminalità e, dall'altro, un largo sostegno alle azioni volte a rafforzare le capacità e l'assistenza tecnica così come al ruolo che l'ONUDC può svolgere in questo settore.

Il Report[247] muove dalla constatazione che l'esponenziale aumento delle connessioni renderà difficile immaginare un "delitto informatico" per il quale non esisterà una prova informatica legata alla connessione Internet. Allo stesso tempo, tuttavia, viene rilevata la difficoltà nell'individuare una definizione di cyber criminalità la quale è variamente delineata in funzione degli obiettivi perseguiti e del contesto nel quale viene utilizzata. A livello globale solo un numero limitato di azioni criminali lesive della confidenzialità, dell'integrità e della disponibilità dei dati o dei sistemi informatici è chiaramente ricondotta nel concetto di cyber criminalità. Concetto dal quale restano esclusi azioni quali l'utilizzazione di computer per realizzare una lesione o un pregiudizio finanziario o di altra natura comprese lo spam e alcune forme di furto di identità e di attentati ai contenuti informatici che generalmente sono ricondotti a fattispecie penali tradizionali.

Il problema che si pone è dunque quello di delineare delle specifiche definizioni per le diverse fattispecie di cyber criminalità. Un'azione chiarificatrice, tuttavia, non strettamente necessaria per la definizione dei poteri speciali in materia di indagini e cooperazione internazionale ove, diversamente, rileva il report, appare più utile giungere ad una definizione di prova informatica in ragione delle conseguenze che da essa discendono sull'incriminazione e quindi sul concreto esercizio dei poteri pubblici rispetto alle libertà fondamentali e ai diritti umani.

Nonostante la facilità con cui è possibile compiere azioni criminali i rischi che ne derivano sono diversamente considerati e affrontati dagli Stati, dalle imprese private e dai singoli utenti. Da qui una prima conseguenza legata all'inesattezza delle rilevazioni statistiche che non forniscono di conseguenza le informazioni necessarie a supportare le azioni di contrasto.

Un primo strumento di contrasto è rappresentato dalla legislazione esistente la cui disciplina, che dovrebbe coprire tutti i principali settori, affronta gli aspetti legati all'incriminazione, previlegiando

[247] UNODC, *Gruppo di Esperti sulla Cyber criminalità*, Report UNODC/CCPCJ/EG.4/2013/2

l'individuazione di fattispecie speciali per le principali azioni criminali. Diversamente le discipline più recenti, o in progetto, tendono ad occuparsi delle indagini, della competenza, delle prove e della cooperazione internazionale.

Sul piano internazionale e regionale si rileva l'adozione di vari strumenti giuridici ed in particolare della Convenzione del Consiglio d'Europa sulla criminalità informatica che, viene sottolineato, costituisce lo strumento giuridico di riferimento per lo sviluppo normativo in materia tanto a livello statale quanto nel contesto delle varie organizzazioni internazionali.

Per quanto riguarda l'incriminazione viene rilevato come alla nozione di cyber crimine vengono generalmente ricondotte alcune determinate fattispecie, mentre solo in alcuni casi vi si riconducono anche i contenuti osceni o il traffico di sostanze stupefacenti e di esseri umani. Varie prospettive si registrano anche rispetto alla qualificazione dell'elemento dell'intenzionalità, valutato differentemente a seconda che l'accesso sia considerato illegale in quanto tale o solo qualora comporti determinate conseguenze come l'accesso a dati e sistemi protetti.

La disciplina giuridica delle fattispecie incriminanti solleva particolari questioni legate alla tutela delle libertà fondamentali e dei diritti umani rispetto all'azione dei poteri pubblici per i quali, come rileva il rapporto, *"le droit iternational des droit de l'homme constitue une arme aussi bien offensive que défensive puisqu'il oblige à la fois à incriminer (de facon limitée) les forme de expression extremes et à protegér les autres forme. Certain limites à la liberté d'expression (…) s'imposent donc aux Etats qui sont parties aux instruments internationaux pertinents relatifs aux droits de l'homme. Les autre disposent d'une certaine marge d'appréciation pour determiner les limites des forms d'expression acceptables compte tenu de leurs cultures et de leurs traditions juridiques"*[248].

La tutela dei diritti umani e delle libertà fondamentali costituisce un aspetto problematico anche rispetto alla legislazione sulle indagini, sulla repressione del cyber crime e sulle prove informatiche, suscettibili di ledere il diritto alla vita privata sancito sul piano internazionale. I caratteri del cyberspace e dell'azione criminale posta in essere per suo tramite determinano infatti, la necessità di sviluppare nuove tecniche di

[248] UNODC, *Gruppo di Esperti sulla Cybercriminalità*, Report UNODC/CCPCJ/EG.4/2013/2, PAR. 17

indagine che sfuggono alla disciplina esistente, così come di coinvolgere soggetti privati, quali i fornitori di servizi informatici, determinando un affievolimento delle tutele previste in ragione tanto delle necessità tecniche quanto dei rapporti di forza tra pubblici poteri e attori privati.

Un vulnus nella tutela dei diritti fondamentali che, evidenzia il report, si manifesta più facilmente nelle fasi di cooperazione internazionale in ragione dei diversi livelli di tutela che possono esistere tra gli Stati coinvolti nelle azioni di inchiesta e repressione transnazionali.

Cooperazione internazionale che, pur basandosi su norme internazionali definite, sempre più spesso richiede di essere adattata ai caratteri delle nuove forme di criminalità ricorrendo ad accordi spesso informali suscettibili di diminuire la tutela dei diritti umani che possono venire in rilievo nelle fasi di indagine e repressione dei crimini.

Il Gruppo di Esperti conclude il suo report proponendo lo sviluppo delle attività legislative nazionali e degli strumenti multilaterali nei diversi settori indicati delineando una serie di possibili interventi volti ad affrontare problemi tanto di carattere generale quanto più di natura prettamente tecnica.

Lo studio condotto in tema di cyber criminalità dal Gruppo di Esperti e presentato nel 2013 ha trovato riconoscimento nel corso del tredicesimo Congresso delle Nazioni Unite sulla prevenzione del crimine e la giustizia penale. A partire dalla Dichiarazione di Doha, che l'Assemblea Generale ha fatto propria con la Risoluzione 70/174, gli Stati lo hanno posto alla base del lavoro di ulteriori Gruppi di Esperti che la Commissione per la prevenzione del crimine e la giustizia penale è stata invitata a istituire. Il lavoro dei successivi GGE è stato quindi volto a sviluppare il dialogo tra gli Stati Membri sulle diverse questioni evidenziate nello studio condotto nel 2013.

Tra queste sono state oggetto dei lavori del GGE del 2017 le questioni relative allo scambio di informazioni sulle legislazioni nazionali, sulle migliori pratiche, sull'assistenza tecnica e sulla cooperazione internazionale. Sono state inoltre discusse le opzioni proposte per rafforzare le normative nazionali e internazionali.

La successiva riunione del 2018 rientra nel piano di discussioni che dovrebbe concludersi nel 2021 e che finora hanno riguardato l'approfondimento delle questioni legislative e dell'incriminazione.

Il lavoro svolto dalla Commissione per la prevenzione del crimine e la giustizia penale si sviluppa sul lungo periodo al fine sostenere le

attività degli Stati Membri volte al contrasto delle diverse forme di criminalità. Entro questa prospettiva l'attività del Gruppo di Esperti risponde alle esigenze poste dall'emergere del fenomeno del cybercrime perseguendo gli obiettivi indicati dalla Commissione: i) aumentare l'efficienza e l'efficacia delle indagini, dei procedimenti giudiziari e delle decisioni in materia di criminalità informatica, in particolare riguardo allo sfruttamento e all'abuso sessuale dei minori in linea, entro il quadro giuridico di diritti umani; ii) di fornire una risposta efficiente ed efficace a lungo termine dell'intero governo alla criminalità informatica, compresi il coordinamento nazionale, la raccolta di dati e lo sviluppo di un quadro giuridico efficace, che porti a una risposta sostenibile e a un maggiore effetto deterrente; iii) il rafforzamento della comunicazione nazionale e internazionale tra il governo, le forze dell'ordine e il settore privato favorendo una maggiore conoscenza dei rischi di criminalità informatica da parte del pubblico.

2.4 Sviluppo di una cultura globale della sicurezza informatica.

Le due risoluzioni su cui si fonda l'azione in materia di cyber criminalità costituiscono, assieme alle precedenti in materia di sicurezza, i presupposti su cui poggia la successiva Risoluzione dell'Assemblea Generale 57/239 del 2003[249] con la quale si delinea la seconda linea di azione indicata.

La risoluzione, intitolata *"Création d'une culture mondiale de la cybersécurité"*, evidenzia come la sicurezza informatica non dipenda dalle sole azioni di governo e dalle leggi ma riposi su un ruolo attivo di tutta la società. Si riconosce infatti che, in base ai rispettivi ruoli, governi, imprese, altre organizzazioni e singoli proprietari e utenti delle informazioni, devono essere consapevoli dei rischi associati alla sicurezza informatica e delle loro responsabilità così come devono prendere provvedimenti per rafforzare la sicurezza nell'utilizzo di tali tecnologie.

Ribadendo, in questa prospettiva, l'importanza della cooperazione internazionale nella creazione di sicurezza informatica, in particolare attraverso il sostegno agli sforzi nazionali per sviluppare la capacità umana, aumentare le opportunità di formazione e occupazione, migliorare i servizi pubblici e la qualità della vita sfruttando le

[249] ASSEMBLEA GENERALE *Risoluzione* A/RES/57/239

tecnologie moderne nella costruzione di reti affidabili e sicure per lo scambio di informazioni e promuoverne l'accesso universale, l'Assemblea Generale indica alcuni elementi funzionali allo sviluppo della sicurezza informatica invitando le rilevanti organizzazioni internazionali e gli Stati membri a prenderli in considerazione nello sviluppo delle rispettive azioni e, in particolare, nel corso dei lavori del World Summit on the Information Society nelle sessioni di Ginevra 2003 e Tunisi 2005[250].

Lo sviluppo di una cultura globale della sicurezza informatica è infatti parte di un'azione più ampia volta a guidare il processo di affermazione di una *"Società dell'Informazione incentrata sulla persona, inclusiva e orientata allo sviluppo, nella quale ognuno possa creare, accedere, utilizzare e condividere informazioni e conoscenza, ponendo le condizioni affinché gli individui, le comunità e i popoli possano sfruttare appieno le proprie potenzialità nel favorire il loro sviluppo sostenibile e nel migliorare la loro qualità di vita"*[251].

A tal fine, la Dichiarazione di Ginevra afferma la necessità di sfruttare le potenzialità delle tecnologie dell'informazione e della comunicazione per promuovere i traguardi di sviluppo enunciati nella Dichiarazione del Millennio nel rispetto degli obbiettivi e dei principi della Carta delle Nazioni Unite e della Dichiarazione dei Diritti Umani, di cui vengono riaffermate l'universalità, l'interdipendenza e l'interrelazione così come la centralità, tra essi, dei diritti alla libertà di opinione e di espressione e al libero sviluppo della propria personalità, oltre che il riconoscimento del principio di accesso universale e non-discriminatorio alle tecnologie ITC sia per le nazioni che per gli individui.

Entro questo quadro generale, l'affermazione di una cultura globale della sicurezza risponde alle necessità di costruire la fiducia e rafforzare la sicurezza delle informazioni e della privacy nella prospettiva della protezione del consumatore, considerati prerequisiti essenziali per lo sviluppo della Società dell'Informazione. Sforzi questi che dovrebbero essere sostenuti da tutti gli stakeholder e le istituzioni

[250] Tali elementi, puntualmente indicati nell'allegato alla risoluzione vengono individuati nella realizzazione di azioni di sensibilizzazione, responsabilizzazione e reazione rispetto ai fatti criminali. Viene inoltre indicata la necessita di porre in essere azioni di valutazione dei rischi funzionali ad azioni di progettazione, realizzazione e gestione oltre che di valutazione dei sistemi di sicurezza. Infine, si evidenzia come tali azioni devono essere realizzate tenendo presenti criteri etici che prendano in considerazione gli interessi dei diversi soggetti coinvolti e i principi democratici volti alla tutela delle libertà fondamentali delle persone.

[251] ASSEMBLEA GENERALE *Risoluzione* A/RES/57/239, par. 1

internazionali competenti, attraverso una maggiore cooperazione internazionale centrata sull'azione delle Nazioni Unite. Un'azione volta a prevenire l'uso potenziale delle ICT per scopi incompatibili con gli obiettivi di mantenimento della stabilità e sicurezza internazionale e che possano danneggiare l'integrità delle infrastrutture nazionali, a danno della sicurezza degli Stati.

Le prospettive e i principi individuati nella Dichiarazione di Ginevra vengono valorizzati nel Piano d'Azione, adottato nella stessa occasione, che si pone l'obiettivo di rappresentare una piattaforma flessibile per la promozione della Società dell'Informazione su scala nazionale, regionale ed internazionale.

Il processo di discussione volto al coinvolgimento, assieme agli Stati e alle istituzioni internazionali, del settore privato e della società civile, delineato nei lavori della Conferenza di Ginevra, costituisce la caratteristica principale dell'azione delle Nazioni Unite nel campo della sicurezza del cyberspazio. Affianco ai governi, a cui viene attribuito un ruolo leader nello sviluppo e nell'applicazione delle politiche digitali, viene valorizzato il contributo di consulenza che il settore privato e la società civile possono fornire. Il loro contributo, inoltre, rileva nello sviluppo e nella diffusione delle tecnologie ITC così come nella creazione di una Società dell'Informazione equa. In questa prospettiva, il piano d'azione attribuisce alle istituzioni internazionali e regionali, incluse le istituzioni finanziarie, un ruolo chiave nell'integrare l'uso delle ICT all'interno del processo di sviluppo e nel rendere disponibili le risorse necessarie per la costruzione della Società dell'Informazione e per la valutazione dei progressi compiuti.

Nel campo della sicurezza e della fiducia nell'uso delle tecnologie ITC la cooperazione fra i governi all'interno delle Nazioni Unite e con tutti gli stakeholder rilevanti viene orientata alla protezione dei dati e della rete attraverso la prevenzione e la risposta alle minacce esistenti e potenziali. Allo stesso tempo la loro azione deve essere volta al contrasto del cybercrime attraverso la definizione di linee guida, di interventi legislativi e lo sviluppo della cooperazione giudiziaria, che consentano un'efficace investigazione e persecuzione degli atti illeciti. Inoltre, i governi e gli altri stakeholder, dovrebbero promuovere attivamente l'istruzione e la sensibilizzazione dell'utente sulla privacy on-line e sulle modalità per la sua tutela, sviluppando iniziative ed elaborando linee-guida sul diritto alla vita privata e la protezione dei dati e del consumatore, condividendo, inoltre, le best practices nel

campo della sicurezza dell'informazione e dell'utilizzo della rete Internet incoraggiandone l'utilizzo da parte di tutti gli stakeholder.

Le azioni delineate in occasione del World Summit on the Information Society di Ginevra si caratterizzano per la loro proiezione di lungo periodo. A questo primo momento di discussione ne sono infatti seguiti altri, a cadenza annuale, che hanno progressivamente definito aspetti specifici della problematica.

Un primo momento di valutazione e rilancio delle azioni svolte è rappresentato dal World Summit on the Information Society tenutosi nel 2014 a Ginevra. In tale occasione sono stati ribaditi i principi ispiratori dello sviluppo di una Società della Conoscenza, ed in particolare dei processi multilaterale aperti, così come la funzionalità delle tecnologie ITC rispetto al mantenimento della sicurezza e della pace internazionale e l'applicabilità, a tal fine, del diritto internazionale, della Carta delle Nazioni Unite e dei Diritti Umani[252].

Per quanto riguarda il tema specifico della sicurezza e del contrasto alla criminalità nel cyberspace si sottolineano le difficoltà riscontrate nel tutelare il rispetto della vita privata e nello sviluppo delle capacità di coordinamento e di intervento in caso di incidenti attraverso l'istituzione di équipe nazionali di intervento[253]. Allo stesso modo viene evidenziata la necessità di sviluppare ulteriormente, ai diversi livelli, le azioni politiche e legislative[254]. A tal fine l'Atto finale della Conferenza rinnova gli sforzi e le tipologie d'azione precedentemente individuate, al fine di rafforzare la fiducia nelle tecnologie ITC, migliorando la sicurezza dell'informazione e dei dati così come la protezione della vita privata e dei consumatori, attraverso la costruzione di una cultura globale della cyber sicurezza fondata sulla cooperazione internazionale e tenendo conto dei diversi livelli di sviluppo tecnologico[255].

Cooperazione internazionale che nel corso dei dieci anni precedenti ha trovato realizzazione attraverso il lavoro svolto nelle numerose iniziative internazionali e regionali volte alla realizzazione del Piano d'Azione di Ginevra. Tra queste un ruolo particolare è stato svolto dal Forum per la Governance di Internet nel quale vengono affrontate le

[252] *Déclaration du SMSI+10 sur la mise en oeuvre des résultats du SMSI*
[253] *Déclaration du SMSI+10 sur la mise en oeuvre des résultats du SMSI; Sez. C. Difficultés rencontrées pendant la mise en oeuvre des grandes orientations et problèmes récemment apparus par. 16*
[254] ID. Par. 23
[255] Vision du SMSI+10 pour le SMSI au cours de l'après-2015 par. 11

problematiche legate alla gestione e alla sicurezza della rete Internet, ovvero dell'infrastruttura fondamentale del cyberspace.

2.5 La sicurezza delle infrastrutture informatiche critiche.

Nel contesto del Forum per la Governance di Internet trova dunque sviluppo la terza linea d'azione definita dall'Assemblea Generale delle Nazioni Unite, in particolare con le Risoluzioni 58/199[256] del 2003 e 64/211[257] del 2009, volta allo sviluppo della sicurezza delle infrastrutture delle tecnologie della comunicazione.

Con la prima Risoluzione indicata, intitolata *"Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information"*, la sicurezza delle infrastrutture diviene un elemento fondamentale della più ampia azione volta alla creazione di una cultura globale della sicurezza del cyberspace in ragione delle *"liens de plus en plus étroit qui existent entre les infrastructures essentielles de la plupart des pays et les infrastructures essentielles de l'information qui, toujours plus, relient et touchent leurs opérations"*.

Ribadendo la necessità di sviluppare la cooperazione multilaterale, la comunicazione e il coordinamento, sia rispetto ai rischi e agli incedenti informatici sia rispetto ai progressi tecnici e legislativi realizzati dagli Stati e dalle Organizzazioni Internazionali, l'Assemblea Generale indica alcuni elementi essenziali che gli Stati Membri sono chiamati a prendere in considerazione sia nella loro azione nazionale sia in quella multilaterale ed in particolare nello svolgimento del World Summit in The Information Society del 2003 e del 2005.

Tali elementi consistono: i) nei sistemi d'allerta rispetto a minacce e incidenti; ii) nelle attività di sensibilizzazione circa la natura e la funzione delle infrastrutture essenziali; iii) l'esame e l'identificazione delle loro interdipendenze al fine di rafforzarne la protezione; iv) la promozione di partenariati tra il settore pubblico e quello privato; v) la creazione di sistemi di comunicazione d'urgenza e di gestione delle crisi; vi) lo sviluppo di politiche di protezione delle infrastrutture essenziali; vii) le attività di indagine sugli attacchi commessi ai danni di tali strutture; viii) lo sviluppo di attività di formazione ed esercitazione per rafforzare le capacità di reazione e resilienza; ix) lo

[256] ASSEMBLEA GENERALE *Risoluzione* A/RES/58/199
[257] ASSEMBLEA GENERALE *Risoluzione* A/RES/64/211

sviluppo di misure di diritto penale e processuale oltre che la formazione di personale specializzato per la conduzione delle indagini; x) lo sviluppo della cooperazione internazionale nel campo della sicurezza e della ricerca sulle infrastrutture essenziali delle telecomunicazioni.

A queste prime indicazioni la Risoluzione 64/2011 del 2009 ne fa seguire altre volte a definire un *"Méthode d'auto-évaluation volontaire des efforts nationaux visant à protegér les infrastructures essentielles".*

L'allegato, così intitolato, alla risoluzione del 2009 delinea, per ogni una delle diverse aree tematiche, una serie di criteri funzionali alla valutazione delle azioni svolte nei campi: i) della definizione dei bisogni e delle strategie in materia di cyber sicurezza; ii) del ruolo e della responsabilità degli attori coinvolti; iii) dell'elaborazione delle politiche e della partecipazione dei diversi attori; iv) della cooperazione tra il settore pubblico e il settore privato; v) della gestione degli incidenti; vi) della definizione del quadro giuridico e, infine, vii) dello sviluppo di una cultura mondiale della cyber sicurezza.

2.6 Internet Governance Forum

Ed è nel contesto di tale ultima azione che l'Assemblea Generale delinea, a partire dai lavori del World Summit on the Information Society, il ruolo del Forum sulla Governance di Internet individuato quale spazio deputato al dialogo multilaterale sulle diverse questioni connesse alla governance di Internet, al fine di assicurare la funzionalità, la stabilità, la sicurezza, la governance e lo sviluppo di questa particolare infrastruttura rispetto alle quali agli Stati è attribuita un'eguale responsabilità.

Il Forum sulla Governance di Internet trova infatti il suo fondamento nella Tunisi Agenda for the Information Society[258] la quale, ai paragrafi da 71 a 80, ne delinea il mandato. Il WSIS riconosce la necessità di sviluppare la discussione sulle politiche pubbliche relative ad Internet e chiede al Segretario generale delle Nazioni Unite di instituire un nuovo forum entro cui sviluppare il dialogo politico tra tutti gli stakeholder.

[258] ITU, WORLD SUMMIT ON THE INFORMATION SOCIETY, *Documento* WSIS-05/TUNIS/DOC/6(Rev. 1)-E

Durante lo sviluppo dell'attività del Forum, le questioni legate alla sicurezza del cyberspace sono state variamente affrontate nel corso dei numerosi workshop tematici venendo declinate in funzione dei progressi registrati dalle tecnologie delle telecomunicazioni.

Di particolare interesse i risultati dell'ultimo IGF tenutosi a Parigi nel novembre 2018 nei quali vengono presi in considerazione i rischi legati alle modalità di utilizzo delle più recenti tecnologie viste nel primo capitolo. L'affermarsi delle tecnologie dell'Internet of Things, delle trasmissioni 5G, della raccolta e analisi dei Big Data e, infine dell'Intelligenza Artificiale il cui sviluppo si basa su tali innovazioni tecniche, *"complicate the cybersecurity question in multiple dimension, introducing new issue and engaging a multiplicity of players"* [259]. Allo stesso tempo le rispose non sono più limitate alla sola dimensione tecnica, funzionale ad eliminare i rischi, ma richiedono un approccio multidisciplinare volto ad indagare i diversi livelli di interazione tra i due estremi del problema costituiti dalla sicurezza dello spazio cyber e dal rispetto delle libertà fondamentali e dei diritti umani. Il problema, come viene rilevato, consiste dunque nella necessità di giungere ad una maggiore comprensione di come i progressi tecnologici" affect *people's lives, and their impact on privacy and human right"* al fine di delineare adeguate soluzioni tecniche e politiche volte ad evitare gli sviluppi negativi di tali tecnologie e a preservare la natura aperta, libera e sicura di Internet[260].

In tale prospettiva i lavori del Forum del 2018 pongono al centro del dialogo internazionale in materia di cyber sicurezza il rispetto della privacy, la protezione dei dati e la sicurezza delle nuove tecnologie, delineandone i tratti principali. Viene anzitutto rilevato come sicurezza e privacy, elementi fondamentali su cui riposa la fiducia degli utenti dalla quale dipende il progresso tecnologico, costituiscano interesse di tutti gli stakeholder il cui ruolo è fondamentale nella definizione di un equilibrio tra i due aspetti del problema. Equilibrio che, rispetto alle relazioni fra attori internazionali, viene perseguito attraverso lo sviluppo di una azione di Cyber diplomacy che coinvolga anche gli attori non statali nella definizione delle strategie di cyber sicurezza e che si basi su norme di comportamento responsabile e sulla definizione di canali di collaborazione e cooperazione.

---

[259] INTERNET GOVERNANCE FORUM, *The Internet of Trust. Chair's Summary & IGF Messagges*, Thirteenth Internet Governance Forum (IGF) 12-14 November 2018 Paris, France, p. 14

[260] INTERNET GOVERNANCE FORUM, *The Internet of Trust. Chair's Summary & IGF Messagges*, Thirteenth Internet Governance Forum (IGF) 12-14 November 2018 Paris, France, p. 14

Sul piano legislativo si evidenzia la necessità di tutelare i dati personali, tra i quali vengono ricompresi i dati biometrici che, inseparabilmente collegati alla persona e alla sua vita, possono essere oggetto di abusi. Il diritto alla privacy è infatti ritenuto cruciale per la salvaguardia delle libertà e lo sviluppo della persona e la sua tutela è determinata anche dallo sviluppo di una disciplina delle attività economiche legate alle nuove tecnologie.

Un particolare interesse rivestono le osservazioni svolte dal IGF in merito alle tecnologie dell'Internet of Things, ritenute essenziali ma al contempo fonte di nuovi rischi. Rischi che possono manifestarsi nella loro applicazione allo sviluppo delle Smart City determinando discriminazioni sociali, ad esempio nell'accesso ai servizi pubblici. Problemi questi legati all'utilizzo di algoritmi rispetto ai quali si ritiene necessario perseguire *"a better understanding of how algorithms afect peope's lives, on the potential risk of automated or algorithmic decision making, and of their impact on human rights and the right to privacy, will allow adequate tecnhnical and policy solution, including a right to explanation"*[261].

I lavori svolti dal IGF in materia di sicurezza si caratterizzano da un lato per la loro aderenza agli sviluppi tecnologici, dall'altro per la loro capacità di anticipare le problematiche che questi possono presentare. In questo senso il IGF del 2018 evidenzia l'attenzione posta non più alle sole problematiche di natura tecnica, oggetto principale dei precedenti lavori, bensì rivolta alle applicazioni e alle interconnessioni tra le diverse tecnologie. In altri termini, nel dibattito internazionale divengono centrali le problematiche legate all'azione del cyberspace, ovvero alle dinamiche di sviluppo del dominio informatico inteso quale fattore di progresso della società. Problematiche rispetto alle quali i diritti umani sono individuati come *limes* del progresso tecnologico.

Il tema della promozione e protezione dei diritti umani nel cyberspace verrà presa in considerazione nei successivi paragrafi. Le questioni emerse e gli approcci adottati verranno osservati partendo dai lavori delle Nazioni Unite in particolare dell'Assemblea Generale e del Consiglio sui Diritti dell'Uomo.

[261] INTERNET GOVERNANCE FORUM, *The Internet of Trust. Chair's Summary & IGF Messagges*, Thirteenth Internet Governance Forum (IGF) 12-14 November 2018 Paris, France, p. 21

3. Promozione e tutela dei diritti umani nel Cyberspace.

Il progresso tecnologico ha radicalmente modificato le forme di comunicazione rendendole istantanee e globalmente condivise, in tal modo facilitando la diffusione delle informazioni e contribuendo allo sviluppo della Società dell'Informazione.

Le tecnologie della comunicazione e le forme in cui essa si svolge sono divenuti i fattori determinanti il dibattito pubblico, tanto locale quanto globale, in ragione della loro capacità di favorire i processi di accesso all'informazione e di partecipazione democratica. Rispetto ai diritti umani la comunicazione informatica permette di amplificare le istanze di quanti operano nella loro difesa favorendo, ad esempio, la denuncia di abusi o la condivisione di valori, idee e azioni che in essi trovano la loro radice. Allo stesso tempo, tuttavia, è chiara la vulnerabilità di tali tecnologie ad attività di sorveglianza e intercettazione elettroniche, perpetrate tanto da poteri Statali quanto da imprese private o anche attori criminali, facilitate dall' intrinseco carattere dual-use delle tecnologie ITC e dal loro sviluppo esponenziale e, al contempo, avvolto dalla segretezza propria delle ricerche industriali o militari.

Come evidenziato dall'Alto Commissario per i Diritti Umani nel suo statement alla 24th sessione del Consiglio dei Diritti Umani del 2013, il progresso della tecnologia delle comunicazioni *"has salso contributed to blurring of lines between the pubblic and private sphere, and made possibile unprecedent levels of interference with the right to privacy"*[262].

Il diritto alla privacy viene dunque individuato come il perno intorno al quale sviluppare l'azione volta ad esaminare ed affrontare le problematiche legate al rapporto tra il progresso delle tecnologie della comunicazione e i diritti umani. Un rapporto in continua evoluzione rispetto al quale è tuttavia possibile individuare alcuni temi partendo dai quali è possibile svolgere un'azione volta a determinare un punto di equilibrio tra l'uso della tecnologia e i diritti umani.

---

[262] Opening Remarks by MS. NAVI PILLAY, United Nations Hight Commissioner for Human Rights to the Side-event at 24th sessio of the UN Human Rights Council "How to safeguard the right to privacy in the digital age?", 20 Settembre 2013, Palais des Nations, Genevra, consultabbile all'indirizo Internet https://newsarchive.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=E

Le Nazioni Unite, ponendo al centro il rispetto del diritto alla vita privata e delle libertà fondamentali e dei diritti umani ad essa legati, identificano cinque specifiche aree tematiche, oggetto dell'azione dell'Assemblea Generale e del Consiglio dei Diritti Umani[263].

La prima di esse viene individuata nelle modalità in cui le autorità legislative, amministrative e giudiziarie tutelano il diritto alla privacy a livello nazionale a cui segue la seconda tematica relativa alla loro mancanza di effettività.

La terza tematica, da cui derivano le incertezze circa il confine tra la dimensione privata dell'individuo, sottratta all'esercizio dei pubblici poteri e la sua dimensione pubblica, in cui tali poteri possono essere esercitati, è costituita dalla necessità di definire il significato di privacy e di comunicazioni private nell'era digitale. Il problema che si pone, in altri termini, è quello di definire quali siano gli interessi privati inerenti alle comunicazioni o al trasferimento di dati attraverso le tecnologie di telecomunicazione.

Ad essi è inoltre collegata la quarta tematica oggetto dell'azione delle Nazioni Unite relativa alla definizione dei parametri di legittimità delle attività di sorveglianza poste in essere dagli Stati per finalità di sicurezza, in particolare nel contesto della lotta al terrorismo.

Attività di sorveglianza, intercettazione, raccolta, conservazione e analisi dei dati che gli Stati spesso demandano o impongono ad imprese private la cui azione, in queste come nella generalità delle loro attività nel cyberspace, è oggetto della quinta e ultima tematica volta alla definizione della responsabilità degli attori economici privati in materia di rispetto e tutela del diritto alla privacy e dei diritti umani in generale.

L'azione delle Nazioni Unite, volta a tutelare i diritti umani rispetto alle attività poste in essere nel cyberspace da attori statali e privati, pone, dunque, al centro la tutela del diritto alla vita privata, articolandosi rispetto ai temi indicati e sviluppandosi attraverso il lavoro dell'Assemblea Generale e del Consiglio dei Diritti Umani.

L'azione dei due organi poggia sui diversi report elaborati nel tempo che affrontano i temi indicati costituendo la base delle decisioni e delle risoluzioni da essi adottate lungo un percorso che inizia a

[263] Vedi Opening Remarks by MS. NAVI PILLAY, United Nations Hight Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Palais des Nations, Ginevra, consultabile all'indirizzo internet https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E

delinearsi a partire dal 2011 e che trova definizione nella sessione dell'Assemblea Generale del 2013 per svilupparsi, successivamente, attraverso i panel tematici promossi dal Consiglio dei diritti Umani nel 2014 e, infine, nel mandato triennale conferito nel 2015 dal Consiglio ad uno special rapporteur il cui lavoro confluisce in report presentati annualmente.

3.1 I primi rapporti tematici.

I confini del problema affrontato iniziano quindi a delinearsi attraverso i tre reports[264] presentati dallo special rapporteur Frank La Rue nel 2011.

Il primo di essi, relativo a *"la promotion et la protection du droit à la liberté d'opinion et d'expressio"*, presentato al Consiglio dei Diritti Umani, delinea le tendenze e le problematiche che emergono rispetto al diritto di cercare, ricevere e condividere ogni tipo di informazione e idea attraverso internet. Entro questa prospettiva il rapporto prende in considerazione i caratteri e l'innovatività della rete Internet. Mette inoltre in evidenza l'applicabilità delle norme internazionali sui diritti umani, relative, in particolare, al diritto alla libertà di opinione e di espressione, alla rete Internet quale mezzo di comunicazione. Individua circostanze eccezionali che giustificano l'applicazione di restrizioni rispetto ad alcuni tipi di informazioni. Prende in considerazione le questioni dell'accesso ad Internet e dell'accesso alle infrastrutture fisiche e tecniche necessarie per accedervi oltre che, infine, il tema dell'accesso universale alla rete Internet.

Il secondo rapporto, presentato all'Assemblea Generale ed intitolato *"Promotion et protection du droit à la liberté d'opinion et d'expression"*, continua lo sviluppo degli argomenti trattati nel precedente rapporto e ne introduce altri. In particolare, esamina la questione delle restrizioni inammissibili e descrive le espressioni che gli Stati, a titolo eccezione, sono tenuti ad interdire in virtù del diritto internazionale. Sottolinea inoltre l'importanza dello sviluppo di una cultura informatica e della formazione in materia di tecnologie dell'informazione per accedere utilmente ed efficacemente all'informazione on-line. Infine pone l'accento sull'obbligazione

[264] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto Special Rapporteur* A/HRC/17/27; ASSEMBLEA GENERALE, *Rapporto* A/69/290; CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto Special Rapporteur* A/HRC/23/40

positiva che, nonostante l'accesso ad Internet non sia ancora riconosciuto quale diritto umano, si impone agli Stati tenuti a facilitare l'esercizio del diritto di esprimersi liberamente attraverso lo strumento Internet.

L'azione delle Nazioni Unite trova definizione, come detto, a partire dal 2013 con la Risoluzione dell'Assemblea Generale 68/167 intitolata *"Le droit à la via privée à l'ère du numérique*" che recepisce il lavoro svolto dallo special rapporteur Frank La Rue nel suo terzo rapporto sulla *"promotion et la protection du droit à la liberté d'opinion et d'expression"* presentato al Consiglio dei Diritti Umani nello stesso anno.

Con la risoluzione indicata l'Assemblea Generale riafferma la centralità della Carta delle Nazioni Unite, della Dichiarazione Universale dei Diritti dell'Uomo e dei due Patti sui diritti civili e politici e sui diritti economici, sociali e culturali, quali strumenti di riferimento per la tutela dei diritti umani nell'era digitale.

In particolare, viene rilevata la centralità del diritto alla vita privata, definito dall'art. 12 della Dichiarazione Universale e dall'art. 17 del Patto sui diritti civili e politici, in base al quale, riafferma esplicitamente la risoluzione, *"nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance et le droit de toute personne à la protection de la loi contre de telles immixtions"*.

La centralità di tale diritto deriva dalla sua importanza *"pour le droit à la liberté d'expression et le droit de ne pas être inquiété pour ses opinions et qu'il constitue l'un des fondements d'une société démocratique"*.

In questa prospettiva viene inoltre riaffermata la necessità di rispettare integralmente la libertà di ricercare, ricevere, trasmettere le informazioni e, in particolare, di garantire, in quanto fondamentale, l'accesso all'informazione e la partecipazione democratica[265].

L'Assemblea Generale ritiene infatti, che il diritto alla vita privata sia particolarmente esposto alle azioni, illecite o arbitrarie, di sorveglianza, di intercettazione e di raccolta dei dati, condotte da soggetti statali così come da imprese private o singoli utenti, che lo sviluppo tecnologico rende sempre più facili e pervasive[266].

[265] ASSEMBLEA GENERALE, *Risoluzione* A/RES/68/167, par. 6
[266] ASSEMBLEA GENERALE, *Risoluzione* A/RES/68/167, par. 4

La rilevanza di tali attività rispetto al godimento dei diritti umani e delle libertà fondamentali era stata messa in evidenza nell'indicato rapporto A/HRC/23/40 nel quale vengono analizzati gli effetti della sorveglianza delle comunicazioni da parte degli Stati sull'esercizio dei diritti alla vita privata e della libertà di espressione sottolineando *"l'urgente nécessité d'examiner plus en détail les nouveaux modes de surveillance et de réviser les lois nationales réglementant ces pratiques conformément aux normes relatives aux droits de l'homme"*[267]. Il dinamismo proprio dei progressi tecnologici, si evidenzia, non ha solamente modificato le modalità di esercizio delle attività di sorveglianza ma anche l'oggetto della stessa determinando la necessità, in primo luogo, di riaffermare il contenuto del diritto alla vita privata che, benché previsto da numerosi strumenti giuridici internazionali, appare nel contesto attuale indefinito. Tale incertezza si riverbera sul godimento di altri diritti essendo il rispetto della vita privata considerato come *"préalable essentiel à la réalisation du droit à la liberté d'expression"*. In questo senso vanno lette le statuizioni iniziali della risoluzione 68/167 volte alla riaffermazione del contenuto di tale diritto e dei suoi legami con altri diritti e libertà fondamentali.

Il rapporto, in secondo luogo, prende in considerazione le condizioni al cui sussistere è possibile attuare delle restrizioni al diritto alla vita privata sulla base dell'art. 17 del Patto sui diritti civili e politici e dell'art. 19 comma 3 della Dichiarazione Universale dei Diritti dell'Uomo. Quest'ultimo in particolare enuncia le condizioni in base alle quali le restrizioni al diritto possono essere permesse differenziandosi dall'art 17 il quale ammette restrizioni che siano necessarie legittime e proporzionate.

L'incerto quadro giuridico che ne deriva costituisce un aspetto problematico in quanto legato, da una parte, all'incidenza di Internet sul diritto alla libertà di opinione e di espressione e, dall'altra, alle sempre più pervasive attività di sorveglianza poste in essere dai poteri pubblici così come da soggetti privati[268] soprattutto nel quadro della lotta al terrorismo[269], nel cui contesto sfuma il rispetto dei principi di necessità e proporzionalità previsti dalle norme internazionali.

Il rapporto dunque procede, in terzo luogo, all'analisi delle diverse modalità di sorveglianza delle comunicazioni e delle norme giuridiche

---

[267] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto Special Rapporteur* A/HRC/23/40, par. 1
[268] CONSIGLIO DEI DIRITTI DELL'UOMO, *Report* A/HRC/17/27; ASSEMBLEA GENERALE, *Report* A/66/290.
[269] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/13/37.

nazionali che, in generale, non riflettono i progressi tecnologici, concludendo con l'indicazione di una serie di azioni volte ad affrontare i singoli aspetti problematici rilevati.

La risoluzione dell'Assemblea Generale 68/167 ne accoglie i risultati sottolineando l'incidenza delle attività di sorveglianza sull'effettività dei diritti umani e notando che nonostante l'interesse pubblico possa giustificare tale attività gli Stati sono comunque tenuti al rispetto degli obblighi derivanti dal diritto internazionale in materia di diritti umani la cui effettività viene distintamente riaffermata nel particolare contesto della lotta al terrorismo.

Le preoccupazioni espresse dal rapporto indicato sono state accentuate dall'emergere, tra il 2013 e il 2014, delle attività di sorveglianza condotte da agenzie statunitensi e britanniche la cui ampiezza ha spinto[270] l'Assemblea Generale all'adozione della risoluzione sul diritto alla vita privata nell'era informatica.

Alla riaffermazione del contenuto del diritto alla privacy, indicata in precedenza, ne segue un'ulteriore volta ad affermare che i diritti delle persone goduti offline devono essere ugualmente protetti nelle attività svolte on line. In questa prospettiva tutti gli Stati sono invitati a rispettare e proteggere il diritto alla privacy nella comunicazione digitale oltre che a rivedere le loro procedure, le pratiche e le normative, relative alla sorveglianza e all'intercettazione delle comunicazioni e alla raccolta di dati sottolineando la necessità che essi garantiscano il pieno rispetto degli obblighi internazionali derivanti dalle norme sui diritti umani.

Sempre nella risoluzione 68/167, l'Assemblea Generale ha chiesto all'Alto Commissario delle Nazioni Unite per i diritti umani di presentare, alla sua sessantanovesima sessione, così come alla ventisettesima sessione del Consiglio dei diritti umani, un rapporto sulla protezione e promozione del diritto alla privacy nel contesto della sorveglianza e dell'intercettazione delle comunicazioni digitali e della raccolta di dati personali sul territorio nazionale e all'estero, anche su larga scala.

Il rapporto A/HRC/27/37, *intitolato "Le droit à la vie privée à l'ère du numérique"*[271], ribadisce inizialmente, tanto le preoccupazioni quanto il legame tra i diversi diritti umani evidenziati in precedenza rilevando, tuttavia, come l'incidenza delle sempre più avanzate

[270] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/27/37 par. 4
[271] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/27/37

tecnologie[272] possa porre in discussione altri diritti quali quello alla salute o a non subire atti di tortura o trattamenti pregiudizievoli. Il report evidenzia in particolare il problema delle attività di raccolta e analisi dati funzionali alla ricerca e cattura di persone o all'utilizzo di droni e alle incertezze giuridiche che sussistono rispetto a tali attività.

Le principali questioni affrontate riguardano le attività di sorveglianza di massa e la loro conformità con le norme giuridiche internazionali e se occorra definire ulteriori garanzie rispetto alla violazione dei diritti umani. A tal fine il report sviluppa gli aspetti legati: alla determinazione di cosa costituisca una violazione della vita privata nel contesto delle comunicazioni informatiche; alla definizione delle espressioni "arbitrarie e illegali"; e alla precisazione di quali soggetti godano della protezione dei diritti umani e in quali casi.

Rispetto al primo problema il punto di riferimento viene individuato nell'Osservazione generale n° 16 del Comitato dei Diritti dell'Uomo nella quale si sottolinea che il rispetto dell'art. 17 del Patto sui diritti civili e politici esige che siano garantiti, in diritto e in fatto, l'integrità e il carattere confidenziale della corrispondenza[273]. Nel contesto del cyberspace viene tuttavia registrato l'emergere di posizioni differenti. Secondo una prima prospettiva la comunicazione e lo scambio dei dati personali attraverso sistemi informatici presuppone un compromesso per il quale gli individui, consapevolmente, cedono le informazioni personali in cambio dell'accesso ai servizi. Altri sostengono che l'intercettazione o la raccolta dei dati personali relativi alle comunicazioni e non al contenuto delle comunicazioni non costituiscono una immissione nella vita privata.

Rispetto a tali posizioni il rapporto evidenzia criticamente i dubbi circa la consapevolezza del contenuto del compromesso tra utenti e fornitori di servizi oltre alla possibilità di quest'ultimi di ricavare informazioni personali dai metadati. Su questo punto in particolare viene richiamata un'osservazione della Corte Europea di Giustizia secondo la quale i metadati delle comunicazioni *"prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont*

[272] In particolare le tecniche di analisi dei metadati, i big data.

[273] ASSEMBLEA GENERALE, *Documento* A/43/40, Allegato VI, par. 8 *"La correspondance doit être remise au destinataire, sans interception, sans être ouverte, et sans qu'il en soit pris autrement connaissance".*

été conservées"[274]. Ne deriva, secondo il rapporto, che tutte le forme di intercettazione, di raccolta e di conservazione costituiscono un'immissione nella vita privata determinata, con riferimento ad una pronuncia della Corte Europea dei Diritti dell'Uomo, dalla stessa possibilità che le comunicazioni siano intercettate275. Conseguentemente l'esistenza stessa di un programma di sorveglianza di massa costituisce un'immissione nella vita privata rispetto al quale lo Stato dovrà dimostrare la non arbitrarietà e la liceità.

Rispetto a questo secondo problema il report richiama anzitutto le osservazioni del Consiglio dei Diritti Umani in cui si chiarisce che il termine illegale comporta che alcuna immissione nella sfera privata della persona può aver luogo *"sauf dans les cas envisagés par la loi. Les immixtions autorisées par les États ne peuvent avoir lieu qu'en vertu d'une loi, qui doit elle-même être conforme aux dispositions, aux buts et aux objectifs du Pacte"*. Viene inoltre sottolineato che per ragionevolezza dell'immissione si intende che *"l'immixtion dans la vie privée doit être proportionnée à l'objectif recherché et doit être nécessaire dans les circonstances particulières à chaque cas"*.

La mancata previsione nell'art. 17 del Patto sui diritti civili e politici di clausole restrittive espresse non esclude tuttavia che le restrizioni possono essere applicate o invocate in maniera tale da ledere l'essenza stessa del diritto enunciato dal Patto. I limiti all'esercizio dei pubblici poteri trovano infatti fondamento nei grandi principi della legalità, necessità e proporzionalità dell'esercizio dei poteri pubblici, la cui applicabilità nel contesto delle comunicazioni informatiche è espressamente ribadita dal report. L'importanza di tali principi appare vieppiù crescente di fronte alla tendenza degli Stati di invocare ragioni di carattere securitario e di tutela dell'interesse nazionale determinate da fenomeni criminali e di natura terroristica per giustificare i programmi di sorveglianza delle comunicazioni informatiche. Quantunque ciò possa costituire un obiettivo legittimo ai sensi dell'art. 17 del Patto, la misura dell'immissione nella vita privata dovrà tuttavia,

---

[274] CORTE EUROPEA DI GIUSTIZIA, *Pronunce* C-293/12 e C-594/12, Digital Rights Ireland e Seitlinger et altri, par. 26 e 27, e 37; Cfr. UFFICIO ESECUTIVO DEL PRESIDENTE DEGLI STATI UNITI, *Documento* Big Data and Privacy: A Technological Perspective
Consultabile all'indirizzo web www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_may_2014.pdf

[275] CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Weber e Saravia vs. Allemagne*, par. 78; *Malone vs. RU*, par. 64.

"être évalué[276] *selon que la mesure est nécessaire ou non à la réalisation de cet objectif et qu'elle présente un intérêt réel à cette fin"*[277].

Valutazioni che appaiono ancor più essenziali rispetto alle attività di intercettazione, raccolta, conservazione e analisi dei dati condotte da soggetti privati e utilizzate dai poteri pubblici.

Il rapporto nota, infatti, come le legislazioni che impongono, alle compagnie telefoniche e ai fornitori di servizi Internet, la conservazione obbligatoria dei dati, e di renderli disponibili all'accesso delle autorità pubbliche o ai servizi di sicurezza, non appaiono né necessarie né proporzionali[278].

La legislazione in materia di intercettazioni, raccolta conservazione e analisi dei dati, è oggetto dell'attenzione del report sotto l'ulteriore profilo del rispetto della norma prevista dal secondo comma dell'art. 17 del Patto sui diritti civili e politici. Questa dispone che ogni individuo ha diritto alla protezione della legge contro le interferenze od offese determinate dall'immissione nella sua vita privata. Ciò presuppone, rileva il rapporto, che tutti i programmi di sorveglianza delle comunicazioni devono essere fondati su una legge accessibile al pubblico la quale, a sua volta, deve essere conforme al regime costituzionale dello Stato e al diritto internazionale dei diritti umani. Viene inoltre chiarito che l'accessibilità non si esaurisce nella pubblicità della legge richiedendo che questa sia sufficientemente precisa da permettere alla persona di comprenderne le disposizioni al fine di determinare i suoi comportamenti e di conoscere le conseguenze di tutti i suoi atti[279].

Il terzo punto problematico evidenziato dal rapporto attiene alla determinazione di quali soggetti abbiano diritto alla protezione della propria vita privata e in quali casi.

La questione riguarda in primo luogo l'applicazione extraterritoriale del Patto sui diritti civili e politici rispetto alle attività

---

[276] COMITATO DEI DIRITTI DELL'UOMO, CCPR/C/21/Rev.1/Add.9, *Osservazione Generale n. 27* sull'art. 12 del Patto Internazionale sui diritti civili e politici ove si sottolinea che *"les restrictions ne doivent pas porter atteinte à l'essence même du droit […]; le rapport entre le droit et la restriction, entre la règle et l'exception, ne doit pas être inversé»1. Il Comitato chiarisce inoltre che "qu'il ne suffit pas que les restrictions servent les buts autorisés; celles-ci doivent être également nécessaires pour protéger ces buts». En outre, les mesures doivent être proportionnées: elles doivent constituer le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché"*

[277] COMITATO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/27/37, par. 24

[278] COMITATO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/27/37, par. 26

[279] COMITATO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/27/37, par. 28

di sorveglianza informatica. L'art. 2 del Patto prevede che gli Stati aderenti si impegnino a rispettare e a garantire a tutti gli individui che si trovino sul loro territorio e siano sottoposti alla loro giurisdizione i diritti riconosciuti dal Patto stesso senza distinzione alcuna. Il report richiama le osservazioni del Comitato dei diritti dell'uomo nelle quali si chiarisce che gli Stati devono rispettare e garantire i diritti riconosciuti dal Patto a chiunque si trovi sotto il loro potere o il loro controllo effettivo.

Rispetto a tale problematica, vengono dunque in rilievo le nozioni di "potere" e di "controllo effettivo" che permettono l'esercizio dei poteri pubblici, rispetto ai quali i diritti umani si pongono come un limite al loro abuso da parte degli Stati. I riflessi di tale impostazione sono particolarmente importanti nel contesto del cyberspace, caratterizzato, come visto nel primo capitolo, da infrastrutture e soggetti fornitori di servizi che, pur localizzabili nel territorio di un dato Stato, supportano e forniscono servizi per attività transnazionali e globali.

La responsabilità dello Stato conseguentemente emerge nel caso in cui esso eserciti un potere sulle infrastrutture o una competenza regolamentare su terze parti che controllano fisicamente le infrastrutture o i servizi di gestione dei dati delle comunicazioni informatiche estendendosi a tutte le persone che ne vengono coinvolte senza alcuna distinzione ai sensi dell'art. 2 del Patto internazionale sui diritti civili ed economici.

Il rapporto prosegue prendendo in considerazione due ulteriori aspetti, su cui svolge osservazioni di carattere generale, relativi agli strumenti giurisdizionali di tutela dei diritti e al ruolo che le imprese private potrebbero svolgere rispetto alle problematiche indicate.

Si conclude, infine, con l'indicazione di alcune raccomandazioni rivolte agli Stati circa le misure legislative e le attività la cui realizzazione determinerebbe una maggiore tutela del diritto alla vita privata nel contesto delle comunicazioni informatiche.

Tali raccomandazioni così come le diverse conclusioni cui giunge il report confluiscono nella Risoluzione adottata dall'Assemblea Generale nella sua successiva sessione del 2014 la quale, inoltre, prende nota dei risultati del dibattito svolto durante i due panel tematici promossi dal consiglio dei Diritti Umani nel 2014[280].

[280] Nella decisione 25/117, adottata nel marzo 2014, il Consiglio dei diritti umani ha deciso di convocare nella sua ventisettesima sessione una tavola rotonda sulla promozione e la tutela del diritto alla privacy nell'era digitale. Ciò è avvenuto rispetto al tema della sorveglianza interna ed extraterritoriale e dell'intercettazione delle comunicazioni digitali e della raccolta di dati

La Risoluzione 69/166[281], anch'essa intitolata *"Le droit à la vie privée à l'ère du numérique"*, riafferma inizialmente il contenuto del diritto alla vita privata nei termini precedentemente espressi sottolineando, egualmente, l'importanza del pieno rispetto della libertà di ricercare, ricevere e comunicare informazioni e del diritto di accesso all'informazione e della partecipazione democratica.

In secondo luogo, la risoluzione constata l'importanza dei metadati e i rischi del loro utilizzo evidenziati dal report sottolineando, nel paragrafo successivo, come la sorveglianza o l'intercettazione e la raccolta di dati privati personali, illecite o arbitrarie, possa ledere il diritto alla vita privata e compromettere la libertà di espressione e i principi di una società democratica, in particolare se tali pratiche vengono effettuate in forma generalizzata o massiva.

Riaffermati i diritti oggetto della tutela internazionale e individuate le attività che possono determinare la loro lesione, la risoluzione, successivamente, delinea, nei termini indicati dal report, i limiti entro cui tali attività possono essere svolte e la responsabilità che ne deriva in capo agli Stati in virtù delle norme internazionali sui diritti dell'uomo e sulle libertà fondamentali.

Rispetto al primo punto l'Assemblea Generale nota in particolare che la sorveglianza delle comunicazioni informatiche deve essere conforme alle obbligazioni internazionali relative ai diritti dell'uomo e riposare su un quadro giuridico accessibile a tutti, chiaro, preciso, completo e non discriminatorio. Inoltre, nessuna limitazione al diritto alla vita privata dovrà essere arbitraria o illecita né irragionevole rispetto all'obiettivo legittimamente perseguito. Infine, ricorda che gli Stati parti del Patto internazionale sui diritti civili e politici devono fare il possibile per adottare leggi o altre misure che possono essere necessarie per garantire l'effettività dei diritti sanciti dal Protocollo.

In merito al secondo aspetto, così come evidenziato dal report, la risoluzione sottolinea le obbligazioni internazionali in materia di diritti

---

personali, anche su scala di massa, al fine di individuare le sfide e le migliori pratiche. Il Consiglio per i diritti umani ha chiesto all'Alto Commissario di organizzare la tavola rotonda in consultazione con gli Stati, gli organismi competenti delle Nazioni Unite, la società civile, le organizzazioni non governative, il settore privato e le istituzioni nazionali per i diritti umani. La discussione si è svolta il 12 settembre 2014. L'OHCHR ha quindi preparato una relazione di sintesi sui risultati, che è stata presentata al Consiglio dei diritti umani nella sua ventottesima sessione. Vedi CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/28/39 Résumé de la réunion-débat du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme.

[281] ASSEMBLEA GENERALE, *Risoluzione* A/RES/69/166

dell'uomo relativi al diritto alla vita privata sussistono in capo agli Stati anche rispetto alle attività di intercettazione delle comunicazioni digitali di singoli individui o alla raccolta di dati personali. Tali obblighi sussistono inoltre nel caso in cui gli Stati chiedano a terzi, in particolare alle aziende private la comunicazione dei dati personali dei loro utenti.

Queste ultime, ricorda la risoluzione, sono tenute a rispettare i diritti umani come previsto dai principi relativi alle imprese private e ai diritti umani elaborati nel quadro delle Nazioni Unite.

Tali affermazioni dell'Assemblea Generale riposano sulle preoccupazioni e inquietudini generate dalle ampie possibilità di intercettazione, raccolta, conservazione ed elaborazione dei dati che la tecnologia offre agli Stati e ai privati suscettibili di ledere diritti e libertà fondamentali attraverso azioni la cui ampiezza può estendersi oltre i confini di un singolo Stato. Azioni, inoltre, cui sempre più frequentemente si fa ricorso al fine di tutelare interessi pubblici fondamentali dai rischi posti dai fenomeni terroristici che, tuttavia, sono ricondotti entro i limiti determinati dagli obblighi internazionali in materia di diritti umani.

Ciò spinge l'Assemblea Generale a riaffermare il diritto alla vita privata e alla sua tutela anche nel contesto del cyberspace domandando agli Stati Membri di garantirne il rispetto adottando le misure necessarie alla sua tutela e rivedendo le loro leggi, pratiche e procedure conformemente agli obblighi internazionali sui diritti umani. Domanda, inoltre, di creare meccanismi nazionali di controllo giudiziario, amministrativo e parlamentare che siano indipendenti, efficaci, imparziali e dotati di poteri e strumenti sufficienti per garantire la trasparenza, nella misura ritenuta opportuna, e la responsabilità degli Stati in termini di sorveglianza e di intercettazione delle comunicazioni e di raccolta dei dati personali. Agli Stati Membri viene infine chiesto di permettere alle persone il cui diritto alla vita privata è stato leso in conseguenza di una sorveglianza arbitraria o illegale, di avere accesso a strumenti di ricorso efficace conformi alle obbligazioni internazionali in materia di diritti dell'uomo.

La risoluzione dell'Assemblea Generale infine incarica il Consiglio dei diritti dell'uomo di continuare lo studio della questione al fine di determinare chiaramente i principi, le norme e le pratiche di riferimento da adottare in materia di promozione e protezione del diritto alla vita privata.

3.2 L'attività del Consiglio dei Diritti Umani delle Nazioni Unite.

L'azione che il Consiglio dei Diritti Umani porrà in essere su impulso dell'Assemblea Generale a partire dal 2014, può essere ricostruita prendendo come riferimento due sue risoluzioni: la risoluzione A/HRC/RES/25/ del marzo 2014 e la risoluzione A/HRC/RES/28/16 dell'aprile 2015, adottata in ottemperanza alla risoluzione dell'Assemblea Generale 69/166 sopra discussa.

Con la prima risoluzione, il Consiglio conferisce allo special rapporteur David Kaye un mandato triennale per la prosecuzione dello studio sulla promozione e protezione del diritto alla libertà di espressione il cui lavoro si articola in tre rapporti presentati annualmente a partire dal 2015.

Il primo di essi, il rapporto A/HRC/29/39 sulla promozione e la protezione del diritto alla libertà di opinione e di espressione, prende in considerazione il ricorso alle tecniche di cifratura e di anonimato nelle comunicazioni informatiche.

Il rapporto in particolare svolge l'analisi di due questioni tra di esse collegate.

La prima riguarda l'applicabilità del diritto alla vita privata e alla libertà d'opinione e espressione rispetto alle tecniche di cifratura e di anonimato nelle comunicazioni informatiche. La seconda indaga, alla luce dei diritti umani, l'esercizio dei poteri statali volti a limitare l'utilizzo di tali tecniche.

Il report giunge alla conclusione che la crittografia e l'anonimato, così come i concetti di sicurezza che ne sono alla base, assicurano la riservatezza e la sicurezza necessarie per l'esercizio del diritto alla libertà di opinione e di espressione nell'era digitale. Ciò è ritenuto essenziale per l'esercizio di altri diritti quali il diritto alla sicurezza economica, alla privacy, a un processo equo, alla libertà di riunione e di associazione pacifica e il diritto alla vita e all'integrità fisica. Conseguentemente le misure adottate dai poteri pubblici volte ad imporre restrizioni all'utilizzo delle tecniche di cifratura e di anonimato sono soggette ai principi di legalità, trasparenza, necessità e proporzionalità oltre che di legittimità dell'obiettivo perseguito.

Il successivo rapporto A/HRC/32/38 del 2016, prende in considerazione il quadro legale della libertà di espressione e i principi applicabili al settore privato rispetto ai quali recensisce le principali questioni giuridiche così come le principali tipologie di attori in funzione dei caratteri e dell'incidenza della loro azione.

Il rapporto A/HRC/35/22 è l'ultimo dei tre presentati in applicazione della risoluzione 25/2 del Consiglio dei Diritti Umani. In esso viene analizzato il ruolo svolto dai soggetti privati fornitori dell'accesso ad Internet e dei servizi di telecomunicazione ponendo particolare attenzione all'utilizzo di diverse forme di censura informatica volte ad impedire o dissuadere le persone ad esprimersi, così come agli ostacoli che incontra la libertà di espressione individuati nell'insufficienza delle infrastrutture di connessione, l'alto costo delle tariffe d'accesso poste dai poteri pubblici, le discriminazioni tra sessi e le barriere linguistiche.

In tale prospettiva, le raccomandazioni finali prendono in considerazione due aspetti relativi, da una parte, agli obblighi degli Stati di proteggere e promuovere la libertà di opinione e di espressione nello spazio informatico e, dall'altra, ai principi che gli attori privati devono rispettare per quanto riguarda i diritti dell'uomo.

Il Consiglio dei Diritti Umani, con la risoluzione A/HRC/RES/28/16 dell'aprile 2015, dà seguito alla richiesta dell'Assemblea Generale, di cui alla risoluzione 69/166, di proseguire lo studio delle tematiche relative alla tutela dei diritti umani nel cyberspace, delineando il mandato per uno special rapporteur che approfondisca i diversi aspetti legati al tema indicato.

In particolare, il Consiglio da mandato di raccogliere informazioni volte a delineare il quadro generale, a livello nazionale ed internazionale, relativo alle attività ed esperienze realizzate, agli studi condotti, agli sviluppi tecnici e alle problematiche correlate alla tutela del diritto alla privacy, delineando le opportune raccomandazioni al fine di implementarne la tutela. Per lo svolgimento di tale attività viene richiesto il coinvolgimento degli Stati, delle Nazioni Unite, delle Organizzazioni Internazionali operanti nel settore dei diritti umani oltre che delle associazioni civili e degli attori privati. Il Consiglio dei diritti umani, inoltre, chiede allo special rapporteur di integrare la tematica del rispetto del diritto alla privacy nella prospettiva gender.

Di particolare interesse l'ulteriore richiesta di presentare specifici report qualora vengano rilevate violazioni del diritto alla privacy e di porre all'attenzione dell'Alto Commissario per i Diritti Umani le violazioni ritenute particolarmente gravi.

Il mandato, di durata triennale, prevede, infine, che, a cadenza annuale, vengano presentati dei report sia al consiglio per i Diritti Umani sia all'Assemblea Generale.

Il primo di tali report, A/HRC/31/64, presentato nel 2016 al Consiglio dei diritti umani, esplicita le metodologie e la programmazione triennale del lavoro delineate dallo special rapporteur oltre ad una panoramica dei vari aspetti legati al diritto alla privacy rilevati all'inizio dell'anno 2016.

Nello stesso anno viene presentato all'Assemblea Generale, un secondo report, A/71/368, in cui viene indicato un gruppo di cinque priorità, definite *"Lignes d'action thématique (LAT)"*, relative a: i) Big data e open Data; ii) sicurezza e sorveglianza; iii) i dati sanitari; iv) i dati a carattere personale trattati dalle società private; v) una maggiore comprensione della nozione di privacy.

Lo studio delle singole questioni indicate viene affidato ad equipe specializzate di cui vengono indicate le prime attività svolte: l'organizzazione del forum internazionale sulla sorveglianza (IIOF 2016) tenutosi a Bucarest nel 2016, finalizzata a rilevare, con il contributo di agenzie di sicurezza e di commissioni parlamentari, le violazioni della vita privata e della libertà di espressione nella raccolta di informazioni, nonché le migliori pratiche che potrebbero migliorare le garanzie e i rimedi in questo settore; la discussione organizzata nello stesso anno a New York con lo scopo di approfondire la comprensione della nozione di privacy.

Il rapporto inoltre affronta alcune problematiche specifiche relative al diritto al silenzio, alla conservazione dei dati e alle attività di sorveglianza di massa e, infine, al contenuto della nozione di privacy.

In merito al primo tema viene posta la questione se i dati acquisiti su uno smartphone possono essere prodotti in tribunale e se il rischio di violazione della privacy sia troppo grande. La problematica è legata al contenzioso sorto tra Apple e FBI per l'accesso ai dati contenuti nei cellulari di soggetti sottoposti ad indagine federale[282]. L'attualità e la novità del problema non permettono allo special rapporteur di sviluppare osservazioni e raccomandazioni in merito se non quella di affrontare uno studio approfondito del tema.

Le attività di conservazione dei dati, di sorveglianza di massa e del ricorso crescente alla cifratura dei dati sono affrontate con riferimento alle attività legislative intraprese dalla Gran Bretagna e dalla Germania, rispetto alle quali si muovono osservazioni critiche evidenziandone, in

[282] F. MASSA, *Il caso San Bernardino: Apple vs FBI*, Sicurezza e Giustizia, Numero III del MMXVII.

generale, l'incidenza negativa sul diritto alla privacy in relazione ad una pluralità di aspetti.

Di particolare interesse le osservazioni svolte in merito all'ultima questione affrontata dal report relativa al contenuto del diritto alla privacy. Il rapporto muove da una pronuncia dell'Istituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) du Mexique nella quale si amplia il concetto di privacy inteso come spazio di libertà entro il quale l'individuo può sviluppare liberamente la propria personalità.

Viene infatti rilevato che "*si le droit à la protection des données personnelles relève, conformément aux règles constitutionnelles du pays, d'un droit autonome à la protection de la vie privée, il est nécessaire de proposer une interprétation plus large de ces deux concepts, selon laquelle le droit à la protection de la vie privée vise à assurer à l'individu un domaine où il peut développer librement sa personnalité"*[283].

In tale prospettiva la tutela della privacy implica ulteriori diritti e garanzie specifiche relativi alla conservazione dei dati, all'accesso ai dati personali così come regole riguardanti la protezione delle comunicazioni private, dei nomi e dell'integrità fisica e morale dell'individuo.

Nel terzo rapporto[284] presentato nel 2017 al Consiglio dei Diritti dell'Uomo, l'attenzione viene posta sulle attività di sorveglianza degli Stati osservate sia nella prospettiva nazionale che internazionale. Vengono esaminate le caratteristiche del quadro giuridico internazionale e l'interpretazione che ne viene data. Infine, vengono descritti i fatti e le tendenze più recenti oltre alle modalità di analisi dati e alla loro incidenza sull'esercizio del diritto alla vita privata e sui diritti connessi.

Il rapporto evidenzia, anche con riferimento alle dichiarazioni rese dall'analista dell'NSA statunitense Edward Snowden[285] e al conseguente dibattito, l'emergere di un quadro generale delle attività di sorveglianza caratterizzato da tendenze dissonanti con l'azione

---

[283] INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI) DU MEXIQUE, Sentenza, Expediente PPD.0050/16 del 13/07/ 2016,
[284] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/34/60
[285] Intervista rilasciata da Edward Snowden allla testata giornalistica The Gardian, consultabile all'indirizzo web https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

sviluppata dalle Nazioni Unite, così come da altri organismi regionali, volta ad accrescere il rispetto e la tutela dei diritti umani.

Viene richiamata anzitutto la Risoluzione 69/166 con la quale l'assemblea Generale domanda agli Stati di creare, o mantenere, meccanismi nazionali di controllo giudiziario, amministrativo o parlamentare indipendenti, efficaci, imparziali, dotati di mezzi sufficienti e di garantire, nella misura opportuna, la trasparenza e la responsabilità dei pubblici poteri nello svolgimento di attività di sorveglianza e di raccolta dei dati personali.

Il report richiama, inoltre, alcuni arresti giurisprudenziali delle corti regionali. In particolare una pronuncia della Corte europea dei Diritti dell'Uomo[286], nella quale vengono definiti obblighi chiari e vincolanti che i governi sono tenuti a rispettare nella definizione e nella realizzazione di attività di sorveglianza, e, una pronuncia della Corte di giustizia dell'Unione Europea[287] nella quale gli stati Membri vengono richiamati al loro dovere di rispettare, promuovere e proteggere il diritto alla privacy e gli altri diritti rilevanti nel contesto informatico.

Il report richiama due particolari passaggi della sentenza nei quali, da una parte, si evidenzia la gravità delle conseguenze sui diritti umani che possono derivare dalla legislazione in materia di intercettazioni e conservazione dei dati[288] e, dall'altra, si ribadisce come tali attività, seppur finalizzate alla tutela di rilevanti interessi pubblici rispetto ai rischi derivanti da attività criminali e terroristiche, deve ugualmente rispettare i principi generali posti a tutela dei diritti e delle libertà fondamentali della persona[289].

---

[286] Tra le molte, CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Roman Zakharov c. Russie*, 4 décembre 2015

[287] CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, *Tele 2 Sverige AB c. Post-och telestyrelsen*, 21 décembre 2016

[288] Per quanto riguarda l'obbligo giuridico dei fornitori di servizi di telecomunicazione di conservare i dati in massa, la Corte ha dichiarato che *"[l]'ingérence que comporte une telle réglementation dans les droits fondamentaux [...] s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constant".* La Corte ha inoltre evidenziato l'inceidenza che tale obbligo può avere sull'esercizio della libertà di espressione.

[289] Secondo la Corte: *"si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lute".*

Un quadro più dettagliato della situazione mondiale viene svolto richiamando i contributi di numerose organizzazioni civili operanti a livello nazionale e internazionale dalle quali emergono diffuse preoccupazioni circa le azioni di sorveglianza e di raccolta dati poste in essere in numerosi paesi[290].

Preoccupazioni condivise dallo Special Rapporteur il quale rileva espressamente che *"L'est profondément inquiétant de constater que malgré l'adoption de la résolution 69/166 et malgré des décisions telles que celles mentionnées au paragraphe 13 ci-dessus, le statut du droit à la vie privée dans le domaine de la surveillance n'a connu aucune amélioration depuis le dernier rapport du Rapporteur spécial. Les États qui sont passés à l'action ont élaboré et adopté de nouvelles lois en la matière qui apportent au mieux des améliorations mineures dans des domaines limités. De manière générale, ces lois ont été élaborées et adoptées en toute hâte pour légitimer des pratiques qui n'auraient jamais dû être mises en oeuvre"*[291].

Tra le attività e le tendenze che destano maggiori preoccupazioni il report pone in evidenza le modalità di elaborazione dei dati, caratterizzate da una generale mancanza di trasparenza.

Vengono dunque posti i problemi relativi alla definizione di criteri applicabili alla raccolta, conservazione, analisi e soppressione dei dati raccolti e, altri, relativi alle tecniche di anonimato e cifratura in quanto funzionali alla tutela dei diritti umani nei termini evidenziati dal Report A/HRC/29/32, sopra analizzato.

Le problematiche indicate vengono inoltre legate alla questione della dimensione transnazionale propria delle comunicazioni informatiche e delle attività connesse dalla quale, evidenzia il report, possono sorgere ulteriori lesioni dei diritti umani in termini di discriminazioni tra le persone fondate, tra le altre, sulla nazionalità, sulle origini, sull'età e sulla religione.

In senso positivo vengono invece accolte le iniziative, tra cui quelle poste in essere dal Consiglio d'Europa, volte a definire un quadro legislativo per le attività in oggetto, le quali prevedano strumenti di tutela quali, fra gli altri, specifiche forme di autorizzazione giudiziaria per lo svolgimento delle attività connesse al trattamento dei dati informatici.

---

[290] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/34/60, par. 14
[291] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/34/60, par. 15

Il report, infine, individua alcune temi generali su cui concentrare l'azione a livello internazionale: i) la necessità di internazionalizzare e armonizzare i termini e il linguaggio utilizzato; ii) la necessità di un dialogo aperto e riservato per comprendere meglio i sistemi nazionali, le loro somiglianze e differenze; iii) la promozione e la tutela dei diritti umani fondamentali per quanto riguarda i metodi utilizzati; iv) misure di salvaguardia e rimedi, preferibilmente a livello internazionale; v) responsabilità e trasparenza; vi) identificazione e analisi delle buone e cattive pratiche; vii) lo stato di avanzamento delle discussioni su come strutturare il controllo della vigilanza statale; viii) risposte a domande relative alla partecipazione del pubblico; ix) la necessità di coltivare meno segretezza e di essere più proattivi per spiegare le attività di sorveglianza dei servizi segreti e delle autorità incaricate dell'applicazione della legge; x) la necessità di più forum di discussione per lo sviluppo delle diverse tematiche.

Nel 2017 viene presentato all'assemblea generale un secondo report292 in cui vengono riportate le attività svolte e il lavoro della Big Data Open Data Taskforce creata dallo Special Rapporteur.

Le nuove metodologie di raccolta e analisi dei dati, aspetti centrali del fenomeno Big Data, e il sempre maggiore ricorso dei governi a forme di pubblicità, in forma anonima, dei dati personali in loro possesso al fine di generare crescita economica e stimolare la ricerca scientifica attraverso l'implementazione del fenomeno degli Open Data, pongono il problema, rilevato dal report, di ridefinire l'oggetto della nozione di privacy e le forme della sua tutela.

Una problematica che, con il riconoscimento effettuato dal Consiglio per i Diritti Umani[293] dell'essenzialità del diritto alla privacy per lo sviluppo della personalità dell'individuo, amplia la sua portata investendo il piano della tutela dei diritti umani.

Vengono tuttavia rilevate incertezze nella comprensione di come gli sviluppi tecnologici possono incidere sui vari aspetti di questa problematica.

Il report illustra le caratteristiche tecniche e le metodologie di analisi dei Big data, evidenziando come le modalità attraverso le quali le tecnologie ITC permettono agli individui di divenire conoscibili

[292] ASSEMBLEA GENERALE, *Rapporto* A/72/43103

[293] CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/34/L.7/ Rev.1, Agenda Item 3 Protection of all Human Rights Civil, Political Economic, Social and Cultural Rights including the Right to Development.

attraverso l'analisi dei loro dati implica che la natura stessa della persona venga considerata nella sua dimensione datizzata.

Entro questa prospettiva nota come lo sviluppo di tali fenomeni ponga in discussione alcuni principi elaborati sul piano internazionale. Vengono presi in considerazione i principi elaborati dall'OCSE nel 1980 nel documento Guidelines on the Protection of Privacy and Transborder Flows of Personal Data e i principi similari contenuti nel Data Protection Convention del 1980 del Consiglio d'Europa e, infine le Guidelines for regulation of computerized personal data files adottate dall'Assemblea Generale delle Nazioni Unite nel 1990.

Il principio di limitazione della raccolta, posto alla base delle norme OCSE e del Consiglio d'Europa, comporta che le informazioni personali devono essere raccolte in modo lecito ed equo e, se del caso, con la conoscenza e il consenso dell'interessato. L'ulteriore principio di limitazione delle finalità richiede che lo scopo della raccolta di informazioni personali sia specificato al momento della raccolta e che l'uso successivo delle informazioni sia limitato allo scopo della raccolta o a uno scopo compatibile e che questi siano specificati ogniqualvolta vi sia un cambiamento di finalità. Il principio di limitazione dell'uso limita la divulgazione di informazioni personali per scopi incompatibili, salvo con il consenso dell'individuo o dell'autorità giudiziaria. Il principio di minimizzazione dei dati è contestato dalla raccolta di grandi quantità di dati e dall'obbligo di trattare solo informazioni personali adeguate, pertinenti e non eccessive. Gli orientamenti delle Nazioni Unite del 1990 per la regolamentazione degli archivi di dati personali informatizzati pongono il principio di proporzionalità della conservazione dei dati rispetto alle finalità del trattamento dei dati[294].

Sul piano internazionale, inoltre, la nozione di privacy è estesa oltre le previsioni dei documenti indicati essendo legata, come visto, a ulteriori diritti fondamentali della persona.

Ora, le capacità di analisi offerte dai Big Data si pongono in contrasto con tali principi in ragione della possibilità di estrapolare informazioni personali a partire da dati diversificati e granulari. In questo senso la complessità dei Big Data è particolarmente legata alla categoria dei metadati i cui aspetti problematici, già oggetto di un precedente report, vengono qui ricondotti alla consapevolezza o meno da parte dell'utente di fornire determinate informazioni o che tramite

[294] ORGANIZZAZIONE DELLE NAZIONI UNITE, *Documento* E/CN.4/1990/72 del 1990.

essi si possano estrapolare informazioni ulteriori e diverse sulla sua sfera personale.

Nel 2018 lo Special Rapporteur presenta al Consiglio dei Diritti Umani, il terzo rapporto[295] elaborato conformemente alla risoluzione 28/16 esponendo un resoconto dell'attività svolta nel corso dei tre anni di lavoro e dei risultati ottenuti.

Nel report vengono riportati i risultati raggiunti rispetto alla questione della protezione della vita privata e alla sorveglianza esercitata dagli Stati e da attori privati nelle cinque aree tematiche indicate nelle *Lignes d'action thématique*. Inoltre, viene proposto il progetto per uno strumento giuridico internazionale in materia di sorveglianza informatica.

Quest'ultimo punto appare particolarmente interessante in ragione soprattutto dell'esplicito collegamento con i lavori, precedentemente visti, del Gruppo di Esperti Intergovernativi (GGE) istituito dall'Assemblea Generale per lo studio dei progressi dell'informatica e delle telecomunicazioni nel cotesto della sicurezza internazionale. Il rapporto concorda con essi nel sottolineare il legame tra la pace e la sicurezza internazionale, i diritti umani e lo sviluppo del cyberspace e come, per il suo sviluppo, occorra rafforzare la condivisione delle lezioni e delle pratiche apprese nella lotta all'uso delle ITC per scopi terroristici e criminali, sviluppando ulteriormente la cooperazione tra Stati e tra essi e il settore privato, al fine, da una parte, di prevenire e combattere l'uso illecito di tali tecnologie e, dall'altra, di garantire una maggiore effettività e tutela dei diritti umani e delle libertà fondamentali.

Entro questa prospettiva lo Special Rapporteur ribadisce la necessità di studiare misure volte a restringere la sorveglianze e altre attività lesive della privacy nel contesto informatico, nella convinzione che *"la cyberpaix dépend de la volonté et de la capacité des États à établir une synergie entre les intérêts en matière de sécurité et le respect de la vie privée dans le cyberespace"*[296].

A tal fine, il rapporto evidenzia come l'adozione da parte delle Nazioni Unite di uno strumento giuridico relativo alla sorveglianza e al diritto alla privacy possa favorire il perseguimento di due obiettivi strumentali al mantenimento della pace e della sicurezza internazionale.

---

[295] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/37/62

[296] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/37/62, par. 15

Il primo viene individuato nella definizione di un insieme di principi e di disposizioni che permettano di tradurre entro le legislazioni nazionali le norme fondamentali relativi ai diritti dell'uomo e di assicurarne l'applicazione, in particolare del diritto alla privacy, in relazione alla questione della sorveglianza informatica.

Il secondo obiettivo viene rintracciato nella definizione di una serie di azioni, elaborate sulla base delle migliori pratiche internazionali, che permettano di conciliare gli interessi in materia di sicurezza, le necessità legate alle attività di sorveglianza e la protezione del diritto alla vita privata.

Il progetto descritto nel rapporto consiste in un testo elaborato nel corso di diverse attività e consultazioni pubbliche dove vengono stabiliti alcuni principi generali a partire dai quali vengono definiti i requisiti fondamentali per la realizzazione di attività di sorveglianza informatica così come per i relativi sistemi e dati. Inoltre, si occupa di definire il suo campo di applicazione, i diritti da esso protetti, le modalità di collaborazione tra più parti interessate e i meccanismi di accesso transfrontaliero ai dati personali[297].

Nel corso del 2018 il rapporteur presenta all'Assemblea Generale un secondo rapporto298 nel quale espone le attività realizzate durante l'anno e presenta la seconda parte del lavoro svolto in materia di Big Data e Open Data attraverso delle consultazioni pubbliche.

Il dibattito in materia ha preso in considerazione vari aspetti: le origini e l'uso dei Big data e degli Open Data; i potenziali benefici e i danni che possono causare; l'impatto dell'uso dei personal data su altri diritti umani; l'adeguatezza delle tecniche di de-identificazione; le buone pratiche nell'uso dei dati personali; l'importanza dei diritti umani e di riferimenti etici nello sviluppo di tecnologie in grado di svolgere autonomamente processi decisionali; la sovranità sui dati indigeni; questioni relative alla tutela dei consumatori e di genere; le prospettive sviluppate da paesi non Europei.

La parte più rilevante delle discussioni ha tuttavia riguardato le conseguenze sul diritto alla privacy derivanti dall'interazione tra Open Data e Big Data.

[297] CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/37/62, allegato 7
[298] ASSEMBLEA GENERALE, *Rapporto* A/73/45712

Capitolo IV

Modelli di governance nel dominio informatico

Introduzione; 1. L'influenza dei caratteri del Cyberspace sulle forme di governance; 1.1 Dal sistema multilaterale al sistema multistakeholder; 2. Il modello multistakeholder; 2.1 Il sistema della governance tecnica di Internet; 3. La pluralità dei regimi di governance; 3.1 Principali regimi normativi che compongono la disciplina giuridica del cyberspace: 3.2 L'azione normativa degli attori privati

Introduzione.

L'analisi svolta nel precedente capitolo permette di evidenziare i tratti più rilevanti delle problematiche poste dall'affermarsi del cyberspace e della forma di governance di questo peculiare spazio delle relazioni internazionali.

Nei diversi documenti presi in considerazione, si afferma l'idea che vi siano interessi riconducibili alla Comunità Internazionale[299], la cui tutela e promozione è affidata tanto agli Stati quanto agli attori privati[300], entro strutture istituzionali, prospettive politiche e procedure,

[299] Dai documenti presi in considerazione emerge il riconoscimento della dimensione internazionale degli interessi coinvolti nelle dinamiche del cyberspace. Possiamo infatti rilevare come l'Assemblea Generale delle Nazioni Unite affronti il tema del ruolo della scienza e della tecnologia nel contesto della sicurezza internazionale consapevole, da una lato, delle possibilità di progresso offerte e delle problematiche legate alla sua duplice natura civile e militare e, dall'altro che *"la diffusion et l'emploi de la téléinformatique intéressent la communauté internationale tout entière et qu'une vaste coopération internationale contribuera à une efficacité optimale" (A/RES/53/70).* Allo stesso modo, rispetto ai rischi legati all'uso criminale delle tecnologie informatiche, riconosciuta l'importanza della libera circolazione delle informazioni nello sviluppo economico e sociale e nella governance democratica, l'Assemblea nota come *"le recours aux technologies de l'information, qui peut varier d'un État à l'autre, a entraîné un accroissement considérable de la coopération et de la coordination au niveau mondial, ce qui implique que l'exploitation des technologies de l'information à des fins criminelles peut avoir des répercussions graves pour tous les États"* (A/RES/55/63).

[300] Nella prospettiva delle Nazioni Unite, Stati e attori privati, sono tenuti a *"coopérer pour lutter contre l'exploitation des technologies de l'information à des fins criminelles" (*.A/RES/55/63) Particolarmente indicativi, inoltre, appaiono i richiami svolti in sede di dibattito sui sistemi LAWS alla necessità di trovare un equilibrio tra la tutela di interessi e valori fondamentali e la necessità di preservare il dinamismo del progresso tecnologico legato, da un lato, alla libertà di ricerca scientifica e, dall'altro, alla sua applicazione civile e militare..

elaborate nel contesto dei diversi ordinamenti entro i quali si sviluppa la cooperazione internazionale[301].

Allo stesso tempo sul piano normativo viene in evidenza l'importanza attribuita ai principi e alle norme di diritto internazionale alle quali si affiancano tanto norme secondarie volte ad aumentare la fiducia tra gli Stati nei reciproci rapporti quanto le norme elaborate attraverso procedimenti dove è sempre più rilevante il ruolo di attori privati.

Nel contesto del cyberspace l'importanza delle Nazioni Unite è dunque legata alla sua capacità di unificare le differenti problematiche entro una prospettiva e un'azione globale che confluiscono nella Società dell'Informazione, a sua volta, elemento essenziale per la realizzazione della più ampia agenda delle Nazioni Unite[302]. Un'azione

[301] I documenti analizzati, permettono di ricondurre la cura dei diversi interessi a specifiche istituzioni. La tutela del preminente interesse alla pace e alla sicurezza internazionale rispetto all'utilizzo delle tecnologie ITC da parte degli Stati viene infatti perseguita dalle Nazione Unite e, in particolare, dall'Assemblea Generale alla quale può essere ricondotto il lavoro di rilevazione e definizione delle problematiche del cyberspace svolto dai Gruppi di Esperti Intergovernativi. La specifica problematica delle armi letali autonome viene affrontata dalle Alte Parti Contraenti della Convenzione delle Nazioni Unite del 1980 sulla proibizione o limitazione dell'uso di alcune armi convenzionali che possono essere dannose o aventi effetti discriminanti (CCW – Convention in Certain Weapons) le quali sviluppano la propria azione dapprima attraverso meeting informali di esperti e, successivamente definendo il mandato e le procedure di un gruppo di esperti governativi. Allo stesso modo l'azione volta al contrasto dell'utilizzo criminale delle tecnologie dell'informazione può essere ricondotta alla Commissione per la prevenzione del crimine e la giustizia penale delle Nazioni Unite, la cui attività si sviluppa fornendo supporto diretto agli Stati e, in una prospettiva di lungo periodo, attraverso i lavori del World Summit on the Information Society, nei quali trova fondamento l'Internet Governance Forum. A quest'ultimo può essere ricondotta l'ulteriore azione delle Nazioni Unite volta alla tutela delle infrastrutture essenziali del cyberspace. I diversi organismi, inoltre, non operano in maniera isolata come evidenziano i numerosi richiami ai reciproci studi e affermazioni contenuti nei documenti considerati. Nel campo della tutela della sicurezza e della pace internazionali vengono richiamate le dichiarazioni di Conferenze Internazionali e le misure regolamentari adottate da specifici enti internazionali. Diversamente, il tema della lotta all'uso criminale delle tecnologie informatiche mette in evidenza i reciproci richiami tra l'azione universale delle Nazioni Unite e quella svolta da organizzazioni internazionali di carattere regionale e l'azione di carattere nazionale degli Stati. Particolari, infine, i rapporti che si creano nel campo della tutela delle infrastrutture essenziali dove rivestono una fondamentale importanza la collaborazione tra il settore pubblico e quello privato della ricerca, dell'industria, delle associazioni. Il sistema multilaterale acquisisce di conseguenza un carattere interdisciplinare rispecchiando la natura dei processi di ricerca e sviluppo del cyberspace e favorendo la comprensione delle problematiche emergenti e una loro più efficace governance.

[302] I documenti analizzati mostrano come gli attori del cyberspace attribuiscano all'Organizzazione delle Nazioni Unite una funzione di sintesi e definizione delle problematiche e delle relazioni di carattere globale. In tal senso si esprimono gli Stati che, pur tendendo a riportare le questioni di natura tecnica o strategica entro enti internazionali di livello regionale o specialistico, riconoscono alle NU un ruolo di sintesi delle problematiche e di definizione di principi e norme, così come di coordinamento dello sviluppo delle relazioni

multilaterale volta ad affrontare le problematiche riconducibili alle tre aree tematiche della sicurezza e della pace internazionale, del contrasto alle attività di cybercrime e della sicurezza delle infrastrutture e, infine, della tutela e promozione dei diritti umani e delle libertà fondamentali nel contesto dei mutamenti determinati dalle nuove tecnologie.

Ogni linea di azione sviluppa una precisa tematica attraverso forme di governance caratterizzate dall'adozione di procedure e strumenti sviluppati entro un modello di cooperazione multilaterale che muove dalla rilevazione, analisi e definizioni delle diverse problematiche, per giungere alla composizione di un equilibrio nel confronto tra i diversi interessi attraverso principi e norme di diritto internazionale.

L'analisi dei lavori delle Nazioni Unite, tuttavia, non esaurisce il tema della forma di governance che si va affermando rispetto al dominio informatico. Tale attività costituisce infatti, solo una parte di un più articolato e vario sistema di governance multilaterale e multistakeholder, la cui attuale rilevanza è ben espressa dalle indicazioni finali del GGE del 2015 e del 2018 le quali delineano la necessita di sviluppare la partecipazione degli attori non statali all'interno dei processi di governance delle diverse tematiche caratterizzanti il cyberspace.

Rispetto al tema ora indicato, nei successivi paragrafi, verranno approfondite le questioni attinenti: a) all'influenza dei caratteri del cyberspace rispetto allo sviluppo dei modelli di governance; b) all'affermazione del modello di governance multistakeholder; c) ai principali regimi normativi che compongono la disciplina giuridica del cyberspace.

rispetto alle varie tematiche. Allo stesso modo i Gruppi di Esperti hanno in più occasioni riconosciuto la capacità dei diversi fori di discussione creati nel contesto delle Nazioni Unite di favorire lo sviluppo della cooperazione rispetto alle diverse tematiche. La centralità dell'Organizzazione delle Nazioni Unite nel sistema delle relazioni multilaterali legate all'emergere del cyberspace viene in evidenziata anche dalla prospettiva di lungo periodo attribuita alla sua azione sviluppata attraverso la Commissione per la prevenzione del crimine e la giustizia penale, il World Summit Information Society, l'Internet Governance Forum oltre che dalla sempre più ampia partecipazione dei diversi stakeholders favorita dall'apertura che caratterizza le procedure di lavoro adottate.

1. *L'influenza dei caratteri del Cyberspace sulle forme di governance.*

Il confronto tra il sistema di relazioni determinato dal cyberspace e il sistema al quale sono informate le relazioni internazionali, permette di evidenziare, anzitutto, come il primo sia un sistema recente ed estremamente mutevole che trova la sua origine nell'affermazione della scienza e della tecnica, differentemente dal secondo fondato sul processo di definizione e affermazione degli Stati dal quale discendono principi e norme il cui sviluppo fa propri i tempi lunghi della storia[303].

[303] Il sistema multilaterale delle relazioni internazionali è, da questo punto di vista, il risultato dei processi di affermazione e sovvertimento di strutture di potere in grado di governare le relazioni tra soggetti statali. Un'alternanza segnata dall'adozione nei diversi momenti di forme e strutture di carattere centralizzante o decentralizzante e che trova il suo avvio con il venir meno della capacità unificante delle relazioni sociali propria del Diritto Romano. Una funzione che tale sistema giuridico continuerà tuttavia ad esercitare nel periodo dei regni romano barbarici, frammentato e decentrato e al contempo ispirato dall'idea dell'unità imperiale romana. Nella successiva fase feudale la naturale tendenza verso l'edificazione di un potere centrale si esprime nella lotta tra i due centri di autorità della Chiesa cattolica, con a capo il Papa, e del Sacro Romano Impero, con a capo l'Imperatore. Il confronto tra i due attori è stato tuttavia risolto dal progressivo affermarsi di due fenomeni storici che hanno minato le fondamenta di entrambi i poteri. Da un lato la scoperta del Nuovo Mondo altera l'equilibrio di interessi esistente favorendo l'emergere di nuovi elementi determinanti la potenza, ridimensionando, in tal modo, il valore dei possedimenti territoriali quale fattore legittimante l'autorità temporale dell'Imperatore. Dall'altro lato, una medesima efficacia può essere attribuita al propagarsi della Riforma protestante che, affermando una nuova prospettiva religiosa, priva la Chiesa cattolica del fattore unificante spingendo gli Stati dove la Riforma si era maggiormente affermata a negare, sul piano giuridico, la preminenza riconosciuta al vescovo di Roma. Entrambi i fattori di rivoluzione poggiano su processi di innovazione della scienza e della tecnica a cui abbiamo visto potersi ricondurre il più ampio fenomeno di affermazione del pensiero scientifico che sorregge la costruzione del cyberspace. Le scoperte geografiche, infatti, sono state rese possibili dallo sviluppo della tecnica navale e della scienza astronomica e hanno determinato l'avvio della globalizzazione dei rapporti internazionali. Allo stesso modo sono state le innovazioni tecniche della stampa che hanno favorito l'affermazione tanto della Riforma quanto di un rinnovato pensiero scientifico grazie alla diffusione del libro, il quale abbiamo visto porsi alla base dei sistemi di creazione, trasmissione, conservazione e manipolazione delle informazioni. Ad essi può dunque ricondursi l'avvio della globalizzazione degli spazi e della conoscenza: entrambi svincolati dalla dimensione europea (territoriale) e religiosa (ideale) potranno svilupparsi in nuove dinamiche storiche, che troveranno la definizione del loro equilibrio nella Pace di Westfalia. In tale occasione vennero infatti definiti i principi e i fattori strumentali all'affermazione del Principio di Equilibrio che informa i rapporti tra entità sovrane a partire dalla Pace di Lodi delineando lo schema entro cui si svilupparono i rapporti tra entità sovrane fino ai due conflitti mondiali. Principi e fattori che troveranno in questo momento nuova definizione. Durante il successivo confronto bipolare, il nuovo ordine mondiale incentrato sul principio di cooperazione, trova una sua fase di definizione e consolidamento. Ad essa segue un momento di sviluppo legato al rinnovato vigore del generale processo di globalizzazione delle relazioni internazionali durante il quale il sistema

L'affermarsi del cyberspace quale peculiare spazio di relazione incide, come abbiamo visto nel capitolo secondo, sui fattori costituenti il Cyberpower determinando l'evoluzione delle dinamiche politiche della cooperazione tra attori internazionali[304]. Come è stato osservato *"the global, often nontransparent interconnections afforded by cyberspace have challenged the traditional understanding of leverage and influence, international relation and power politics, national security boundaries – as well as a host of other concept and their corresponding realities"*[305].

Sintetizzando quanto precedentemente osservato in una prospettiva di teoria politica, possiamo rilevare come il cyberspace incida sia rispetto ai caratteri e alla dinamica dei fatti politicamente rilevanti, sia rispetto agli attori e alla loro azione. In questa prospettiva l'*informazione* influisce sulla dimensione temporale[306] degli eventi iscrivendoli in una sostanziale istantaneità, attribuendogli al contempo una dimensione globale slegata dai limiti geografici e determinandone, infine, la rilevanza politica all'interno di confini e ordinamenti diversi da quelli di origine. Eventi e dinamiche politiche che si sviluppano, inoltre, in un contesto fluido, in continua riconfigurazione, quale è il cyberspace. Rispetto agli attori politici e alla loro azione il cyberspace, riducendo le barriere all'espressione e all'azione politica, favorisce la partecipazione di nuovi attori. Allo stesso tempo, tuttavia, le difficoltà di attribuzione delle azioni condotte nel cyberspace ostacola la rilevazione degli attori e delle loro azioni determinando, inoltre, il venir meno dell'effettività dei meccanismi di responsabilità.

In altri termini il cyberspace introduce nuovi fattori di complessità rispetto alla rilevazione ed elaborazione politica delle fondamentali questioni di chi fa cosa, come e quando[307].

---

di relazioni internazionali definisce la sua struttura, ampliando al contempo le sue competenze e l'effettività della sua azione, entro i modelli del multilateralismo.

[304] Allo stesso modo, quale fattore di progresso, il suo sviluppo incide, rispetto ad una pluralità di elementi, sulle strutture e sul processo di sviluppo della società ponendo in discussione sia i fondamenti sostanziali dei poteri pubblici quanto le finalità dell'azione di governo a cui sono preordinati. Si rinnova dunque, da un lato, il problema di comprendere in quale misura i progressi scientifici e tecnologici possono determinare mutamenti negli elementi sostanziali che sorreggono i poteri pubblici così come nei fattori rilevanti per le relazioni tra attori internazionali. Da altro punto di vista si pone il problema di definire nuovi e più attuali modelli di governance.

[305] NAZLI CHOUCRI, *Cyberpolitics in International Relation*, The MIT Press, 2012, p. 3

[306] TIM STEVENS, *Cybersecurity and the Politics of Time*, Cambridge University Press, 2017

[307] H. D. LASSWELL, *Politics: who gets what, when and how*, McGraw-Hill, New York, 1958;

Entro questa prospettiva, vengono posti in discussioni i riferimenti finora sviluppati nell'ambito della teoria delle relazioni internazionali. Gli approcci tradizionali si occupano di studiare i fattori determinanti il potere e il suo esercizio entro un paradigma centrato, inizialmente, sull'uomo e i suoi caratteri sociali e, successivamente, esteso a ricomprendere le relazioni con il contesto entro cui gli attori politici interagiscono. Oggetto della teoria realista delle relazioni internazionali è la sicurezza nazionale, la politica di potenza e i conflitti di tipo tradizionale entro rapporti di tipo puramente interstatali. Allo stesso modo la teoria istituzionalista sviluppa i meccanismi, formali e informali, di cooperazione e coordinamento secondo una logica stato centrica volta a regolamentare le relazioni tra soggetti statali. Il costruttivismo infine ritrova i fondamenti delle relazioni internazionali nei caratteri propri della società internazionale per la quale il conflitto è strumento predisposto allo svolgimento delle relazioni tra i suoi membri.

Tali teorie, al di là delle differenze, hanno favorito una migliore comprensione della politica internazionale attraverso lo studio degli aspetti sociali, economici, politici e strategici rilevanti nei sistemi statali. Diversamente una minore attenzione è stata rivolta al ruolo, oggi sempre più rilevante, degli attori non statali. Allo stesso modo l'analisi teorica si è concentrata sugli aspetti statici anziché sulla dinamica di trasformazione trascurandone gli effetti di breve e lungo periodo. Inoltre, il processo di globalizzazione non ha favorito l'affermarsi di un solido consenso in merito alle principali teorie delle relazioni internazionali[308].

La *cyberpolitics* pone tuttavia, nuove e complesse questioni relative alle interconnessioni tra i sistemi di interazione (non solo tra i sistemi sociali e ambientali ma anche con il sistema cyber); alle dinamiche di trasformazione e cambiamento; alla definizione del ruolo di nuovi attori ed entità sia nella teoria che nel sistema delle relazioni internazionali.

Come è stato osservato *"the construction of cyberspace is clearly a globalizing phenomenon, irrespective of how one views the globalization process itself. Its organization and management are under the control of a wide range of non-state actor, and its properties differ significantly from those of the social system and the environmental system. Cyber-based interactions are already recognized to influence human activities at all levels of analysis.*

[308] NAZLI CHOUCRI, *Cyberpolitics in International Relation*, The MIT Press, 2012

Consequently, the sovereign state, the anchor of traditional theory, finds itself in an increasingly complex international system, far different from the structure of the nineteenth century and most of the twentieth century"[309].

1.1 Dal sistema multilaterale al sistema multistakeholder.

Alla fine dei conflitti mondiali del secolo scorso si fa risalire[310] l'avvio di un nuovo processo di trasformazione della Comunità Internazionale e del suo ordinamento giuridico. Un processo caratterizzato dal maggior ruolo progressivamente assunto da enti sovranazionali e dalla maggiore attenzione del diritto internazionale all'azione dei poteri statali in ambiti tradizionalmente ascritti alla sfera della Sovranità interna, come tale sottratta alla disciplina giuridica internazionale.

A partire da questo momento, il sistema delle relazioni internazionali si sviluppa nella prospettiva del decentramento attraverso la creazione di una pluralità di enti sovranazionali a carattere regionale e tecnico che hanno favorito la diffusione del potere tra una pluralità di attori garantendo finora la stabilità e la sicurezza internazionali e con essi il progresso della Società Internazionale[311].

Sul piano teorico, tale dinamica di sviluppo delle relazioni internazionali viene ricondotta all'idea di multilateralismo a partire dall'ultimo decennio del secolo scorso.

---

[309] NAZLI CHOUCRI, *Cyberpolitics in International Relation*, The MIT Press, 2012, p. 16

[310] HOBSBAWM, *Age of extremes. The short twentieth century 1914-1991*, Penguin Books, 1994; E. DI NOLFO, *Storia delle relazioni internazionali. Dal 1918 ai giorni nostri*, Editori Laterza Roma-Bari 2011.

[311] La Comunità Internazionale, fino alla metà del secolo scorso espressione degli Stati europei e del loro modo di condurre le relazioni interstatali definiti tra Lodi e Westfalia, assume, a partire dalle due guerre, una vocazione e una dimensione sempre più universale per la pluralità degli interessi e degli attori rilevanti sul piano delle relazioni internazionali. Al principio dell'equilibrio di potenza, su cui si basavano i rapporti tra i pochi Stati europei, viene quindi a sostituirsi il principio della collaborazione più aderente ai nuovi caratteri della Comunità Internazionale. Tale principio ha trovato concretizzazione soprattutto nella creazione di ordinamenti giuridici sovranazionali sui quali poggia il sistema multilaterale delle relazioni internazionali. Rispetto a quest'ultimo, la Società delle Nazioni prima, e le Nazioni Unite poi, rappresentano il punto centrale di un sistema istituzionale volto alla cooperazione internazionale la cui struttura di base può farsi coincidere con le organizzazioni create a Bretton Woods: la Banca Mondiale, il FMI e il sistema del commercio internazionale allora costituito dalla GATT1947.

Generalmente inteso come *"la pratica di coordinare le politiche nazionali in gruppi di tre o più Stati"*[312] il concetto di multilateralismo è stato progressivamente approfondito nella sua dimensione qualitativa e sostanziale.

Rispetto alla prima è stato evidenziato come il multilateralismo *"is an institutional form which coordinates relations among three or more States on the basis of generalized principles of conduct"*[313].

Rispetto al secondo aspetto, ai mutamenti strutturali della Comunità Internazionale ha fatto seguito, come noto, un processo di evoluzione del suo ordinamento giuridico. Da diritto della mera coesistenza pacifica volto a regolare le relazioni esterne degli Stati, esso si è trasformato in diritto della cooperazione tra Stati prestando, di conseguenza, una maggiore attenzione all'azione dei poteri pubblici Statali nella loro dimensione nazionale nella misura in cui questi incidano su interessi riconducibili ad altri Stati o alla Comunità Internazionale in quanto tale[314].

Da questo punto di vista, occorre rilevare come le crudeltà dei due conflitti mondiali abbiano reso evidente l'esistenza di valori di cui la

---

[312] ROBERT O. KOANE, *Multilateralism: An Agenda for Research*, International Journal 45 (Autumn 1990), p. 731

[313] JOHN GERARD RUGGIE, *Multilateralism: The Anatomy of an Institution*, International Organization, Vol. 46 no.3 (Summer, 1992) pp. 561-598, The MIT Press, 1992)

[314] Il diritto internazionale generale, si basa su un'idea secondo la quale il contenuto normativo è costituito da un insieme di limiti all'uso della forza da parte degli stati che possono riguardare sia la c.d. forza internazionale, sia la c.d. forza interna, intesa come potere di governo esplicato sugli individui. In particolare, si ritiene che *"il potere di governo così come limitato dal diritto internazionale sia costituito da qualsiasi intervento concreto di organi statali, sia avente esso stesso natura coercitiva sia in quanto, e solo in quanto, suscettibile di essere coercitivamente attuato. In questo senso può dirsi che il diritto internazionale pone dei limiti alla forza interna degli stati"* (BENEDETTO CONFORTI, *Diritto Internazionale*, Editoriale Scientifica, Napoli, 2002, pag. 193; in generale sul contenuto del diritto internazionale si veda tra i molti: R. QUADRI, *Diritto internazionale pubblico*, V° Ediz. Napoli 1968; MANN, *The doctrine of Jurisdiction in International Law*, RC, 1964 I, 9 ss.; AMERICAN LAW INSTITUTE, *Restatement of the Law. The Foreign Relations of The United States*, St. Paul Minn., 1987 Vol I; PICONE, *L'applicazione extraterritoriale delle regole sulla concorrenza e il diritto interno e internazionale*, Padova, 1989, 81 ss.) Il diritto internazionale inteso come una serie di limiti all'autorità di governo permette di fornire uno schema all'interno del quale inserire le norme materiali internazionali diverse da quelle che si occupano della forza internazionale. Tuttavia, non spiega lo sviluppo, iniziato dopo la Seconda guerra mondiale e accentuatosi con il fenomeno della globalizzazione, di convenzioni internazionali che perseguono valori di cooperazione e solidarietà (CONDORELLI, SCHW. J, 1990. Citato in B. CONFORTI, op. cit. pag. 197). Soprattutto, per quanto qui interessa, non spiega la capacità delle norme predisposte dai sistemi regolatori globali di incidere finanche sulla discrezionalità amministrativa degli stati

società internazionale avverte la necessità di garantirne la tutela[315]. Allo stesso modo l'aumento delle relazioni globali tra i diversi attori, statali e non, all'interno del più ampio fenomeno della globalizzazione, ha fatto emergere nuove problematiche di dimensione transnazionale. Questioni particolarmente rilevanti quali la tutela dell'ambiente, la tutela del lavoro, la protezione dei beni culturali, la gestione dei flussi migratori vengono affrontate dagli Stati[316] all'interno degli ordinamenti giuridici delle diverse organizzazioni internazionali le quali si pongono quali *"poteri pubblici globali"*[317]. In altri termini, laddove all'organizzazione internazionale è affidata in misura sempre maggiore la determinazione degli obiettivi e dei metodi di tutela di un interesse riconducibile alla Comunità Internazionale, quali sono la sicurezza e il progresso internazionale, gli Stati sono chiamati ad agire, nel perseguimento dei loro interessi nazionali, coerentemente con gli scopi dell'organizzazione di riferimento ed entro il quadro giuridico ad essa riconducibile.

Attualmente, tuttavia, il sistema multilaterale sembra progressivamente perdere la sua capacità di sostenere le sempre più complesse relazioni tra attori internazionali[318].

Entro questa fase di sviluppo del sistema multilaterale, il carattere aperto e integrato proprio delle tecnologie informatiche, determina un

---

[315] ANTONIO CASSESE, *L'apertura degli ordinamenti nazionali all'ordinamento della Comunità Internazionale*, collana Lezioni Magitrali dell'Università degli Studi Suor Orsola Benincasa, Facoltà di Giurisprudenza, Edizione Scientifiche, Napoli.

[316]Il rapporto tra gli Stati e il sistema delle relazioni internazionali si è sviluppato progressivamente durante il secolo scorso. Rispetto ad esso già Santi Romano osservava come non si potesse escludere *"a priori che gli Stati, o anche solo taluni (...) non debbano col tempo, più che svolgersi, rimanere in un certo senso, compresi e forse assorbiti in maggiori organizzazioni non propriamente statuali"* (SANTI ROMANO, *Discorso inaugurale dell'anno accademico 1917-1918*). Successivamente M.S. Giannini sottolineava come vi erano *"amministrazioni internazionali in numero crescente" che comportavano il mutamento del "quadro di riferimento"* (M. S. GIANNINI, *Il pubblico potere*, Bologna 1985 pp. 12 e 138) Attualmente si osserva *"che gli Stati sono condizionati da fatti economici e sociali che non possono influenzare, almeno non in modo determinante" e " per porvi rimedio, almeno in parte, hanno creato nuovi poteri pubblici ultra statali"* (G. DELLA CANANEA *Legittimazione e accountability nell'organizzazione mondiale del commercio*, Riv. Trim. Dir. Pubb. Pag 732; Cfr. anche S. CASSESE, *La crisi dello Stato*, Bari-Roma 2002, dello stesso Autore, *Lo spazio giuridico globale*, Bari- Roma 2003).

[317] In generale sullo sviluppo dei poteri pubblici globali, tra i molti, si vedano: STEFANO BATTINI, *La globalizzazione del diritto pubblico*, Riv. Trim. Dir. Pubb. N. 2/2006; G. DELLA CANANEA, *I pubblici poteri nello spazio giuridico globale*, Riv. Trim. Dir. Pubb. N 1/2003; S. BATTINI, *L'impatto della globalizzazione sulla pubblica amministrazione e sul diritto amministrativo: quattro percorsi*, Giornale di diritto amministrativo n. 3/2006

[318] HARLAN GRANT COHEN, *Multilateralism's Life Cycle*, The American Society of International Law, 2018, doi:10.1017/ajil.2018.11;

ulteriore processo di sviluppo delle relazioni internazionali caratterizzato dall'emergere di nuove dinamiche di relazione e di nuovi attori da cui nuovi modelli di cooperazione multilaterale e di processi normativi di tipo multistakeholder.

2. Il modello multistackeholders.

Il modello multistakeholder può essere definito come *"two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules"*[319].

Esso si presenta articolato in diverse forme in base alla varietà degli attori coinvolti e alla natura delle relazioni tra essi sviluppate.

Rispetto agli attori, questi possono essere raggruppati in quattro classi: Stati, organizzazioni intergovernative, industrie e società civile[320]. Occorre tuttavia notare come al loro interno possono essere svolte ulteriori specificazioni. Rispetto agli Stati vengono in evidenza le autorità regolatorie indipendenti, identificabili come una specifica classe di attori in ragione della loro partecipazione a network internazionali fondamentali in molti settori della governance globale. Allo stesso modo vengono in rilievo diverse tipologie di imprese, pubbliche o private, nazionali o transnazionali o espressione di diversi e, talvolta, contrapposti settori produttivi. Infine, tra gli attori civili, vengono in rilievo le ONG, i movimenti e le reti sociali e, infine, gli stessi individui attraverso la loro attività privata.

Allo stesso modo possono essere individuati quattro modelli ideali di governance: il modello gerarchico, i modelli di poliarchia eterogenea ed omogenea e, da ultimo, il modello anarchico.

Tuttavia, sono le due forme di poliarchia a meglio rispondere ai caratteri del cyberspace e delle relazioni che vi si sviluppano.

Si può infatti osservare come il modello anarchico, notoriamente posto alla base della teoria delle relazioni internazionali, presenti, come

---

[319] MARK RAYMOND, LAURA DENARDIS, *Multi-stakeholderism: anatomy of an inchoate global institution*, in GLOBAL COMMISSION ON INTERNET GOVERNANCE, *Who runs the Internet? The global Multi-stakeholder model of Internet governance, Research Volume Two*. Degli stessi Autori, Thinking clearly about Multistakeholder Internet Governance, Paper presented at Eight Annual GigaNet Symposium, Bali, Indonesia, October 21, 2013.

[320] JEFFREY S. HARRISON, JAY B. BARNEY, R. EDWARD FREEMAN AND ROBERT A. PHILLIPS, *The Cambrige Handobook of stakeholder theory*, Cambridge University Press, 2019

rilevato dai più recenti studi[321], diversi livelli di autorità determinati dalla necessità di individuare norme procedurali funzionali allo sviluppo delle relazioni tra gli attori. Nonostante in tale modello l'autorità appaia egualmente e simmetricamente suddivisa tra gli attori ciò, come è stato osservato, *"should not be mistaken for the absence of autority*"[322]. L'attributo dell'autorità può, infatti, essere riconosciuto anche alle norme procedurali definite e accettate dagli stessi attori al fine di disciplinare l'azione reciproca.

Entro questa prospettiva, la rilevanza degli attori privati nel domino informatico, introduce, come abbiamo visto, nuovi elementi di complessità che rendono il modello anarchico non coincidente con le particolarità della cyberpolitics. Allo stesso modo il modello strettamente gerarchico costringe gli attori privati nella posizione di rule-taker la quale, tuttavia, non rispecchia la reale azione di rule-maker da essi svolta nel dominio informatico.

Alle peculiarità del cyberspace meglio si adattano i modelli di tipo poliarchico a cui generalmente si riconducono i modelli di cooperazione multistakeholder. Due fondamentali caratteri di tali modelli sono, infatti, la rappresentatività dei diversi interessi economici e sociali e l'attribuzione alla società civile di una funzione rappresentativa affianco ai governi e alle industrie. Allo stesso modo il carattere aperto, che abbiamo visto esser proprio della cultura scientifica alla base del cyberspace, sostiene l'elaborazione di processi di partecipazione, più o meno ampia, che caratterizzano i modelli multistakeholder. Ugualmente, la rilevanza al contempo globale e locale delle tecnologie ITC, si riflette nell'azione condotta dagli attori sia in una prospettiva internazionale che con riferimento a tematiche prettamente nazionali.

Altri caratteri qualificanti i modelli multistakeholder possono essere individuati nei processi di output, nelle relazioni con i poteri Statali,

---

[321] JASON C. SHARMAN, *International Hierarchies and Contemporary Imperial Governance: A Tale of Three Kingdoms*, European Journal of International Relations, 19 (2): 189-207, 2013; EDWARD KEEN, *A Case Study of the Construction of International Hierarchy: British Treaty-Making against the Slave Trade in the Early Nineteenth Century*, International Organization 61 (2): 1077-90, 2007; JOHN M. HOBSON, JASON C. SHARMAN, *The Enduring Place of Hierarchy and Political Change*, European Journal of International Relations 11 (1): 63-90, 2005; IAN HURD, *Legitimacy and Authority in International Politics*, International Organization 53 (2): 379-408, 1999;

[322] MARK RAYMOND, LAURA DENARDIS, *Multi-stakeholderism: anatomy of an inchoate global institution*, in GLOBAL COMMISSION ON INTERNET GOVERNANCE, *Who runs the Internet? The global Multi-stakeholder model of Internet governance, Research Volume Two,* p. 23

nella definizione delle tematiche rilevanti e nel coordinamento dell'azione condotta dai vari attori.

Rispetto al primo punto si può osservare come tali modelli, attraverso una varietà di procedimenti, possano determinare diverse tipologie di outputs. In alcuni casi essi gestiscono effettivamente le risorse tecniche delle infrastrutture informatiche. In altri il prodotto di output consiste nella definizione di standard, best practices e codici di condotta.

Altrettanto varie sono le tipologie di relazione che si instaurano tra i modelli multistakeholder e i governi. In alcuni casi tali procedimenti ed organizzazioni derivano i loro poteri dagli stessi governi, i quali, cercano di delegare alle organizzazioni multistakeholder specifiche responsabilità in ordine allo sviluppo di codici di condotta e standard. Generalmente, tuttavia, i poteri di tali organizzazioni e procedimenti multistakeholder, risiedono sul consenso, rispetto alle regole di natura procedurale, espresso da quanti hanno accettato di parteciparvi.

Tali aspetti, tuttavia, contribuiscono ad aumentare l'incertezza circa la definizione delle tematiche prioritarie così come rispetto alle competenze esercitate da organizzazioni e procedimenti multistakeholder relativamente ad una specifica problematica o alle interconnessioni tra i diversi temi.

Tale sviluppo dei sistemi di governance internazionale ha trovato le sue prime manifestazioni nei sistemi normativi caratterizzati da una forte componente privata e tecnica, quali i settori della proprietà intellettuale e, per quanto qui interessa, delle infrastrutture ITC, in particolare della governance di Internet.

2.1 Il sistema della governance tecnica di Internet.

La governance della rete Internet[323] poggia, infatti, su enti di natura privata a vocazione prettamente tecnica quali sono la Internet Coorporation for Assigned Names and Numbers (ICANN); la Internet Assigned Numbers Authority (IANA); la Internet Society (ISCOC); i Regional Internet Registry (RIRs); La Internet Engineering Task Force (IETF); il World Wide Web Consortium (W3C); e il Internet Architecture Board (IAB).

[323] ERIC BROUSSEUA, MERYEM MARZOUKI, CÉCILE MÉADEL, *Governance, Regulations and Power on the Internet*, Cambridge University Press, 2015.

Tra essi una particolare importanza è attribuita all'ICANN, organizzazione privata no profit registrata in California nel 1998 che, raccogliendo alcune delle funzioni svolte dalla IANA, e interagendo con le altre organizzazioni, definisce gli standard tecnici alla base del funzionamento della rete Internet.

La struttura, l'organizzazione e l'azione proprie di tale ente sono comunemente considerate il riferimento per l'analisi del più generale modello di governace multistackeholder. Come è stato osservato l'ICANN costituisce*"a new type of organization that is tied deeply to private sector, yet it has the unprecedented power to implement a set of rules, which will then be followed all around the world"*[324]

In particolare, l'ICANN si occupa di assegnare gli indirizzi IP, di gestire il sistema dei nomi a dominio generici di primo livello e dei country code Top Level Domain nonché dei root server. La competenza dell'ICANN riguarda dunque aspetti tecnici relativi ai Domain Name System (DNS) ed è finalizzata ad assicurarne, sul piano universale, il corretto funzionamento al fine di garantire la fruibilità della rete Internet da parte degli utenti. Lo Statuto, tuttavia, esclude lo svolgimento di attività di regolamentazione dei servizi forniti tramite Internet così come dei loro contenuti, affermando chiaramente che *"ICANN not hold any governamentally authorized regulatory authority"*[325].

Le attività proprie dell'ente devono essere realizzate, nell'interesse della comunità di Internet, conformemente agli impegni e ai valori previsti dallo Statuto e nel rispetto del diritto internazionale e delle leggi locali applicabili, attraverso un processo aperto e trasparente che consenta la concorrenza e l'accesso nei mercati collegati a Internet[326]. In particolare, lo Statuto impegna l'ente a *"rispettare l'innovazione creativa e il flusso di informazioni reso possibile da Internet, limitando le attività dell'ICANN a questioni che rientrano nella missione dell'ICANN e che richiedono o beneficiano in modo significativo di un coordinamento globale"*[327].

Rispetto al tema qui trattato dei modelli di governance multistakeholder, rileva l'esplicita previsione dell'impegno a

---

[324] VERONICA ZOLNERCIKOVA, *ICANN: Trasformation of approach toward Internet Governance*, Masaryk University Journal of Law and Technology, vol. 11 n. 1, Summer 2017, p. 158, HeineOnline

[325] STATUTO ICANN, *art. 1.1 lettere b) e c)*

[326] STATUTO ICANN, *art. 1.2 lettera a)*

[327] STATUTO ICANN, *art. 1.2 lettera a) punto iii)*

"impiegare un processo di sviluppo delle politiche aperto, trasparente e dal basso verso l'alto, multistackeholders, guidato dal settore dei privati"[328]. Vengono dunque sviluppati procedimenti volti a favorire il contributo del pubblico, a promuovere una decisione ben informata basata sul parere di esperti e, infine, a garantire che le entità maggiormente interessate possano contribuire al processo di sviluppo delle politiche dell'ente.

Per quanto riguarda i valori di riferimento, di cui all'art. 1.2 dello Statuto, essi sono volti a favorire la diffusione delegata delle competenze e la partecipazione rappresentativa delle peculiarità geografiche e culturali, oltre che personali e professionali, al fine di sviluppare processi decisionali multistakeholder verificabili e trasparenti che permettano la definizione degli interessi pubblici. Rispetto a questi ultimi, viene chiarito che i governi e le autorità pubbliche sono responsabili delle politiche pubbliche delle quali occorre tenerne debitamente conto, pur restando l'ente radicato nel settore privato.

Coerentemente con gli scopi, gli impegni e i valori definiti dall'art.1, lo Statuto successivamente si occupa di delineare gli organi di governance così come i termini e le modalità d'azione dell'ICANN. Rilevano anzitutto le norme volte ad attribuire competenze e poteri a determinati organi dell'ente. Per quanto qui di specifico interesse, l'art.2 si occupa di attribuire i poteri mentre i successivi articoli da 5 a 9 delineano i singoli organi quali l'Ombudsman, la Empowered Community[329], il Board of Director, il Nominating Commitee e, infine, le Address Supporting Organizations (ASO)[330].

L'art. 2 attribuisce al Consiglio l'esercizio, sulla base di un voto a maggioranza dei Direttori, dei poteri propri dell'ICANN così come il controllo delle proprietà e la conduzione degli affari e delle attività

---

[328] STATUTO ICANN, *art. 1.2 lettera a) punto iv)*

[329] STATUTO ICANN, *art. 6.* La Empowered Community consiste in un'associazione senza scopo di lucro costituita secondo le leggi dello Stato della California dall'ASO, dal ccNSO, dal GNSO, dall'ALAC e dal GAC. Singolarmente vengono indicati come "Partecipante Decisionale" o "associato" mentre, collettivamente, sono indicati come "Partecipanti Decisionali".

[330] STATUTO ICANN, *art. 9.* La Address Supporting Organization (ASO) è un Ente instituito attraverso il Memorandum d'intesa stipulato tra l'ICANN e la Number Resource Organization (NRO), il 21 ottobre 2004. I suoi compiti consistono nel fornire al Consiglio la propria consulenza in merito a questioni politiche relative al funzionamento, all'assegnazione e alla gestione degli indirizzi internet

.

dell'ente in particolare attraverso standard, politiche e procedure conformi al principio di non discriminazione.

L'art. 7 dello Statuto dell'ICANN disciplina la composizione, le funzioni e le modalità d'azione del Consiglio. Tale organismo è composto di sedici Direttori con diritto di voto, a cui si aggiungono quattro funzionari senza diritto di voto designati, ai sensi della normativa civilistica californiana, dall'Empowered Community sulla base delle nomine presentate dal Nominating Commitee, dal ASO, dal ccNSO[331], dal GNSO[332] e, infine, da AT-Large Community[333]. Da ultimo, il presidente svolge il ruolo di Direttore ex officio. Le nomine devono, assicurare la diversità geografica e culturale oltre che di esperienza e prospettiva. Sono inoltre previste due condizioni di incompatibilità con la carica di direttore. Nello specifico l'art 7.4 prevede che non possono ricoprire la carica di Direttore coloro che ricoprono cariche in un governo nazionale o in un'organizzazione internazionale o che svolgono servizio, anche come funzionari, in qualsiasi Consiglio di una delle organizzazioni collegate all'ICANN. Infine, per quanto riguarda le modalità di funzionamento dell'organo, lo Statuto prevede lo svolgimento di Riunioni Annuali oltre che ordinarie e speciali, specificando le forme di voto e di notifica.

La principale attività del Consiglio consiste nell' elaborare Linee Guida (Board Governance Guidelines) volte a fornire una struttura all'interno della quale l'ente e il Consiglio stesso possono efficacemente perseguire gli scopi statutari. Tali linee guida, tuttavia,

---

331 STATUTO ICANN, *art. 10* Il Country-Code Names Supporting Organization (ccNSO) è un organismo competente a sviluppare e raccomandare al Consiglio le politiche globali relative ai domini di primo livello dei codici paese. La sua azione è volta alla costruzione del consenso tra i vari membri e può coordinare la propria attività con quella di altri organismi. Nomina due membri del consiglio di amministrazione. In particolare, ha la competenza a sviluppare attività ulteriori rispetto a quelle statutarie, volte all'elaborazione di Best Practices nel campo tecnico di riferimento.

332 STATUTO ICANN, *art. 11*. La Generic Names Supporting Organization (GNSO) è un organismo responsabile di sviluppare e raccomandare al Consiglio le politiche relative ai domini generici di primo livello.

333 La At-Large Community agisce all'interno dell'ICANN nell'interesse degli utenti. Può essere composta da gruppi per i diritti dei consumatori, organizzazioni accademiche o individui la cui azione è volta promuovere lo sviluppo delle TIC e di contribuire alle politiche che influenzano il coordinamento tecnico del Domain Name System. Attualmente sono 230 At-Large Structures (ALSes) e 85 Membri individuali in tutto il mondo. https://atlarge.icann.org/about/index

sono intese non come un insieme di obblighi vincolanti quanto piuttosto come un quadro flessibile entro cui condurre le attività dell'ente[334]

A partire dall'ottobre 2016 il potere di designare i membri del Consiglio è stato attribuito all'Empowered Community. Tale organismo trova il suo fondamento nella disciplina privatistica californiana ed è regolamentato dall'art 6 dello Statuto. In particolare, la Empowered Community è un'associazione non profit composta da ASO, ccNSO, GNSO, oltre a specifici comitati consultivi, definiti Decisional Partecipant, a cui sono attribuiti specifici poteri.

Questi consistono, ai sensi dell'art. 6.2, nel potere di rimuovere singoli Direttori o richiamare l'intero Consiglio, di rigettare gli atti di programmazione economica e operativa dell'ICANN e dalla IANA e approvare gli emendamenti allo Statuto.

Il processo di nomina del Consiglio coinvolge un ulteriore organismo, il Nominating Commitee. Disciplinato dall'art. 8 dello Statuto esso ha competenza in materia di nomina dei Direttori così come delle altre figure per cui lo Statuto richiede un procedimento di nomina.

Al di là della sua composizione e delle diverse norme sul suo funzionamento, appare particolarmente interessante, nella prospettiva qui adottata, la previsione dell'art. 8.7 ai sensi del quale *"the nominating commitee shal adopt such operating procedure as it deems necessary, which shall be pubblished on the web site"*. Ciò che viene in evidenza è l'attribuzione di autorità alla procedura e alle sue norme che si è visto essere il tratto distintivo dei modelli multistakeholder. La centralità delle norme procedurali è inoltre rafforzata dalla previsione di un meccanismo di tipo giurisdizionale strutturato nell'Ufficio dell'Ombudsman. Questi, ai sensi dell'art. 5.2, è chiamato ad agire *"as a neutral dispute resolution practioner"* le cui funzioni consistono nel fornire una valutazione interna indipendente dei reclami da parte di membri della comunità ICANN e nel risolvere i conseguenti conflitti attraverso attività di negoziazione, facilitazione e *"shuttle diplomacy"*.

Dal punto di vista strutturale, dunque, l'ICANN mostra i tratti caratteristici degli enti e dei modelli multistakeholder. Rileva, in primo luogo la sua natura privata stante il suo fondamento nelle norme civilistiche dell'ordinamento Californiano a cui lo Statuto rinvia espressamente. In secondo luogo, viene in rilievo la centralità attribuita allo sviluppo di procedimenti funzionali alla definizione delle politiche

[334] Cfr. ICANN, Guide Lines, consultabili alla pagina Internet https://www.icann.org/resources/pages/governance/guidelines-en

e delle azioni dell'ente. In terzo luogo, lo Statuto espressamente chiarisce la posizione di autonomia dell'ente rispetto ai governi così come rispetto alle organizzazioni internazionali da essi costituite. Infine, emerge il tratto caratteristico degli enti multistakeholder consistente nel ruolo centrale degli attori privati a cui spettano poteri di nomina degli organi dell'ente, di definizione e controllo delle loro politiche e del loro operato e, infine, poteri di emendamento dello Statuto e delle diverse procedure.

Tali caratteri vengono ulteriormente in evidenza in sede di analisi della disciplina dell'azione dell'ICANN che, come si è accennato, appare orientata a favorire la più ampia partecipazione degli attori privati valorizzando i principi di trasparenza, responsabilità e riesame.

Entro questa prospettiva, rilevano gli articoli 3 e 4 i quali disciplinano la forma e gli strumenti di trasparenza e accountability.

L'art. 3 dello Statuto fornisce un'originale interpretazione e applicazione del principio di trasparenza intendendo per essa che *"ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness, including implementing procedures to (a) provide advance notice to facilitate stakeholder engagement in policy development decision-making and cross-community deliberations, (b) maintain responsive consultation procedures that provide detailed explanations of the basis for decisions (including how comments have influenced the development of policy considerations), and (c) encourage fact-based policy development work. ICANN shall also implement procedures for the documentation and public disclosure of the rationale for decisions made by the Board and ICANN's constituent bodies"*.

Viene in evidenza, affianco alla centralità riconosciuta al principio di trasparenza, il suo stretto legame con le norme procedurali essendo volta a favorire la partecipazione degli stakeholder nei processi decisionali consultivi e di verifica.

Il principio di trasparenza costituisce dunque il fattore legittimante l'azione di governance dell'ente ed in tale funzione esso viene sorretto e rafforzato dalla previsione statutaria di strumenti di responsabilità e riesame delineati dall'art. 4 dello Statuto.

Sono quindi previsti meccanismi di riesame, revisione indipendente, di divulgazione delle informazioni, oltre all'Ombudsman e alla Empowered Community di cui si è detto. Sono inoltre delineati specifici meccanismi per la revisione dell'attività delle organizzazioni

che partecipano all'azione dell'ICANN e, infine, meccanismi di revisione per specifiche problematiche tecniche.

3. La pluralità dei regimi di governance.

Il sistema dei regimi regolatori in cui si articola la governance del cyberspace si presenta particolarmente articolato, dal punto di vista soggettivo così come da quello funzionale. Coerentemente con i caratteri tecnici e la natura ideale alla base dello sviluppo del dominio informatico il centro di tale sistema di governance è costituito da enti di regolamentazione tecnica aventi natura privata e rilevanza globale, tra i quali il modello ICANN sopra descritto costituisce il principale esempio.

Diversamente, sul piano politico, si registrano una pluralità di organizzazioni internazionali, globali, regionali e settoriali, alle quali si aggiungono specifici accordi interstatali.

Affianco ad essi, inoltre, acquisiscono sempre maggior rilevanza organizzazioni non governative, imprese private, conferenze e commissioni d'inchiesta indipendenti, anch'esse riconducibili all'azione di attori privati.

Secondo il documento conclusivo dei lavori del WGIG del 2005 la Internet Governance "*is the application by government, the private sector and civil society of principles, norms, rule, procedures and programs that shape the evolution and the use of Internet"*[335]

Tale sistema di governance può essere ricostruito, seppur in forma necessariamente parziale, sulla base della teoria dei regimi normativi sviluppata sul piano delle relazioni internazionali a partire dagli anni 70 del secolo scorso. Entro questa prospettiva i regimi normativi consistono in principi, norme, regole e procedure che governano le diverse aree tematiche degli affari internazionali[336]

In particolare, si tratta di sottoinsiemi di norme espressione di aspettative condivise circa i comportamenti ritenuti appropriati nei diversi contesti. In termini generali tali norme possono essere descrittive e/o predittive, così come istituzionalizzate o meno. Qualora

---

[335] WORKING GROUP ON INTERNET GOVERNANCE, *Report of the Working Group on Internet Governance*, Chateau de Bossey, 2005, www.wgig.org/docs/WGIGREPORT.pdf.

[336] JOH GERARD RUGGIE, *International Regimes, Transactions, and change: Embedded Liberalism in the Post War Economic Order*, International Organization 36 (2); ROBERT O. KEOHANE, JOSEPH S. NYE, *Power and Interdependence*, Boston: Little Brown, 1977

tra di esse sussista un rapporto di tipo gerarchico viene a definirsi uno specifico regime normativo.

Tali regimi normativi, tuttavia, possono interagire tra di essi. Da questo punto di vista viene in rilievo la figura del *regime complesso* o, in altri termini, *"a loosely coupled set of regimes"*[337] . Tale regime si pone, da un punto di vista formale, tra i due estremi rappresentati da un singolo strumento giuridico da una parte e da una serie di accordi frammentati dall'altra.

Nel contesto delle tecnologie dell'informazione tale forma di regime normativo costituisce il modello di riferimento. La governance del cyberspace, infatti, non riposa su un unico regime normativo quanto piuttosto su un insieme di norme e istituzioni che liberamente interagiscono tra di esse. La governance del cyberspace costituisce dunque un sistema a metà strada tra sistemi istituzionali che impongono una data regolamentazione sulla base di un principio gerarchico e altri che si basano su pratiche altamente frammentate e istituzioni prive di una struttura organizzativa e di un riparto di competenze interne chiaramente identificabile.

Inoltre, lo studio dei regimi complessi permette di evidenziare alcuni caratteri peculiari della governance del cyberspace. In primo luogo, emerge l'importanza dei collegamenti tra la dimensione cyber e i regimi istituzionali e normativi esterni al dominio informatico. Occorre infatti considerare che, dati i fattori e i caratteri del Cyberpower visti nel secondo capitolo, attori e istituzioni attivi nel cyberspace svolgono, al contempo, la loro azione anche negli altri domini delle relazioni internazionali.

In secondo luogo, emerge l'estrema balcanizzazione della governance nella quale la cooperazione tra attori può realizzarsi rispetto a specifiche tematiche e assumere segno opposto in altri settori[338].

Ciò evidenzia infine, una generale mancanza di coerenza che viene compensata da una maggiore flessibilità e adattabilità (resilienza) così rispecchiando i caratteri di base dello spazio informatico visti nel primo capitolo.

Dal punto di vista normativo è possibile classificare i regimi relativi alle diverse tematiche sulla base di quattro parametri[339]. Il primo attiene

---

[337] JOSEPH S. NYE. Jr, *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance, Paper Series: no.1, May 2014, p. 9

[338] Umberto gori cyberwarfare testo di Massolo

[339] JOSEPH S. NYE. Jr, *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance, Paper Series: no.1, May 2014.

al rapporto gerarchico tra gli insiemi normativi. Il secondo prende in considerazione gli scopi per i quali gli Stati Membri e gli attori non Statali hanno accettato un dato regime normativo. Il terzo tiene in considerazione il ruolo e i rapporti tra attori statali e non in una determinata area d'azione. Il quarto, infine, pone attenzione alla corrispondenza dei comportamenti tenuti dagli attori rispetto alle norme delineate.

3.1 Principali regimi normativi che compongono la disciplina giuridica del cyberspace.

Quanto fin ora rilevato permette di costruire una mappa dei principali regimi normativi in cui si articola la governance del cyberspace strutturata sulla base delle tre direttrici dell'azione delle Nazioni Unite evidenziate nel precedente capitolo.

Ciò permette di ricostruire la dimensione funzionale dell'azione condotta dai singoli attori. Entro questa prospettiva i regimi regolatori verranno singolarmente ricondotti alle aree tematiche del mantenimento della pace e della sicurezza internazionale, del contrasto alla criminalità e della sicurezza delle infrastrutture, della promozione e tutela dei diritti umani.

Le problematiche relative al mantenimento della sicurezza e della pace internazionali possono essere ricondotte all'azione di governance svolta, in primo luogo, da organizzazioni internazionali aventi carattere universale, regionale o tecnico. Affianco all'attività sviluppata in sede di Nazioni Unite viste in precedenza, sul piano politico rilevano le posizioni espresse da forum internazionali quali il G20[340] e l'azione sviluppata dall' Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD)[341]. Così come gli accordi bilaterali, anche in

[340] L'ultima riunione del G20 si è tenuta nel giugno del 2019 in Giappone e, per quanto attiene alle nuove tecnologie, sono stati discussi i temi riguardanti il commercio digitale. https://www.japan.go.jp/g20japan/tsukuba.html . Inoltre, la dichiarazione finale del G20 gli Stati hanno adottato una serie di principi sullo sviluppo dell'Intelligenza Artificiale (cfr. https://www.mofa.go.jp/files/000486596.pdf) che richiamano i lavori in materia dell'OECD.

[341] L'OECD sviluppa la sua azione in materia di cyberspace con riferimento a diversi aspetti, dalla Blockchain allo sviluppo dell'Intelligenza Artificiale. Rispetto a quest'ultima, nel maggio del 2019 i Paesi Membri hanno approvato una Raccomandazione del Consiglio contenete una serie di principi per lo sviluppo di tali tecnologie (cfr. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449).

materia di intelligence, che regolano i rapporti tra i principali attori internazionali.

Sul piano delle organizzazioni regionali e tecniche vengono in evidenza i regimi di governance riconducibili ad organizzazioni quali l'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE)[342], l' Asean Regional Forum (ARF)[343], la Shanghai Cooperation Organization (SCO)[344] e l'Organizzazione per gli Stati Americani (OAS)[345].

Lo sviluppo di pacifici rapporti interstatali è oggetto dell'azione anche di organizzazioni e attori non governativi quali Electronic Frontier Foundation (EFF), Freedom House e Access. Un'importanza crescente è riconosciuta alle conferenze internazionali quali il London process, il NET Mundial e lo 1NET Group. Rileva infine, per quanto attiene agli armamenti, il sistema regolatorio del Wassenar Arrangement

Il tema del contrasto della criminalità e della sicurezza delle infrastrutture trova i suoi principali regimi regolatori, in primo luogo, nell'azione di law enforcement svolta dagli organismi specializzati delle Nazioni Unite e da organizzazioni di cooperazione internazionale quali l'INTERPOL. In secondo luogo, una particolare importanza viene attribuita alla *Convenzione di Budapest* elaborata in sede di Consiglio d'Europa[346]. Per quanto riguarda il più specifico tema della sicurezza

---

342 Di particolare interesse la Decisione del Consiglio Permanente n. 1202 del 10 marzo 2016 nella quale sono state adottate misure per rafforzamento della fiducia volte a ridurre i rischi di conflitto derivanti dall'uso di tecnologie informatiche e di comunicazione. Cfr. https://www.osce.org/files/f/documents/2/9/228511.pdf .

343 ASEAN REGIONAL FORUM, *Concept Paper For the Establishment of Asean Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies (ISM on ICTs Security)*; ASEAN REGIONAL FORUM, *Work Plan on Security of and in the Use of Information and Communication Tecnologies (ICTs)*, 7 May 2015. Entrambi sono consultabili all'indirizzo https://aseanregionalforum.asean.org/librarycat/icts-security/ .

344 SHANGHAI COOPERATION ORGANIZATION (SCO), *Agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security*, 2009. https://ccdcoe.org/organisations/sco/ ; in argomento si veda anche BRUNA TOSA DE ALCANTARA, *SCO and Cybersecurity: Eastern Security Vision for Cyberspace*, International Relation and diplomacy, Volume 6, Number 10, (Serial Number 61) October 2018

345 ORGANIZATION AMERICAN STATES, GENERAL ASSEMBLY, Resolution AG / RES. 2004 (XXXIV-O/04), *The Inter-American Integral Strategy to Combat Threats to Cyber Security*, http://www.oas.org/en/council/AG/ResDec/

346 CONSIGLIO D'EUROPA, *Convenzione sulla criminalità informatica*, Budapest 23/11/2001. La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche. Si occupa, in particolare, delle violazioni dei diritti d'autore, della

delle infrastrutture informatiche l'azione di governance è svolta attraverso forum e conferenze internazionali quali Internet Governance Forum, World Summit of Information Society Working Group on Internet Governance.

Le organizzazioni non governative attive rispetto al mantenimento della sicurezza e della pace internazionale generalmente svolgono la loro azione anche rispetto al tema del contrasto alla cyber criminalità. Ad esse tuttavia si aggiungono, in particolare per quanto riguarda la sicurezza delle infrastrutture organismi quali ISPs e Telcos.

Infine, rispetto alla tematica della tutela e promozione dei diritti dell'uomo viene in evidenza il ruolo centrale svolto dal Consiglio dei Diritti Umani la cui attività è stata precedentemente delineata. Ad esso si affianca l'azione condotta da organizzazioni regionali quali il COE, l'OSCE, lo SCO, la OAS e ARF. Mentre l'azione degli attori privati trova i suoi riferimenti, anche rispetto a questa tematica, nell'EFF, nella Freedom House e in Access.

3.2 L'azione normativa degli attori privati

L'azione normativa dei privati rispetto alle emergenti tematiche del cyberspace non si esaurisce nella partecipazione ai diversi fori internazionali indicati.

Il cyberspace, e in particolare i suoi aspetti dinamici, favoriscono il processo di *"giuridificazione"* privata[347] emerso con lo sviluppo della globalizzazione.

L'aumento delle relazioni tra privati aventi dimensione trans nazionale ha posto in crisi la capacità degli ordinamenti nazionali di governare le dinamiche di fenomeni sempre più globali. Allo stesso tempo l'assenza di un governo globale ha favorito lo sviluppo di processi normativi fondati sull'attività dei privati.

---

frode informatica, della pornografia infantile e delle violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure specifiche, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la criminalità informatica, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

[347] GUNTHER TEUBNER, *Economia del dono, positività della giustizia: la reciproca paranoia di Jacques Derrida e Niklas Luhmann*, Sociologia e politiche sociali, 6, 1 2003, pp. 113 – 130.

L'esempio tipico riguarda lo sviluppo della *lex mercatoria*[348] rispetto alla quale si pone il problema se essa costituisca o meno diritto in quanto espressione delle relazioni tra soggetti privati e non di processi legislativi di tipo costituzionale propri degli ordinamenti statali[349].

Il carattere giuridico risiederebbe nel riferimento che vi fanno gli attori privati per la regolamentazione dei loro rapporti.

Entro questo quadro, con riferimento al cyberspace, è stato sviluppato il concetto di *Quasi-norms* ovvero "norme che sono state etichettate come norme, ma che mancano delle caratteristiche chiave qualificanti delle norme: vale a dire, la forza prescrittiva e di valutazione, e l'ampia accettazione e l'internalizzazione da parte dei membri di una particolare comunità"[350].

Il cyberspace costituisce un nuovo ambito di sviluppo per tali processi normativi in particolare per quanto riguarda la Cybersecurity, settore nel quale sono particolarmente impegnati attori privati quali Microsoft e Symantec.

L'interazione, la pervasività delle tecnologie ITC, così come il ruolo centrale dei privati nella costruzione del cyberspace favoriscono lo sviluppo dell'azione normativa privata in molteplici altri settori delle relazioni sociali: dalla tutela della proprietà intellettuale alla disciplina degli strumenti e delle forme del diritto di espressione o di informazione.

Posto che le tecnologie del cyberspace sono in grado di determinare i comportamenti sociali e individuali, come descritto nei precedenti capitoli, si pone il problema di regolamentare il design tecnico di tali tecnologie. È questo il tema della funzione normativa degli algoritmi alla base dei prodotti e dei servizi di natura informatica.

In questo ambito è possibile rilevare diverse proposte generalmente orientate alla definizione di parametri etici per lo sviluppo degli algoritmi, ai quali generalmente si fa riferimento in termini di Intelligenza Artificiale. Proposte che tuttavia non sono ancora confluite in atti normativi rilevanti sul piano internazionale.

---

348 GUIDO ALPA, MADS ANDENAS, *Fondamenti del diritto privato europeo*, Giuffré, 2005

349 GUNTHER TEUBNER, *Breaking Frames: la globalizzazione economica e l'emergere della lex mercatoria*, in GUNTHER TEUBNER, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Armando Editore, 2005

350 TONI ERSKINE AND MADELINE CARR, *Beyond "Quasi-Norms': The challenges and potential of engaging with norms in cyberspace*, in, a cura di, ANNA-MARIA OSULA, HENRY ROIGAS, *International Cyber Norms: Legal, Policy & Industry Perspective*, NATO CCD COE Publications, Tallinn 2016.

Capitolo V

L'influenza del Cyberspace sul diritto internazionale

Introduzione

Nei precedenti capitoli si è inteso delineare i caratteri fondamentali del cyberspace e le problematiche poste dal suo processo di sviluppo.

Inizialmente sono state prese in considerazione le dimensioni strutturale e funzionale dello spazio informatico. I caratteri individuati hanno costituito il presupposto per la successiva analisi dei cambiamenti determinati dal progresso tecnologico sia rispetto alle relazioni di potenza che caratterizzano i rapporti tra attori internazionali, sia rispetto alle dinamiche economiche che sorreggono i processi di sviluppo della società.

Attraverso la successiva ricostruzione dell'azione svolta dalle Nazioni Unite, si è inteso rilevare le problematiche concretamente determinate dai fattori di cambiamento precedentemente delineati. Problematiche ricondotte alle tre aree tematiche del mantenimento della sicurezza e della pace internazionale, della sicurezza dello spazio informatico rispetto ad attività criminali e della promozione e tutela dei diritti dell'uomo. Azioni svolte entro la più ampia prospettiva politica dello sviluppo di una Società della Conoscenza.

Sul piano giuridico, nel quarto capitolo, sono state rilevate le principali novità in tema di governance e di processi normativi determinati dall'affermarsi del cyberspace. In questa sede si è evidenziata la rilevanza progressivamente acquisita dai modelli di

governance guidati da attori privati ai quali è possibile ricondurre i principali sviluppi dei regimi normativi che disciplinano le diverse aree del cyberspace.

Tuttavia, i caratteri dello spazio informatico e le dinamiche, relazionali ed economiche, determinate dal suo processo di sviluppo, incidono in maniera peculiare sulle norme di diritto internazionale finora elaborate dalla Comunità Internazionale.

Nuovi elementi di complessità sono introdotti all'interno del sistema delle fonti così come emergono nuove questioni interpretative rispetto all'applicazione delle norme internazionali a nuove e complesse fattispecie. Se da un lato, infatti, sussiste un generale consenso circa l'applicabilità al cyberspace delle norme di diritto internazionale[351], dall'altro permangono incertezze e problemi relativi alla definizione del modo in cui le norme trovino concreta applicazione rispetto alle tecnologie dell'informazione e alle azioni condotte per loro tramite nel cyberspace.

Inoltre, il dominio informatico non costituisce solamente uno spazio relazionale di natura conflittuale rispetto al quale occorre definire le norme relative alle azioni che gli attori vi attuano. Il cyberspace, in ragione dei caratteri propri del progresso scientifico e tecnologico che ne sostiene lo sviluppo visti nei capitoli iniziali, costituisce un autonomo fattore di progresso in grado di informare dei suoi caratteri la società umana e il suo sviluppo. Affianco alle norme di diritto internazionale volte a disciplinare l'agire degli attori internazionali occorre dunque individuare le norme internazionali volte a disciplinare il processo di sviluppo del cyberspace quale fattore di progresso al fine di preservare all'uomo il ruolo centrale rispetto al progresso della Società Umana.

Nel presente capitolo, pertanto, verranno osservate le principali questioni poste dal processo di affermazione del cyberspace rispetto al sistema delle fonti di diritto internazionale e alla disciplina dell'azione

[351] In termini generali si può osservare come i lavori dei gruppi di esperti, le risoluzioni dell'Assemblea Generale e i lavori dei diversi organismi cui si è fatto riferimento, abbiano progressivamente rilevato l'applicabilità all'azione degli Stati nel cyberspace delle norme e dei principi propri del diritto internazionale. Il Report del 2013 del Gruppo di Esperti Intergovernativi istituito in materia di sicurezza, sintetizza il generale consenso circa l'applicabilità degli strumenti pattizi esistenti al cyberspace rilevando che *"Le droit international et, en particulier, la charte des Nations Unies sont applicables et essentiels au mantien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique, sur, pacifique et accessible"* (Cfr. ASSEMBLEA GENERALE, *Rapporto GGE A/68/98 del 2013 paragrafo19*).

degli attori nello spazio informatico. Infine, verrà delineata la duplice funzione dei diritti umani rispetto alla definizione del *Limes*, da un lato, dell'azione degli attori internazionali e, dall'altro, del progresso scientifico e tecnologico al fine di promuovere e tutelare la dignità della persona.

1. *L'influenza del cyberspace rispetto al sistema delle fonti di diritto internazionale*

Nei precedenti capitoli si è evidenziato come lo sviluppo del cyberspace introduca all'interno delle relazioni internazionali nuovi fattori di complessità i quali esplicano i propri effetti anche sul sistema delle fonti giuridiche e sulla disciplina giuridica applicabile.

In particolare, incidono sui processi di formazione delle norme internazionali i fenomeni di riduzione dei tempi degli accadimenti politicamente rilevanti, della diffusione del potere tra più attori non solo statali e, infine, la disomogeneità degli interessi perseguiti in ragione del carattere dual-use delle tecnologie dell'informazione e della loro integrazione e pervasività.

Allo stesso modo la rilevanza acquisita da nuovi fattori della potenza e da nuove metodologie e strumenti di esercizio della stessa, determinando nuove e complesse fattispecie, incidono sui processi di interpretazione e applicazione delle norme internazionali.

Entro questa prospettiva, pertanto, le problematiche indicate verranno sviluppate con riferimento al sistema delle fonti di diritto internazionale muovendo dalle questioni poste rispetto alle norme consuetudinarie, alle norme convenzionali e ai principi generali di diritto. Inoltre, considerata la loro rilevanza all'interno del sistema normativo del cyberspace verranno prese in considerazione le norme di soft law.

1.1 La consuetudine

La consuetudine ricopre un ruolo centrale nel diritto internazionale nonostante venga indicata successivamente alle fonti pattizie dall'art.38 dello Statuto della Corte Internazionale di Giustizia, essendo quest'ultimo volto a delineare i riferimenti per la conduzione e la soluzione delle controversie internazionali.

Sul piano formale la centralità delle norme consuetudinarie deriva dalla circostanza che *"mentre le altre fonti internazionali sono obbligatorie perché così la consuetudine stabilisce, la consuetudine costituisce un fenomeno a formazione spontanea la cui giuridicità non dipende da altre fonti bensì dalla socialità intrinseca nel diritto"*[352]. La norma consuetudinaria, come noto, nasce, si modifica, si estingue a seguito dei comportamenti dei consociati, accompagnati dall'opinione degli stessi consociati che tali comportamenti siano obbligatori dal punto di vista giuridico e, comunque, socialmente doverosi[353]. L'importanza della consuetudine conseguentemente, è legata alla sua validità *erga omnes* e alla sua capacità di individuare un nucleo fondamentale dei principi giuridici inderogabili.

La natura e i caratteri della consuetudine pongono problemi di ordine generale relativi all'inquadramento giuridico e al processo di formazione che, nel passaggio dalla Comunità Internazionale classica (composta da pochi Stati omogenei per valori, interessi ed esigenze di coesistenza) alla Comunità Internazionale moderna (composta da molti Stati aventi caratteri e interessi disomogenei), hanno posto in crisi la capacità della fonte consuetudinaria di rispondere alle attuali esigenze delle relazioni internazionali[354].

Tuttavia, l'importanza della consuetudine ha spinto la Comunità Internazionale all'individuazione di meccanismi e strumenti giuridici di reazione alla sua crisi. Vengono qui in rilievo le consuetudini istantanee, basate sul carattere relativo del fattore tempo, e le consuetudini particolari o locali, che fanno riferimento al numero degli Stati coinvolti nel procedimento di formazione della norma così come

---

[352] CARLO FOCARELLI, *Diritto Internazionale*, CEDAM, Milano, 2019, p. 125, 126

[353] Il diritto internazionale consuetudinario, come noto, può quindi essere inteso come la sintesi di due elementi. Il primo, di carattere oggettivo o materiale, è rappresentato dalla *diuturnitas*, ovvero il comportamento costante e uniforme tenuto dalla generalità dei soggetti della Comunità Internazionale, che assicura l'effettività della norma impedendo di supporre esistenti norme che non operano nella realtà. Il secondo, di carattere soggettivo o psicologico, consite nell'*opinio juris*, ovvero il convincimento della doverosità o necessità sociale prima ancora che giuridica di dover tenere quel comportamento, e permette di distinguere la prassi seguita per motivi extra-giuridici e non intesa a vincolare gli Stati, dalla prassi che è invece seguita come giuridicamente obbligatoria.

[354] I mutamenti strutturali determinati dall'aumento dei soggetti della Comunità Internazionale, disomogenei nei valori e negli interessi, impediscono la formazione di nuove norme consuetudinarie favorendone, viceversa, la contestazione da parte dei nuovi attori. Allo stesso modo, le esigenze della cooperazione internazionale a cui è informata la comunità Internazionale moderna, richiedono certezza dei rapporti, specializzazione della norma, speditezza nella individuazione della norma di fronte a problemi sempre nuovi. Funzione svolta con maggiore efficacia dalle norme convenzionali e di soft law.

allo specifico regime giuridico a cui sono riconducibili. Al medesimo problema risponde anche lo sviluppo di accordi di codificazione, ovvero la trasposizione in norme scritte del diritto internazionale consuetudinario al fine di ovviare all'incertezza del suo contenuto, la cui vincolatività, tuttavia, è limitata agli Stati contraenti potendosi estendere *erga omnes* solo nella misura in cui vi sia coincidenza con il diritto consuetudinario.

Rispetto alle relazioni internazionali sviluppate nel contesto del cyberspace, i caratteri di quest'ultimo contribuiscono a ridimensionare ulteriormente il ruolo della fonte consuetudinaria.

L'attualità e variabilità del cyberspace, assieme all'istantaneità che caratterizza i comportamenti nel dominio informatico, contrastano con la continuità su cui riposa l'elemento della *diuturnitas*. Allo stesso modo la disomogeneità di valori e interessi determinata dall'affermarsi di nuovi attori non statali, la difficoltà di attribuzione delle attività cyber e, soprattutto, la segretezza che le caratterizza, complicano la rilevazione dell'esistenza dell'elemento dell'*opinio juris*. Entro tale contesto, inoltre, la sua ricostruzione è resa ulteriormente difficoltosa dalle dichiarazioni degli Stati, generalmente volte ad indicare un'aspettativa piuttosto che ad affermare una posizione giuridicamente definita[355].

In questa prospettiva è stato osservato come appaia improbabile la formazione di nuove norme consuetudinarie mentre possono più facilmente presentarsi problemi di interpretazione delle norme consuetudinarie esistenti[356].

Tuttavia, come vedremo con riferimento ai problemi di interpretazione e applicazione, è possibile tracciare l'*opinio juris* finora espressa prendendo in considerazione i documenti di politica nazionale, le linee guida, i report e i manuali predisposti da organizzazioni internazionali, così come talune qualificate dichiarazioni politiche, nella misura in cui tali documenti siano chiaramente attribuibili agli Stati ed esprimano una chiara e non estemporanea convinzione circa la giuridicità di una norma. Tra questi sono particolarmente utili le strategie nazionali in materia di cyber security elaborate dagli Stati che,

---

[355] HAROLD HONGJU KOH, *International law in cyberspace*, Yale Law Faculty Scholarship Series 2012; MICHEL N. SCHMITT, SEAN WATTS, *The decline of International Humanitarian Law Opinio Juris and The Law of Cyber Warfare*, Text. Int'ILJ 50, 2018, pag. 217

[356] MICHAEL N. SCHMITT AND LIIS VIHUL, *The Nature of International Law Cyber Norms*, in ANNA-MARIA OSULA AND HENRY ROIGAS, *International Cyber Norma: Legal, Policy & Industry Perspective*, NATO CCD COE Pubblications, Tallin 2016 P. 45

seppur non costituiscono documenti propriamente giuridici, evidenziano interpretazioni basate su solide prospettive di lungo periodo rispetto ai temi più rilevanti in materia di diritto consuetudinario[357].

Problemi che, in termini generali, vengono individuati nell'interpretazione e nell'applicazione nel contesto del cyberspace, dei principi di sovranità, di due diligence, di autodifesa e uso della forza e, infine, del principio di responsabilità sotto il profilo particolare dell'attribuzione degli atti internazionalmente illeciti.

1.2 I trattati internazionali

Accanto alle problematiche indicate rilevano le questioni poste dall'applicazione allo spazio cyber dei regimi giuridici convenzionali finora elaborati nei diversi settori del diritto internazionale.

Nella moderna Comunità Internazionale i trattati costituiscono il principale strumento di governance della pluralità delle tematiche e delle problematiche internazionali e globali[358].

In termini generali si può definire il trattato come l'unione o l'incontro delle volontà di due o più soggetti di diritto internazionale dirette a istituire modificare o estinguere, determinati rapporti giuridici riguardanti tali soggetti[359].

Con riferimento ai rapporti tra diritto internazionale generale e diritto internazionale convenzionale, è possibile effettuare una prima distinzione con riferimento al procedimento di formazione della relativa norma. Mentre le norme di diritto generale non presentano fonti formali, in quanto espressione del corpo sociale della Comunità Internazionale, il diritto pattizio è munito di fonti formali. L'efficacia giuridica dei trattati, infatti, trova fondamento nella norma consuetudinaria *pacta sunt servanta.*

---

[357] ANN VALJATAGA, *Tracing opinion juris in National Cyber Security Strategy Documents*, NATO CCD COE, Law Researcher, Tallinn, 2018

[358] Nella Comunità Internazionale moderna i trattati hanno svolto una funzione codificatrice del diritto generale e di recepimento delle nuove istanze emergenti nelle relazioni di carattere internazionale

[359] Indipendentemente dal *nomen juris* attribuito all'atto, come rilevato dalla Corte Penale Internazionale nel 1931, questo costituisce un trattato internazionale quando contiene diritti e obblighi per le parti contraenti. Diversamente si è in presenza di una semplice intesa, non obbligatoria per le parti che la hanno sottoscritta e il cui mancato rispetto non determina la responsabilità internazionale della parte inadempiente. Egualmente non costituiscono trattati le intese stipulate tra uno Stato e una persona fisica o giuridica.

È inoltre possibile distinguere le norme di diritto internazionale generale da quelle di diritto convenzionale in base alla diversità del contenuto rispondendo, le prime, ad esigenze di coesistenza, le seconde, ad esigenze di cooperazione. Aspetto dal quale deriva l'importanza, quantitativa e qualitativa, della fonte convenzionale all'interno della Comunità Internazionale moderna[360].

Allo stesso modo, la varietà di interessi statali ed individuali di cui gli accordi si occupano ha ampliato le tipologie di trattati rendendone impossibile una classificazione in base al loro contenuto, pur essendo possibili altre distinzioni con riferimento alle parti contraenti e agli scopi del trattato[361].

Infine, retti dal principio consuetudinario *pacta sunt servanda*, i trattati internazionali trovano la loro disciplina formale nella Convenzione di Vienna del 1969 sul Diritto dei Trattati che, secondo *communis opinio*, risponde largamente al diritto internazionale consuetudinario in materia di formazione e interpretazione dei trattati[362] trovando applicazione anche nel contesto del cyberspace.

---

[360] La rilevanza quantitativa del diritto convenzionale è data dall'aumento dei settori disciplinati dal diritto internazionale in ragione sia dell'aumento dei rapporti interstatali, sia dell'aumento dei rapporti umani sul piano internazionale in settori prima disciplinati dal diritto interno. L'elemento qualitativo è dato dalla circostanza che in una fase di disomogeneità degli interessi degli Stati e di crisi della consuetudine internazionale l'unica via percorribile per disciplinare aspetti della vita di relazione internazionale particolarmente importanti e delicati, è quella della conclusione di trattati internazionali, la cui negoziazione permette la mediazione tra le opposte posizioni degli Stati.

[361] Con riferimento alla sfera soggettiva di applicazione i trattati possono essere distinti in bilaterali o multilaterali. Nell'ambito di quest'ultimi assumono una particolare rilevanza le Convenzioni di Codificazione che hanno la funzione di trasporre in forma scritta in modo sistematico ed organico il diritto internazionale generale pur potendo contenere norme di sviluppo progressivo del dirittto internazionale. I trattati inoltre possono essere distinti in trattati aperti o chiusi e contenere regole materiali o sostanziali.

[362] L'opera di codificazione delle norme consuetudinarie in materia è stata compiuta sotto gli auspici delle Nazioni Unite nell'ambito della Commissione di Diritto Internazionale che sin dalla sua prima sessione nel 1949, ha incluso il diritto dei trattati all'ordine del giorno dei suoi lavori. Tuttavia, soltanto dal 1961 la Commissione si è occupata concretamente del diritto dei trattati, adottando nel 1966 un progetto di articoli trasmetto all'Assemblea Generale delle Nazioni Unite per l'esame e per le decisioni relative alla fase ulteriore dei lavori di codificazione. La Convenzione di Vienna successivamente adottata è largamente riproduttiva del diritto internazionale generale anche se non mancano norme di sviluppo progressivo. La stessa Corte Internazionale di Giustizia ha in diverse occasioni sostenuto che la Convenzione di Vienna riflette il diritto internazionale generale (SENTENZA CORTE INTERNAZIONALE DI GIUSTIZIA caso *Gabcikovo-Nogymaras* del 1997). Si consideri inoltre che gli Stati, convenuti nel 1989 per stipulare una Convenzione sul Diritto dei Trattati tra Stati e Organizzazioni Internazionali, hanno ritenuto d ripetere tutte le norme della Convenzione di Vienna del 1969, con modifiche legate a singole particolarità del fenomeno delle organizzazioni internazionali.

Rispetto alla disciplina del cyberspace i trattati internazionali non rispecchiano quanto appena illustrato rivestendo un'importanza minore sia dal punto di vista quantitativo che da quello qualitativo.

Entro questa prospettiva occorre rilevare, in primo luogo, l'esistenza di un numero esternamente limitato di trattati internazionali in materia di cyberspace. Alcuni particolari aspetti sono disciplinati nella Convenzione sul Cybercrime del Consiglio d'Europa e nel suo Protocollo Addizionale del 2006. Sul piano delle organizzazioni regionali rileva inoltre l'International Information Security Agreement negoziato nel contesto della Shangai Cooperation Organization. Sul piano universale, infine, vengono in rilievo la Constitution and Convention of the International Telecommunication Union e, in particolare, l'International Telecommunication Regulations.

L'assenza di specifici trattati deriva dalla contemporaneità del fenomeno cyberspace, mentre gli Stati, storicamente, giungono alla definizione di un trattato quando i vari aspetti di una specifica materia e gli interessi connessi, risultino ormai consolidati.

Rileva, inoltre, la disomogeneità degli Stati rispetto al grado di sviluppo tecnologico così come nella capacità di definire i propri interessi e le modalità di azione volte al loro perseguimento nel dominio informatico. Aspetti questi che, nel contesto delle tecnologie dell'informazione, rendono gli Stati particolarmente riluttanti a vincolarsi a norme suscettibili di non rispondere alle esigenze di sviluppo della loro azione poste dai continui progressi tecnologici.

Infine, i caratteri del cyberspace complicano il processo di verifica del rispetto degli obblighi pattizi eventualmente assunti, facendo emergere un ulteriore fattore ostativo allo sviluppo di una disciplina convenzionale del cyberspace.

Tuttavia, è possibile rilevarne un iniziale sviluppo a partire dall'applicazione dei trattati relativi ad altri settori del diritto internazionale. In particolare, è stata evidenziata l'applicabilità al cyberspace di alcune norme del diritto del mare e del trattato sulle attività degli Stati condotte sulla Luna e su altri corpi celesti. Maggiori sviluppi si registrano in materia di diritti umani ed in particolare rispetto all'applicazione della Convenzione Europea sui Diritti Umani le cui disposizioni sorreggono l'azione dell'Unione Europea nei vari settori della disciplina giuridica del cyberspace.

Come abbiamo visto nel capitolo terzo, il Gruppo di esperti intergovernativi istituito dall'Assemblea Generale delle Nazioni Unite nel 2013, aveva chiarito che *"international law, and in particular the*

Charter of United Nations, is applicable and is essential to manteining peace and stability and promoting an open, secure, peaceful and accessible ICT environment"[363].

Ciò ha permesso gli sviluppi sopra indicati ma ha anche evidenziato problematiche nell'applicazione di alcuni specifici settori del diritto internazionale, quali il diritto internazionale umanitario, escluso dalla stesura finale del report in ragione delle diverse sensibilità emerse circa l'opportunità di applicare tale regime normativo al cyberspace.

In termini generali si pongono problemi legati all'interpretazione delle concrete modalità di applicazione delle norme internazionali al cyberspace. Come avremo modo di approfondire nel prosieguo, i principali punti controversi riguardano l'interpretazione rispetto alle fattispecie cyber delle norme relative all'uso della forza nella relazioni internazionali e all'esercizio del diritto di autodifesa.

1.3 I principi generali di diritto

I problemi di interpretazione e applicazione del diritto internazionale possono essere sciolti, come indicato dall'art. 38 par. 1 let. C) dello Statuto della Corte Internazionale di Giustizia, ricorrendo ai *principi generali di diritto riconosciuti dalle nazioni civili*. La norma indicata ricalca l'art. 38 par.3 dello Statuto della Corte Penale di Giustizia Internazionale che introduce tali principi tra le fonti che possono essere richiamate per la soluzione di una controversia. Principi che, come noto, vengono intesi, come chiarito da Lord Phillimore, membro inglese del Comitato Consultivo istituito dalla Società delle Nazioni per la redazione dello Statuto della Corte, nel senso di principi accettati dalle nazioni in foro domestico.

Entro questa prospettiva si risolve il problema sollevato dai principi generali di diritto, ovvero se essi costituiscano una fonte di diritto internazionale autonoma distinta dalle altre e quale rango occupi nel rapporto con esse. È stato infatti osservato[364] come la prassi ammetta da sempre, in un modo o nell'altro, l'idea che il diritto internazionale possa derivare anche dalle norme comuni agli Stati nei loro ordinamenti interni, soprattutto a fronte di un vuoto normativo o dell'insufficienza delle norme ai fini della risoluzione di una questione. I principi generali

[363] NAZIONI UNITE, ASSEMBLEA GENERALE, *Risoluzione A/68/98*.
[364] CARLO FOCARELLI, *Diritto Internazionale*, CEDAM, Milano, 2019

del diritto sono dunque intesi a colmare le lacune di diritto positivo e processuale, così come a stabilire standard di umanità universali che gli Stati condividono nei loro ordinamenti interni e di cui ne accettano l'applicazione sul piano internazionale. Applicazione che tuttavia non è permessa ove esistano di fatto norme positive appositamente create e applicabili[365]. Tali principi dunque *"possono essere configurati come fonti autonome di diritto internazionale sulla base del diritto internazionale consuetudinario e nei limiti da esso stabiliti"*[366].

Il loro contenuto può essere individuato nei principi di giustizia e di logica giuridica così elementari e così inerenti all'idea di giustizia da far presumere che esistano in ogni ordinamento giuridico. Si tratta in particolare dei principi di giustizia e logica giuridica quali *nemo iudex in res sua, pacta terziis neque nocet neque prosunt.* Principi di teoria generale del diritto relativi all'abuso del diritto, alla certezza del diritto, al legittimo affidamento, ai vizi del consenso, all' interpretazione dei trattati. Altri principi sono relativi al contenzioso tra Stati e alla loro responsabilità così come al rispetto del diritto di difesa. Un ulteriore principio pone attenzione agli atti giuridici e impone il bilanciamento degli interessi nel caso di invalidità degli atti. Infine, trovano spazio tra i principi generali i principi di rispetto dei diritti dell'individuo[367].

I principi generali di diritto costituiscono, da un diverso punto di vista, uno degli strumenti attraverso i quali è possibile reagire alla crisi

[365] Si può osservare come la Corte Internazionale di Giustizia abbia fatto ricorso a tali principi con estrema cautela. Benchè taluni giudici della Corte nelle opinioni dissidenti abbiano non di rado invocato i principi generali, la maggioranza della Corte non sembra mai aver basato una sua pronuncia esclusivamente su uno di tali principi, né aver mai invocato a sostengno di una sua decisione la disposizione dellìart. 38 let. C). inoltre quanto la corte ha applicato un principio generale di diritto lo ha fatto per lo più ad abundantiam, cioè per confermare un risultato già raggiunto. Inoltre, quando un principio è stato applicato la Corte si è astenuta da analisi di diritto comparato.

[366] C. FOCARELLI, *Diritto Internazionale*, CEDAM, Milano, 2019, p. 150

[367] In particolare possono ricondursi tra i principi generali evocati dalla Corte Penale di Giustizia Internazionale i principi: i) kompetenz-kompetenz (SENTENZA del 1926 relativa all'Accordo Greco-Turco) ; ii) nemo iudex in res sua (PARERE del 1925 sull'interpretazione dell'art. 3 p.2 dell'Accordo di Losanna); iii) rispetto dei diritti acquisisti (PARERE del 1926 sugli interessi della Germania nell'Alta slesia polacca); iv) principio della riparazione (SENTENZA del 1928 relativa all'Officina di Chorzow). Successivamente la Corte Internazionale di Giustizia ha richiamato i principi: i) res iudicata(SENTENZA del 1949 sullo Stretto di Corfù); ii) il principio Estoppel (SENTENZA del 1960 sul Tempio di Preah Vihear): iii) il principio ex iniura jus non oritur; iv) il principio secondo cui uno Stato non si può sottrarre alla competenza della Corte attraverso la revoca della sua accettazione allorchè la giurisdizione esisteva al momento del ricorso (SENTENZA del 1960 sul diritto di passaggio); v) la Corte di Giustizia Internazionale ha invece escluso che il principio di buona fede sia in se una fonte di obbligazione nel caso in cui non ve ne siano altre (SENTENZA del 1986 caso Nicaragua vs Stati Uniti) .

della consuetudine internazionale. Permettono infatti, di far riferimento non soltanto alla prassi degli Stati sul piano delle relazioni internazionali esterne ma anche alla loro prassi sul fronte dei rispettivi ordinamenti interni così ampliando l'area di rilevazione delle norme di diritto internazionale generale. Ciononostante, il loro ruolo è venuto progressivamente regredendo ma mano che l'esistenza di regole nella vita di relazione internazionale ha potuto essere attestata non più con riferimento a siffatti principi, ma con un diretto riferimento alla prassi. Ciò appare evidente nelle materie storicamente rientranti nel diritto internazionale e concernenti le relazioni interstatali. Il limitato ruolo dei principi generali dipende dalla crescente eterogeneità della Comunità Internazionale, derivante dalla coesistenza di Stati con regimi economici e sociali divergenti e con un diverso livello di sviluppo giuridico politico economico e sociale. Contesto questo in cui risulta molto difficile rinvenire principi comuni.

Diversamente nei nuovi ambiti di sviluppo del diritto internazionale, in particolare relativi alla disciplina delle persone fisiche e giuridiche e del diritto internazionale penale, i principi generali di diritto rivestono un ruolo particolarmente importante stante l'assenza di precedenti desumibili direttamente ed esclusivamente dal diritto internazionale generale. In questi casi si tratta di disciplinare fattispecie concrete, riguardanti persone fisiche e giuridiche, analogamente a quanto accade negli ordinamenti nazionali[368].

Per questa ragione l'uso dei principi generali di diritto è molto frequente nel diritto internazionale penale sia in seno elle organizzazioni internazionali. Infatti, negli ordinamenti particolari istituiti da queste organizzazioni i fattori di analogia si moltiplicano dato che gli stessi parzialmente si ispirano a modelli statali sia per quanto riguarda le modalità di esercizio delle loro competenze sia per i mezzi di azione e le regole di funzionamento.

Rispetto alle problematiche poste dall'azione degli attori nel cyberspace lo spazio in cui possono trovare applicazione i principi generali di diritto appare limitato. In particolare, essi acquisiscono rilevanza *"when disputes between states over cyber matter arise"*[369].

---

[368] C. FOCARELLI, *Diritto Internazionale*, CEDAM, Milano, 2019.

[369] M. N. SCHIMTT, L. VIHUL, *The Nature of International Law Cyber Norms*, in, a cura di ANNA MARIA OSULA E HENRY ROIGAS, *International cyber Norms. Legal, Policy & Industry Perspective*, NATO CCDCOE COE Pubblications, Tallin, 2016, p.46

Ciononostante, i documenti analizzati hanno mostrato l'importanza attribuita, da un lato, alle procedure di partecipazione dei diversi stakeholder alla governance del cyberspace e, dall'altro, alla definizione e applicazione di procedure di controllo e verifica della progettazione, sviluppo e utilizzo delle tecnologie ITC nei diversi settori. In entrambi i casi, il progresso tecnologico impone costanti evoluzioni le cui incertezze possono essere affrontate attraverso il ricorso ai principi generali di diritto, in particolare per quanto riguarda il piano procedurale. Appare infatti evidente l'applicabilità, ad esempio, del principio *nemo iudex in res sua* nel contesto di un processo di verifica e controllo delle varie fasi di progettazione, sviluppo ed utilizzo di un sistema d'arma letale autonomo sul quale tuttavia gli Stati hanno interesse ad incidere limitando ed escludendo l'intervento di soggetti terzi. Allo stesso modo i principi indicati possono contribuire a definire i caratteri della partecipazione di attori non statali all'interno dei processi di governance sviluppati sul piano multilaterale e a stabilire standard comuni rispetto alle problematiche di natura penale legate alla criminalità informatica.

Gli attuali sviluppi del diritto internazionale del cyberspace così come la tendenza degli Stati a mantenere una stretta riservatezza sulle attività cyber più sensibili, non permette di rilevare la misura dell'importanza che tali principi di diritto possono acquisire in questo nuovo contesto. È tuttavia possibile individuare nel soft law delle organizzazioni internazionali, in particolare nelle Confidence Building Measures e nei sistemi multistakeholder, i principali ambiti di sviluppo dei principi di diritto internazionale all'interno della disciplina del cyberspace.

1.4 Il Soft Law

La presenza e l'azione nella Comunità Internazionale delle organizzazioni internazionali ha introdotto e impresso alcuni elementi nuovi nel diritto internazionale, in particolare rispetto ai processi di formazione normativa. Elementi che acquisiscono rilevanza nel contesto del cyberspace in ragione della maggior flessibilità che caratterizza il loro processo di formazione e applicazione.

Per funzione normativa[370] delle organizzazioni internazionali si intende l'attività formale diretta a disciplinare il funzionamento interno dell'organizzazione[371] e, più spesso, a indirizzare e determinare i comportamenti degli Stati nei loro reciproci rapporti o, meno frequentemente, nei confronti di soggetti degli ordinamenti interni quali le persone fisiche e le persone giuridiche[372].

Attraverso i diversi atti[373] emanati dalle organizzazioni internazionali vengono dunque poste norme di diritto derivato il cui

[370] La funzione normativa delle organizzazioni internazionali deve distinta da altre funzioni quali: i) le funzioni materiali, alcune delle quali aventi carattere preparativo all'esercizio di funzioni normative; ii) le funzioni operative, che comprendono l'attività diretta esplicata dalle organizzazioni internazionali, ad esempio in un dato territorio; iii) infine, le funzioni di controllo nei confronti degli Stati Membri rispetto all'adempimento degli obblighi statutari a cui vanno affiancate le funzioni sanzionatorie.

[371] Il potere di autoregolamentazione delle organizzazioni internazionali è spesso previsto nell'atto costitutivo dell'organizzazione, ma può anche essere considerato implicito alla luce dell'esigenza di permettere il funzionamento dell'ente. Agli atti interni delle organizzazioni deve essere riconosciuta portata obbligatoria, come ha affermato la CORTE INTERNAZIONALE DI GIUSTIZIA nel *Parere sugli effetti delle decisioni di indennizzo da parte del tribunale amministrativo delle Nazioni Unite* del 1954.

[372] Gli atti delle organizzazioni internazionali si traducono in manifestazioni di volontà che enunciano in un testo scritto regole di condotta, indirizzate o agli organi delle organizzazioni o agli Stati Membri o, meno frequentemente, ai loro cittadini. Gli atti di natura vincolante possono avere a carico degli Stati Membri sia un effetto reale che un effetto obbligatorio. Nel primo caso non è necessario alcun provvedimento dello Stato perché l'atto possa produrre i suoi effetti; nel secondo caso, che è molto più frequente, l'emanazione dell'atto da parte delle organizzazioni comporta l'obbligo per gli Stati di adottare i necessari procedimenti interni di esecuzione ed attuazione. Con riferimento agli atti vincolanti viene in rilievo la Carta delle Nazioni Unite la quale prevede la vincolatività di una serie di atti dell'organizzazione. In particolare, l'art. 17 attribuisce all'Assemblea Generale il potere di approvare il bilancio ONU e di decidere la ripartizione delle relative spese. Di maggior rilievo, tuttavia, le norme del Capo VII Carta ONU, con particolare riferimento all'art. 41, che attribuisce al Consiglio di Sicurezza il potere di adottare misure non implicanti l'uso della forza e di imporle a tutti gli Stati Membri. La portata obbligatoria di tali decisioni è determinata dall'art. 25 il quale prevede che gli Stati Membri convengono di accettare e realizzare le decisioni del Consiglio di Sicurezza. L'art. 50 prevede inoltre che il mancato adempimento può essere segnalato allo Stato Membro e giustificato per ragioni economiche. Rileva infine l'art. 94 par. 2 che attribuisce al Consiglio di sicurezza il potere di decidere oltre che di raccomandare, misure per obbligare uno Stato condannato dalla Corte Internazionale di Giustizia ad adempiere la sentenza di condanna, ove non lo faccia spontaneamente e su richiesta dello Stato a favore del quale la sentenza è stata emessa. Infine, occorre rilevare come atti giuridicamente vincolanti possano essere adottati da alcuni istituti specializzati delle Nazioni Unite su questioni di natura essenzialmente tecnica. Tra questi rientrano gli atti dell'Organizzazione mondiale della Sanità, dell'Organizzazione Internazionale del Lavoro, dell'Organizzazione Internazionale dell'Aviazione Civile e, di particolare interesse nel contesto del cyberspace gli atti dell'Unione Internazionale delle Comunicazioni.

[373] In merito alla classificazione degli atti delle organizzazioni internazionali si deve far riferimento non già alle caratteristiche formali dell'atto, quindi al suo *nomen juris*, bensì ai suoi caratteri sostanziali, ossia agli effetti che l'atto produce. Relativamente alla qualificazione degli

fondamento riposa nel Trattato istitutivo dell'organizzazione il quale ne definisce i procedimenti di formazione.

In questo contesto, con l'espressione *Soft Law* si intende far riferimento a quei fenomeni giuridici diversi dai tradizionali strumenti normativi di *Hard Law*, la cui caratteristica essenziale è data dal fatto di essere privi di efficacia vincolante. Si tratta di proposizioni aventi la struttura logica delle vere e proprie norme giuridiche vincolanti: un dato comportamento viene infatti indicato come doveroso. Tale doverosità si colloca però ad un livello diverso da quello proprio dell'obbligo giuridico, risolvendosi nell'indicazione dei comportamenti meramente raccomandati oppure delineati come doverosi dal punto di vista morale, sociale e politico. Il soft law, in altri termini, non impone obblighi ma si limita a suggerire parametri di comportamento per gli Stati[374].

---

atti delle organizzazioni internazionali regnano infatti, incertezze terminologiche e ambiguità concettuali. Un atto denominato allo stesso modo in due organizzazioni internazionali può avere effetti sostanzialmente diversi nell'una e nell'altra. Allo stesso modo è possibile che atti con effetti identici vengano denominati differentemente. Talvolta i trattati istitutivi delle organizzazioni internazionali si esprimono in termini assai vaghi, disponendo la competenza dell'organizzazione in una certa materia ad assumere, ad esempio, *disposizioni*[373] (Cfr. Art. 68 e 70 Carta Nazioni Unite), ad intraprendere *opportune iniziative* o a fornire *suggerimen*ti. Si pensi poi all'Assemblea Generale delle Nazioni Unite che denomina talune sue risoluzioni *dichiarazioni*, altre *carte*, altre ancora *programmi d'azione*. In questo senso la Corte di Giustizia dell'Unione Europea al fine di identificare gli effetti dell'atto attribuisce valore preminente ai suoi caratteri sostanziali, a prescindere dalla sua denominazione sulla base della c.d. teoria dello smascheramento implicito (ANTONIO TIZZANO, ROBERTO ADAM, *Manuale di diritto dell'Unione Europea,* G. Giappichelli Editore, 2017).

[374] Il Soft Law trova i suoi strumenti in una pluralità di atti i cui caratteri distintivi sono determinati dai caratteri dell'ente regolatore internazionale che li ha adottati. Rilevano, in primo luogo, le dichiarazioni statali di intenti, le dichiarazioni congiunte, gli atti adottati dalle conferenze internazionali e ogni altro atto che, pur proponendosi di creare una certa aspettativa di comportamento, non costituisce un trattato vero e proprio. In secondo luogo, vengono in rilievo le c.d. intese politiche che non creano obblighi giuridici tra le parti contraenti ma solo impegni giuridici il cui rispetto è rimesso alla volontà delle parti (Cfr. ad esempio OSCE, Atto finale di Helsinki del 1975). Infine, sono strumenti di soft law, gli accordi politici e i memorandum d'intesa adottati in ambito di riunioni stabili e permanenti o conferenze istituzionalizzate. Nell'ambito della più generale categoria del soft law si è imposto all'attenzione il livello più alto rappresentato dal diritto dei raggruppamenti internazionali di natura presidenziale, espressione di conferenze o riunioni periodiche del più alto livello capi di stato e di governo e definito da parte della dottrina come diritto presidenziale o *Top Law*. Nel quadro degli atti di soft law rientrano anche gli atti non vincolanti delle organizzazioni internazionali adottati nell'ambito dell'attività c.d. para normative. Benché generalmente trascurati dalla dottrina in quanto non corrispondono ad una categoria giuridica omogenea, esse sono nella pratica dotate di una grande importanza per l'armonizzazione progressiva delle condotte e soprattutto delle legislazioni nazionali degli Stati Membri nei più disparati settori tecnici. Tali attività para normative, che sono in particolare poste in essere dalle istituzioni specializzate delle Nazioni Unite, si traducono in una abbondante produzione di standard di riferimento, nella definizione delle linee direttrici dello sviluppo delle legislazioni nazionali. Tali attività vengono realizzate attraverso l'elaborazione di codici, messi a disposizione degli

I motivi che hanno determinato lo sviluppo degli atti di soft law sono essenzialmente riconducibili all'universalizzazione della Comunità Internazionale. Fattore il quale, come abbiamo visto, si pone alla base delle problematiche delle fonti giuridiche del diritto internazionale. Problematiche poste dalle emergenti esigenze connesse alle profonde trasformazioni economiche, sociali, culturali e tecnologiche della seconda metà del Novecento e che attualmente trovano un nuovo fattore di sviluppo nel processo di affermazione del cyberspace e, con esso, della Società dell'Informazione.

Questo insieme di fattori ha portato allo sviluppo nel diritto internazionale degli atti di soft law le cui caratteristiche rispondono alle esigenze della Comunità Internazionale moderna. Si tratta infatti di atti flessibili, più facili da adottare in relazione a tematiche sulle quali gli Stati non sono in grado di raggiungere una convergenza di vedute tale da condurre alla stipulazione di accordi internazionali. Sono inoltre atti più rapidi da preparare e più facili da modificare, soprattutto in materie tecniche che richiedono revisioni costanti in funzione dello sviluppo tecnologico. Atti infine, comunque capaci di esercitare, sia pure in misura diversa a seconda delle circostanze, una pressione sugli Stati che non li condividono senza provocare il loro aperto dissenso[375].

Stati a titolo puramente indicativo, sia attraverso risoluzioni sia, più semplicemente, attraverso pubblicazioni dirette provenienti dal segretario dell'organizzazione. È questo il caso, ad esempio, della AIEA, che emette norme di radioprotezione relative alla protezione contro il rischio nucleare che sono frequentemente riprese dagli Stati Membri nelle loro legislazioni nazionali, tanto è riconosciuta la loro autorità scientifica. Egualmente l'Organizzazione Internazionale del Lavoro, l'Organizzazione Mondiale della Sanità o l'Organizzazione delle Nazioni Unite per l'Alimentazione e l'Agricoltura, svolgono attività di questo genere che possono considerarsi quali intermedie tra l'azione normativa e quella operativa. Nel quadro del soft law può essere ricondotta anche la *lex mercatoria*, di cui un esempio sono i principi UNIDROIT, generalmente definita come quel corpo di regole aventi diversa origine e contenuto creata dalla comunità dei commercianti per servire i bisogni del commercio internazionale.

[375] Per quanto riguarda gli effetti prodotti dagli atti di soft law il problema si è posto principalmente rispetto agli atti non vincolanti delle organizzazioni internazionali. Anzitutto può dirsi che il contenuto delle raccomandazioni diviene vincolante perché mutuato da un atto diverso avente natura vincolante. Ciò è avvenuto per molte risoluzioni dell'Assemblea Generale delle Nazioni Unite il cui contenuto è stato successivamente trasfuso in un trattato internazionale. Non si è in queste ipotesi, né in altre analoghe, in presenza di raccomandazioni che producono effetti obbligatori, dato che questi effetti promanano dall'atto giuridico vincolante successivamente adottato. La dottrina, tuttavia, ha cercato di rinvenire un qualche effetto obbligatorio riconducibile direttamente agli atti di soft law adottati dall'organizzazione internazionale, in particolare nel caso delle raccomandazioni che vadano oltre la mera esortazione politica. Da una parte, ciò è funzionale a dare un qualche valore alla mole di atti prodotti dalle organizzazioni internazionali, dall'altra è funzionale a riconoscere a quest'ultime un potere decisionale più esteso in grado di limitare o di condizionare il potere dei singoli Stati. In particolare, è stato sostenuto che la raccomandazione sarebbe vincolante almeno per gli Stati

Il principale effetto riconducibile al soft law è, dunque, legato al contributo che esso può dare alla formazione di una norma di diritto internazionale generale. Le dichiarazioni di principio e le raccomandazioni delle organizzazioni internazionali possono esprimere l'*opinio juris* della maggioranza degli Stati della Comunità Internazionale e, a tale titolo, contribuire alla rilevazione del diritto internazionale generale. Nulla esclude poi che tali dichiarazioni, nella misura in cui riflettano non solo l'opinio juris ma anche la prassi generalizzata e costante della generalità degli Stati, possano codificare il diritto consuetudinario[376].

La rilevanza del soft law nella Comunità Internazionale moderna si spiega, quindi, in una prospettiva dinamica delle fonti del diritto internazionale generale. Le "raccomandazioni" per definizione non creano diritto, non producono effetti giuridici di alcun tipo. Ma, dati i caratteri dell'ordinamento giuridico internazionale, le raccomandazioni potrebbero essere seguite dagli Stati anche in misura maggiore rispetto agli atti vincolanti. Inoltre, quando non riproducono già il diritto vigente, le raccomandazioni promuovono un nuovo diritto

---

che hanno votato a favore della sua adozione in seno agli organi che l'hanno emanata. Allo stesso modo la reiterazione di una raccomandazione finirebbe con il far diventare il comportamento esortato come giuridicamente dovuto. Infine, è stata sostenuta la vincolatività delle raccomandazioni che confermano gli obiettivi dell'organizzazione internazionale fissati nel Trattato Istitutivo. Parte della dottrina ha invece posto l'accento sul c.d. *effetto di liceità* delle raccomandazioni internazionali ritenendo che non commetta illecito lo stato il quale, per eseguire una raccomandazione di un'organizzazione internazionale, tenga un contegno contrario ad impegni in precedenza assunti mediante accordi od obblighi derivanti dal diritto internazionale consuetudinario. L'effetto di liceità, tuttavia, non ha valore assoluto ma vale soltanto nei confronti degli Stati Membri dell'organizzazione internazionale e può verificarsi soltanto in presenza di raccomandazioni legittime, ossia di raccomandazioni che rientrano nell'ambito delle competenze degli organi e siano rispettose del dettato del trattato istitutivo. Inoltre, l'effetto di liceità può verificarsi solo tra quegli Stati Membri che abbiano votato a favore delle raccomandazioni. Il fondamento giuridico dell'effetto di liceità discende dall'obbligo di cooperare con l'organizzazione internazionale che è implicito in ogni trattato istitutivo.

[376] In questo senso nel 1986 il Tribunale Iran-Usa ha dichiarato che le risoluzioni dell'Assemblea Generale delle Nazioni Unite non sono direttamente vincolanti per gli Stati Membri e non sono in genere prova del diritto consuetudinario. Ciò non di meno è generalmente accettato che tali risoluzioni, in circostanze specifiche, possono venire considerate come prova del diritto internazionale consuetudinario o possono contribuire insieme ad altri fattori alla creazione di un diritto. Nel 1986 la Corte Internazionale di Giustizia, nel caso Nicaragua vs USA, ha affermato che, sia pure con la prudenza necessaria, il consenso degli Stati alle risoluzioni può servire ad accertare l'*opinio iuris* relativo all'esistenza di norme generali. Nella stessa prospettiva *l'Institut de Droit International* nel 1987 ha affermato che l'Assemblea Generale può fare raccomandazioni che contribuiscono allo sviluppo progressivo del diritto internazionale, al suo consolidamento e alla sua codificazione, così distinguendo le risoluzioni che dichiarano il diritto da quelle che sviluppano il diritto.

internazionale ritenuto più giusto dalla Comunità Internazionale tanto più se adottato dall'Assemblea Generale. Nel promuovere il diritto futuro le raccomandazioni lo avverano. Così esercitando una sorta di pressione d'alto sugli Stati.

Rispetto al cyberspace i documenti presi in considerazione permettono di tratteggiare la rilevanza della funzione normativa di secondo grado all'interno del processo di sviluppo della disciplina giuridica dell'azione degli attori nel dominio informatico.

Il diritto derivato concorre al processo di definizione della disciplina giuridica delle azioni nel cyberspace apportandovi i caratteri della flessibilità, della specializzazione e della pervasività, attraverso cui la complessiva funzione normativa della Comunità Internazionale può esplicarsi rispetto alla pluralità di tematiche su cui incidono gli sviluppi della scienza e della tecnica.

Allo stesso tempo, trovando fondamento in ordinamenti giuridici internazionali già delineati e consolidati, le norme secondarie permettono di ricondurre lo sviluppo della disciplina giuridica del cyberspace e la sua applicazione entro il sistema multilaterale delle relazioni internazionali. La funzione che esse svolgono rispetto alla dimensione organizzativa e funzionale delle organizzazioni internazionali, permette concretamente di ricondurre entro i tempi e gli strumenti propri del sistema multilaterale lo sviluppo della disciplina giuridica dell'azione degli attori nel cyberspace.

Infine, il contributo che gli atti di soft law forniscono sul piano della rilevazione della formazione del diritto generale concorre a consolidare i valori, i principi, le finalità definite dalla Comunità Internazionale moderna, in un contesto, quale quello del cyberspace, caratterizzato da un'ampia varietà di interpretazioni e prospettive sorrette da valori tra di essi contrastanti.

Rispetto alle dinamiche relazionali del cyberspace caratterizzate, come visto, da un carattere sostanzialmente conflittuale, il soft law svolge una funzione similare a quella svolta rispetto allo sviluppo degli armamenti nucleari. In entrambi i casi la loro principale funzione riposa nella definizione delle norme di comportamento dei diversi attori[377].
Le dinamiche economiche, sociali e culturali, legate allo sviluppo del cyberspace, evidenziano, inoltre, l'ulteriore funzione di tale tipologia di

[377] Michael S. Rogers, A conversation whit Mike Roger's, Cybersecurity for a New America: big ideas and new voice, February 23, 2015, consultabile all'indirizzo https://www.newamerica.org/cybersecurity-initiative/events/cybersecurity-for-a-new-america/

norme volta a delineare valori comuni in grado di sostenere lo sviluppo della disciplina giuridica del cyberspace.

I lavori delle Nazioni Unite mostrano la particolare attenzione rivolta allo sviluppo di Confidence Building Measures (CBM's). Un'attenzione che, allo stesso modo, caratterizza l'azione di organizzazioni regionali quali l'OSCE, l'ASEAN Regional Forum e l'Organizzazione degli Stati Americani.

I report dei Gruppi di Esperti, le risoluzioni dell'Assemblea Generale e degli altri organismi delle Nazioni Unite, così come le dichiarazioni finali dei summit e delle conferenze svolte nei diversi fori internazionali, contengono raccomandazioni dettagliate rivolte agli Stati che sono chiamati a darvi seguito. Attraverso gli atti di soft law viene dunque indirizzata l'azione degli Stati chiamati, rispetto alle problematiche del cyberspace, ad adottare una serie di misure di azione e di cooperazione volte a garantire un utilizzo pacifico degli strumenti informatici, la sicurezza dello spazio informatico e delle infrastrutture che lo sorreggono così come il rispetto nei diritti umani.

Entro questa prospettiva, gli atti delle Nazioni Unite presi in considerazione, permettono di delineare, le forme e i modi in cui si concretizza la funzione attribuita al diritto internazionale derivato.

2. *Problemi di interpretazione e applicazione del diritto internazionale al cyberspace.*

Le problematiche emerse nel sistema delle fonti internazionali conseguentemente all'affermarsi del cyberspace si riverberano sul processo di definizione della disciplina giuridica applicabile alle azioni condotte dagli attori in tale spazio relazionale.

Gli Stati, infatti, ribadita l'applicabilità del diritto internazionale, sia convenzionale che pattizio, esprimono posizioni e prospettive interpretative differenti circa il concreto operare delle norme internazionali nello spazio informatico.

Nei successivi paragrafi verranno delineate le principali questioni emerse rispetto all'interpretazione e all'applicazione del diritto internazionale. Questioni che saranno suddivise con riferimento alle tre aree tematiche alle quali si è ricondotta l'azione delle Nazioni Unite e analizzate a partire da quanto sopra esposto in merito al sistema delle fonti internazionali.

2.1 Tutela della sicurezza e della pace internazionali.

Il rapporto tra progresso tecnologico e i temi della sicurezza e della pace internazionale è stato evidenziato dall'Assemblea Generale delle Nazioni Unite fin dalla sua prima risoluzione in materia, nella quale si dichiarava preoccupata per il crescente utilizzo delle tecnologie ITC per finalità incompatibili con il mantenimento della sicurezza e della pace internazionale[378]. Una tendenza evidenziata anche nel Rapporto del Gruppo di Esperti presentatole nel 2010 nel quale veniva rilevato che: *"il est de plus en plus souvent signalé que des Etats développent des techniques informatiques comme instruments de guerre et de reinsigment, ainsi que des fins politiques"*[379].

I successivi lavori dei Gruppi di Esperti istituiti dall'Assemblea Generale hanno consolidato il generale consenso circa l'applicabilità al cyberspace dei principi consuetudinari di sovranità, di due- diligence, del divieto dell'uso della forza e del diritto di autodifesa in quanto essenziali allo sviluppo di relazioni internazionali pacifiche.

---

[378] NAZIONI UNITE, ASSEMBLEA GENERALE, *Risoluzione n. 53/70* del 1998
[379] NAZIONI UNITE, ASSEMBLEA GENERALE, *GGE Report A/65/201*, par. 7

A tale scopo risponde, anzitutto, il principio consuetudinario della Sovranità, intesa come *"il diritto di esercitare le funzioni statali su una data porzione del globo con l'esclusione di ogni altro Stato*". Diritto a cui fa da corollario "*l'obbligo di proteggere entro il territorio il diritto di altri Stati, in particolare il loro diritto all'integrità e inviolabilità in tempo sia di pace che di guerra, insieme ai diritti che ogni Stato può rivendicare per i suoi cittadini in territorio straniero"*[380].

Cardine delle relazioni interstatali, in esso trovano fondamento ulteriori principi e norme internazionali volte a disciplinare l'esercizio dei poteri sovrani sia nella loro dimensione interna che in quella esterna. All'interno degli ordinamenti statali il principio di sovranità si concretizza, da un lato, nel diritto di esercitare i pubblici poteri e, dall'altro, nel rispetto degli obblighi derivanti dal principio di due diligence e dalle norme convenzionali relative ai diritti dell'uomo.

Allo stesso modo, sul piano delle relazioni esterne, derivano da esso i principi di uguaglianza tra gli Stati e di non ingerenza così come i principi del divieto di uso della forza e del diritto di autodifesa.

Le fattispecie emergenti nel cyberspace pongono in discussione gli assunti finora consolidati rispetto all'oggetto dei poteri sovrani e ai presupposti per il loro esercizio con riferimento ai principi e alle norme internazionali indicate.

In termini generali si può osservare come le caratteristiche strutturali e dinamiche del cyberspace richiedano di reinterpretare il contenuto del principio di sovranità in considerazione della rilevanza acquisita dalle infrastrutture ITC e dal loro utilizzo svincolato dai confini territoriali degli Stati. Allo stesso modo, i caratteri delle attività condotte nello spazio informatico, determinando lo sviluppo di nuove forme di esercizio della forza, introducono nuovi fattori di complessità nei processi di rilevazione e qualificazione giuridica delle azioni lesive del diritto internazionale.

In particolare, la natura di infrastruttura di infrastrutture propria delle tecnologie ITC amplia, in primo luogo, l'area dell'interesse nazionale, potendo esservi ricondotte tanto le nuove infrastrutture quanto le relazioni economiche, politiche, sociali e culturali sviluppate attraverso le tecnologie dell'informazione. In secondo luogo, introducendo nuovi fattori di potenza amplia, da una parte, le azioni suscettibili di costituire una violazione del divieto di intervento negli affari interni di uno Stato

[380] CORTE PERMANENTE DI ARBITRATO, *Sentenza caso Isola di Palmas*, 1928

e del divieto di uso della forza e, dall'altra, i presupposti per l'esercizio del diritto all'autodifesa.

Entro questo quadro generale si può rilevare come la disciplina giuridica dell'azione degli attori nel cyberspace, pur poggiando su riferimenti consolidati, condivide con il dominio informatico il carattere dell'incertezza.

2.1.1 La sovranità quale norma primaria o principio generale

Il primo elemento di incertezza si registra con riferimento allo stesso concetto di sovranità declinato, nella prima versione del Manuale di Tallinn, nel senso che *"a State may exercise control over cyber infrastructures and activities whitiin its sovereign territory"*[381].

Il commento alla norma chiariva come una cyber operation in grado di causare danni fisici ad infrastrutture cyber, sia pubbliche che private, costituisce una violazione della sovranità dello Stato nel quale sono condotte determinando un illecito internazionale, così sorreggendo l'adozione di contromisure e l'esercizio del diritto di autodifesa. Viene inoltre sottolineata la rilevanza delle sole cyber operation condotte da soggetti statali in ragione dell'embrionale sviluppo delle capacità cyber nel campo militare di soggetti privati.

La successiva versione del Manuale di Tallinn pubblicata nel 2017 approfondisce la questione in oggetto nell'analisi delle Rule 2 *"Internal sovereignty"* e della Rule 4 *"Violation of sovereignty"*.

La prima declina la Sovranità nel senso che lo Stato è libero di esercitare la propria autorità *"whit regard to the cyber infrastructures, person, and cyber activities located whitin its territory, subject to its international legal obbligations"*[382].

La seconda prevede che *"a State must not conduct cyber operation that violate the sovereignty of another State"*[383].

Inoltre, il commento alla norma afferma, in termini generali, che le *"cyber operations that prevent or disregard another State's exercise of*

---

[381] MICHAEL N. SCHMITT, *Tallinn Manual on the International law applicable to cyber warfare*, Cambridge University Press,2013, Rule 1.

[382] MICHAEL N. SCHMITT, LIIS VIHUL, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*, Cambridge University press, 2017, Rule 2

[383] MICHAEL N. SCHMITT, LIIS VIHUL, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*, Cambridge University press, 2017, Rule 4

its sovereign prerogative constitute a violation of such sovereignty and are prohibited by international law".

Il Manuale di Tallinn sembra riflettere l'idea che la sovranità consista sia in un principio di diritto internazionale sul quale fondano determinate norme (non ingerenza, divieto di uso della forza, auto-difesa), sia in una norma primaria di diritto internazionale suscettibile in di essere violata. Tuttavia, il principale problema che si pone il Manuale di Tallinn 2.0 attiene piuttosto all'identificazione dei tipi di operazioni informatiche che, oltrepassando il limes della liceità, determinano le condizioni per l'uso della forza[384].

In questo senso il commento alla Rule 4, chiarisce che la violazione della sovranità dipende (i) dal grado di violazione dell'integrità territoriale dello Stato bersaglio e (ii) da un'interferenza o un'usurpazione della sua funzione di governo[385].

Tale ricostruzione presenta tuttavia alcuni punti controversi con riferimento ai parametri adottati per la valutazione delle azioni cyber. Rispetto al primo punto vengono considerate dannose le attività in grado di incidere in modo relativamente permanente sulla funzionalità dell'infrastruttura colpita. Tuttavia, non vi è accordo tra gli esperti sulla qualificazione degli scopi e del concetto di perdita di funzionalità di cui al punto due. Allo stesso modo rimane incerta la nozione di funzione governativa intrinseca.

Il Manuale di Tallinn ha dato avvio ad un intenso dibattito tra accademici, professionisti e commentatori. Di particolare rilievo la discussione svoltasi durante tre meeting internazionali convocati dal Ministero degli Affari Esteri olandese nel 2015 e nel 2016, ai quali hanno partecipato altre cinquanta tra Stati e Organizzazioni Internazionali. In questa sede non si sono registrate significative obiezioni all'impostazione data dal Manuale di Tallinn, mentre maggiore attenzione è stata posta all'applicazione di specifiche norme a specifiche situazioni quali, in particolare, le azioni poste in essere da attori non statali[386].

---

[384] MICHAEL SCHMITT, *In defence of Sovereignty in Cyberspace*, justsecurity.org, may 8, 2018, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

[385] MICHAEL N. SCHMITT, LIIS VIHUL, *Sovereignty in cyberspace: lex lata vel non?* in THE AMERICAN SOCIETY OF INTERNATIONAL LAW, *Symposium on Sovereignty, cyberspace and Tallinn Manual 2.0*, 2017; Michael Schmitt, In defence of sovereignty in cyberspace, Just Security, May 8, 2018, http://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

[386] MICHAEL SCHMITT, *The Tallin Manual 2.0 on the International Law of Cyber Operation: What it is and isn't*, Just Security, 9 Feb. 2017, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ [http://perma.cc/5YRS-F5TB]; ASSER

Tuttavia il punto centrale, sul quale si è sviluppato un rilevante dibattito dottrinale, ruota intorno alla qualificazione della Sovranità quale norma primaria del diritto internazionale applicabile alle operazioni informatiche, la cui violazione costituisce di per sé un atto illecito a livello internazionale, o, diversamente, quale principio fondamentale, che potrebbe essere violato solo violando altre norme primarie basate sulla sovranità (divieto di intervento, divieto dell'uso della forza) [387].

Quanti ricostruiscono la sovranità quale principio muovono dalla norma dell'art. 2 comma 4 della Carta delle Nazioni Unite secondo cui *"i Membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza contro l'integrità territoriale"*. La sovranità è qui intesa come legata al territorio e la sua lesione è ricondotta alla violazione del divieto di uso e minaccia della forza. Entro questa prospettiva il Limes della liceità di questi due atti non viene ricondotta all'operatività del principio stesso.

Tale posizione viene argomentata[388] muovendo dalla prassi registrata relativamente alle attività di spionaggio rispetto le quali si osserva che violino il diritto internazionale solo quando condotte con modalità che costituiscono una violazione di specifiche previsioni di diritto internazionale, quali, appunto il divieto di intervento e di uso della forza.

Inoltre, prendendo in analisi i diversi modi in cui la sovranità è declinata nel diritto internazionale rispetto ai domini spaziale, aereo e marino, la sovranità e ricostruita quale principio soggetto ad aggiustamenti in funzione dei caratteri e dei problemi del dominio di riferimento. Inoltre, lo sviluppo di differenti regimi non permette di qualificare il principio di sovranità quale norma primaria di chiara applicazione nel dominio cyber.

Infine, viene rilevato come non vi siano prove sufficienti né della prassi né dell'opinio juris a sostegno dell'affermazione secondo cui il principio di sovranità funzioni come regola primaria indipendente dal diritto internazionale che regola l'azione degli Stati nel cyberspace.

INSTITUTE, *The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime*, Report https://www.asser.nl/about-the-institute/asser-today/the-tallinn-manual-20-and-the-hague-process-from-cyber-warfare-to-peacetime-regime/

[387] PHIL SPECTOR, *In defence of sovereignty, cyberspace, and Tallinn Manual 2.0*, in THE AMERICAN SOCIETY OF INTERNATIONAL LAW, *Symposium on Sovereignty, cyberspace and Tallinn Manual 2.0,* 2017

[388] GARY P. CORN, ROBERT TAYLOR, *Sovereignty in the age of cyber*, in THE AMERICAN SOCIETY OF INTERNATIONAL LAW, *Symposium on Sovereignty, cyberspace and Tallinn Manual 2.0,* 2017

Diversamente, quanti sostengono l'idea della sovranità quale norma primaria ritengono di poter fondare le proprie argomentazioni su una più consistente base che *"support the assertion that a primary rule non to violate the territorial sovereignty of other States exist"*[389]

In primo luogo, viene sottolineato come lo stesso articolo 2, della Carta delle Nazioni Unite riconosca, al comma 1, che "*l'Organizzazione è fondata sul principio della sovrana uguaglianza di tutti i suoi Membri",* in tal modo delineando per la sovranità un carattere autonomo, slegato dalla componente territoriale e dal rispetto di specifiche norme internazionali. Allo stesso modo viene richiamata la Dichiarazione ONU sulle Relazioni amichevoli e la cooperazione tra Stati, sottolineando che essa tratta del principio di sovrana uguaglianza in maniera autonoma individuandone una serie di elementi qualificanti, inclusa l'idea che ogni Stato gode dei diritti inerenti alla piena sovranità, oltre all'inviolabilità dell'integrità territoriale e politica degli Stati[390]. Inoltre, si ritiene che la giurisprudenza internazionale abbia ulteriormente chiarito il punto individuando la principale restrizione imposta agli Stati dal diritto internazionale nel divieto di esercitare i propri poteri in ogni forma, all'interno del territorio di un altro Stato[391]. Sovranità territoriale che consiste nel diritto di esercitare in via esclusiva le funzioni Statali[392]. Infine, si ritiene che la dottrina riconosca l'esistenza di una norma primaria vincolante di diritto internazionale riguardante la sovranità territoriale rilevando come il diritto internazionale tradizionale si basava su un insieme di regole che stabilivano l'uguaglianza giuridica degli Stati e ne proteggevano la sovranità la quale include, tra gli altri, il c.d. *jus excludendi alios*[393].

Entro una prospettiva generale è stato evidenziato come *"whether one chose to call it soverignty, or territorial sovereignty, or territorrial integry, or something else entirely, an overwhelming and unavoidable body of treaties, jurisprudence, and scholary opinion stands for the proposition that there is a primary rule of international law that requires one state to refrain from taking a pubblic act or exercising*

---

[389] MICHAEL N. SCHMITT, LIIS VIHUL, *Respect for Sovereignty in Cyberspace*, Texas Law Review, Vol. 95:1639, 2017, pag. 1650

[390] NAZIONI UNITE, ASSEMBLEA GENERALE, *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States*, Ris. 2625 del 1970

[391] CORTE PERMANENTE DI GIUSTIZIA INTERNAZIONALE, *Sentenza caso Lotus*, 7 settembre 1927.

[392] CORTE PERMANENTE DI ARBITRATO, *Sentenza caso Isola di Palmas*, 1928.

[393] ANTONIO CASSESE, *International Law*, Oxford University Press Second Edition, 2004.

authority in the territory of another state, in the absence of consent or another provision of international law to the contrary''[394].

Con riferimento alle argomentazioni espresse a sostegno della tesi precedente, viene rilevato, in senso contrario, che i regimi giuridici che governano i domini aereo, spaziale e marino, si basano comunque sull'integrità e inviolabilità della sovranità. Allo stesso modo, con riferimento alle osservazioni svolte rispetto alle attività di spionaggio, si evidenzia come esse costituiscano de jure una violazione della sovranità territoriale di uno Stato. Violazione rispetto alle quali il problema principale, in particolare nel caso di attività cyber condotte da remoto, consiste nell'identificazione del limite superato il quale tali azioni non possono più essere tollerate determinando una violazione della sovranità dello Stato[395].

La ricostruzione dottrinale dell'idea di sovranità poggia su una prassi che, seppur ampia, solo in parte permette di rilevare l'opinio juris degli Stati in ragione della riservatezza e della prudenza riservate alle tematiche più delicate del cyberspace.

A tal fine, tuttavia, presentano una particolare utilità i documenti strategici in materia di sicurezza informatica elaborati dagli Stati. Documenti che, seppur non esprimono una chiara posizione di diritto, delineano comunque una prospettiva di lungo periodo entro la quale gli Stati orientano la loro azione al fine di tutelare interessi nazionali di valore primario[396].

Nel 1999 il dipartimento della difesa (DoD) statunitense ha rilasciato un documento, intitolato *An assessment of international legal issues in information operation*, nel quale considerava l'applicazione del corpus giuridico dello *jus ad bellum* e dello *jus in bello*; del diritto internazionale dello spazio e delle telecomunicazioni; del diritto che governa le azioni di spionaggio oltre a specifici regimi convenzionali. In particolare, la posizione espressa dagli Stati Uniti affermava che determinate cyber operation condotte da gli Stati potessero violare la sovranità statale costituendo un illecito internazionale[397].

---

[394] PHIL SPECTOR, *In defence of sovereignty, cyberspace, and Tallinn Manual 2.0*, in THE AMERICAN SOCIETY OF INTERNATIONAL LAW, *Symposium on Sovereignty, cyberspace and Tallinn Manual 2.0*, 2017.

[395] MICHAEL N. SCHMITT, LIIS VIHUL, *Respect for Sovereignty in Cyberspace*, Texas Law Review, Vol. 95:1639, 2017

[396] ANN VALJATAGA, *Tracing opinio juris in National Cyber Security Strategy Documents*, NATO CCD COE, Law researcher, Tallinn, 2018

[397] U.S. Dep't of Def., Office of Gen. Counsel, An assessement of international legal issue in information operations (2nd ed 1999), in Computer Network Attack and International Law 459,

Recentemente, tuttavia, il DoD sembra orientarsi verso la tesi della sovranità quale principio la cui violazione non determina un illecito internazionale[398].

Una posizione condivisa dal Governo inglese e recentemente espressa nelle dichiarazioni del Procuratore Generale Jeremy Wright secondo il quale *"some have sought to argue for the existence of a cyber specific rule of a violation of territorial sovereignty in relation to interference in the computer networks of another State without its consent. Sovereignty is of course fundamental to the international rules-based sustem. But i am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law"* [399].

Diversamente, la Russia e la Cina condividono la tesi secondo cui la sovranità consiste in una norma primaria di diritto internazionale suscettibile di per sé di essere violata. I due stati hanno siglato nel 2016 un accordo di cooperazione nello sviluppo dello spazio informatico in cui sostengono congiuntamente il rispetto e l'opposizione alle violazioni della sovranità di ogni paese nello spazio dell'informazione[400].

In particolare, La National Cyber Security Strategy elaborata dalla Cina espressamente prevede che *"no infringement of sovereignty in cyberspace will be tollerated, the rights of all countries to independently choose thei development path, network management*

463-65, Michael N. Schmitt, Brian T. O'Donnel, 2002. In particolare, il documento osservava che "an unauthorized electronic intrusion into another nation's computer system may very well end up being regard as a violation of the victm's sovereignty. It may even de regarded as equivalent to a physical trespass into a nation's territory".

[398] Memorandum from Jennifer M. O'Connor, Gen. Counsel of the Dep't of Def., International Law Framework for Employing cyber Capabilities in Military Operation (Jan. 19, 2017). Tale documento fu inizialmente rilasciato pubblicamente per essere successivamente riservato ad uso interno dell'amministrazione statunitense. Tuttavia, il suo contenuto è stato oggetto di analisi nei lavori citati in sede di analisi della teoria della sovranità quale principio di diritto internazionale.

[399] UK GOVERNEMENT. ATTORNEY GENERAL JEREMY WRIGHT, *Cyber and International Law in the 21st Century*, http://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[400] RUSSIA, CHINA, *Joint Statement on Cooperation in Information Space Development*, il testo è consultabile all'indirizzo, https://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm

method and Internet public policy, as well as to equally participate in international cyberspace governance will be respected"[401].

La Federazione Russa, inoltre, ha elaborato una originale idea di Sovranità Tecnologica che pone attenzione all'indipendenza economica degli Stati rispetto ai principali attori economici del settore tecnologico enfatizzando l'uso di hardware e software sviluppati in Russia[402].

Una diversa declinazione del concetto di sovranità è stata elaborata anche dalla Francia che, nei suoi documenti strategici, individua l'idea di "sovranità digitale", ovvero *"the ability of France to retain in space the autonomous ability of appreciation, decision and action, as well as to preserve the most traditional elements of its sovereignty in the face of the new threats that exploit the incresing digitisation of society".* Entro questa prospettiva si afferma che *"the principle of sovereignty applies to cyberspace. In the respect, France reaffirms its sovereignty over information and communication technologies (ICT) infrastructures, person and cyber activities located whitin its territory, subject to its international legal obligations"*[403].

2.1.2 Il principio di due diligenze nel cyberspace

Il principio di sovranità costituisce il fondamento dell'ulteriore principio di due diligence secondo cui lo Stato deve assicurare che il suo territorio o gli elementi che vi insistono, non siano utilizzati per offendere un altro Stato. Da esso deriva una particolare tipologia di obblighi internazionali che, come è stato osservato, *"richiedono ai loro destinatari di prendere tutte le misure ragionevoli, o appropriate, o in loro potere, oppure di sforzarsi, per prevenire (o all'inverso realizzare), un determinato risultato"*[404].

---

[401] CINA, *International Strategy of Cooperation on cyberspace*, 3 Jan. 2017, una traduzione non ufficiale è disponibile all'indirizzo web http://www.xinhuanet.com//english/china/2017-03/01/c136094371.htm

[402] FEDERAZIONE RUSSA, *Doctrine of Information Security on the Russian Federation*, 5 Dec. 2016,http://www.mid.ru/en/foreignpolicy/officialdocuments/-/assetpublisher/CptlCkB6BZ29/content/id/2563163

[403] FRANCIA, *Cyberdefense Strategic Review*, 2018

[404] CARLO FOCARELLI, *Diritto internazionale, Quinta Edizione*, CEDAM, 2019

Inizialmente delineato nel XVII secolo da Grotius[405] trova oggi estesa applicazione nei diversi ambiti del diritto internazionale[406].

Tuttavia, rispetto allo sviluppo della disciplina giuridica del cyberspace, il principio di due diligence non richiama la stessa attenzione riscossa da altri temi pur rappresentando un ulteriore elemento di incertezza.

I report dei gruppi di esperti istituiti dall'Assemblea Generale così come i documenti strategici sopra richiamati, evidenziano il generale consenso in merito, da un lato, al legame di tale principio con il principio di sovranità, da cui la sua applicabilità al cyberspace. Dall'altro sottolineano che esso, in ragione delle caratteristiche del cyberspace, presuppone un livello minimo di sviluppo tecnologico. Diversamente, non vi è una comune prospettiva in merito al valore giuridico e all'oggetto degli obblighi di due diligence. In altri termini vi è incertezza sul se e sul come il principio di due diligence possa costituire una base per la responsabilità degli Stati[407].

Allo stesso modo, il report del gruppo di esperti istituito dall'Assemblea Generale delle Nazioni Unite nel 2013, pur ribadendo l'applicabilità del diritto internazionale e della Carta ONU si esprime in termini meno perentori rispetto al principio di due diligenze. Il report si limita ad indicare che *"States should seek to ensure that their territories are not used by non-state actors for unlawful use of ITC".*

Il Manuale di Tallinn 2.0 declina il principio di due diligence rispetto al cyberspace nel senso che *"A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operation that affect the rights of, and produce serious adverse consequence for, other States"*. Inoltre, in merito al rispetto della due diligence ritiene che *"The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequence for, other States"* [408].

---

[405] JAN ARNO HESSBRUEGGE, *The historical development of the doctrines of attribution and due diligence in International Law*, New York Univ. Jour. of International Law and Politics, 2004

[406] INTERNATIONAL LAW ASSOCIATION, *Study Group on Due Diligence in International Law*, First Report (7 March 2014), Second Report (July 2016)

[407] ANN VALJATAGA, *Tracing opinio juris in National Cyber Security Strategy Documents*, NATO CCD COE, Law researcher, Tallinn, 2018

[408] MICHAEL N. SCHMITT, LIIS VIHUL, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*, Cambridge University press, 2017, Rule 6 e 7. Per una disamina dell'impostazione seguita dal Manuale di Tallinn 2013 e durante la preparazione della seconda

Il commento elaborato dal Gruppo di Esperti che ha redatto il Manuale si esprime sui punti che presentano maggiore incertezza.

In primo luogo, viene rilevato come gli obblighi di due diligence si applicano agli elementi costituenti i tre livelli del cyberspace (fisico, logico, sintattico) posti all'interno del territorio dello Stato. Tali obblighi si estendono oltre il limite territoriale nei casi in cui uno Stato eserciti il controllo di un territorio per annessione o occupazione territoriale e nel caso in cui lo Stato eserciti il controllo su infrastrutture cyber collocate all'estero. Rispetto alla nozione di controllo si evidenzia come essa non necessariamente coincide con la nozione di giurisdizione. Il Gruppo di Esperti ritiene che *"the key to attachment of due diligence obligation extraterritorially is that the State is in actual control of the cyber infrastructure is on territory, premises, or objects it fatally controls"*[409].

In secondo luogo, è stata discussa la responsabilità dello Stato attraverso le cui infrastrutture transitano i soli dati, ad esempio tramite i cavi in fibra ottica[410]. In tale situazione lo Stato di transito, quando è a conoscenza di un'operazione illecita che raggiunge la soglia di danno richiesta può adottare, in adempimento degli obblighi di due diligence, misure concrete per porvi fine in modo efficace. Occorre tuttavia rilevare come i caratteri del cyberspace rendano particolarmente difficile per uno Stato acquisire la conoscenza che tali attività siano condotte tramite il suo territorio. Un aspetto questo che porta il Gruppo di Esperti ad evidenziare la centralità del problema della conoscenza da parte dello Stato di transito piuttosto che l'applicabilità del principio di due diligence a tali fattispecie.

Per quanto riguarda i danni materiali prodotti dalle attività informatiche, la norma richiede che sussistano i due requisiti, tra loro cumulabili, della contrarietà rispetto i diritti dello Stato offeso dalle cyber operation e della gravità delle loro conseguenze. In altri termini, gli obblighi di due diligence sussistono quando le cyber operation determinano un atto internazionalmente illecito.

Nonostante il Manuale di Tallinn 2.0 ritenga che le cyber operation rilevanti siano solo quello condotte da attori statali, viene sottolineato

---

edizione, vedi MICHAEL N. SCHMITT, *In defense of Due Diligence in cyberspace*, The Yale Law Journal Forum, June 22, 2015

[409] MICHAEL N. SCHMITT, LIIS VIHUL, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*, Cambridge University press, 2017, Rule 6, punto 11.

[410] Situazione diversa da quella in cui sul territorio dello Stato vengano installate specifiche infrastrutture cyber con lo scopo di utilizzarle per fini illeciti.

come il principio di due diligence si applichi anche alle cyber operation condotte da soggetti non statali, anche se non lesive del diritto internazionale, quando determino comunque serie conseguenze e incidano sui diritti dello Stato offeso.

L'esatta definizione del livello di danno al quale si applica il principio di due diligence costituisce un ulteriore elemento di incertezza nel diritto internazionale del cyberspace. Il Manuale di Tallinn 2.0 fa riferimento ad *"serious adverse consequence"*, mutuando tale concetto da altri settori del diritto internazionale, in particolare il diritto ambientale, senza tuttavia esplicitarne il contenuto.

2.1.3 L'uso della forza ai sensi dell'art. 2 par. 4 Carta delle Nazioni Unite nel dominio informatico

Le diverse problematiche indicate riflettono la complessità e le incertezze relative alle attività informatiche determinate dai caratteri del cyberspace[411]. Quanto sopra, permette di rilevare come, da una parte, sussista un generale consenso circa l'applicabilità del principio di sovranità nel cyberspace nonostante le differenti ricostruzioni della sua natura giuridica, dall'altro, come resti indefinita la soglia oltre la quale una operazione cyber costituisce una fattispecie di uso della forza nelle relazioni internazionali lesiva della sovranità statale.

[411] Le due ricostruzioni del valore giuridico del principio di sovranità sottintendono una duplice prospettiva rispetto alle azioni cyber e ai loro limiti, così come rispetto ai rischi ad esse connessi. Quanti ricostruiscono la sovranità quale principio ritengono che introduca nella disciplina del cyberspace un elemento di flessibilità maggiormente rispondente alla realtà delle condotte degli Stati. Solamente le cyber operation determinanti una violazione del divieto di intervento e di uso della forza, giustificherebbero la reazione, anche armata, dello Stato leso e la sanzione dello Stato autore dell'illecito internazionale. Aspetto questo che, da una parte, permetterebbe agli Stati una migliore azione a tutela dei legittimi interessi nazionali potendo svolgere la propria azione entro limiti più ampi rispetto alla sovranità come regola primaria. Dall'altra, diminuirebbe il livello, e dunque la pericolosità rispetto alla sicurezza internazionale, dei contrasti nelle relazioni tra Stati nel cyberspace. Allo stesso modo quanti sostengono l'idea della sovranità quale norma primaria del diritto internazionale evidenziano la necessità di una chiara definizione dei limiti delle cyber operation. Allo stesso tempo, riconoscendo, data l'ampia tipologia di condotte realizzabili, che non tutte le cyber operation oltrepassano il limite della sovranità, valorizzano, quale strumento di flessibilità, l'individuazione di criteri che permettono di correttamente qualificare l'azione degli Stati nel cyberspace. In questa prospettiva, il Manuale di Tallinn 2.0, muove dal presupposto della sovranità quale norma primaria, per svolgere un'analisi puntuale delle condotte cyber. Come inizialmente indicato, il Manuale individua specifici criteri al fine di determinare la liceità delle cyber operation. L'applicazione di tali criteri, oltre a non determinare nuovi vincoli all'azione degli Stati, favorisce il ricorso ad una più ampia serie di strumenti di tutela dei propri interessi.

Nel diritto internazionale classico l'uso della forza armata non incontrava limiti sostanziali. Il ricorso alla guerra e alle misure coercitive diverse dalla guerra era considerato una manifestazione naturale della sovranità statale e uno strumento ordinario per la soluzione delle controversie. Almeno fino alla Prima guerra mondiale, la Comunità Internazionale non ha elaborato regole finalizzate a bandire la guerra nei rapporti tra Stati, limitandosi a disciplinare le modalità di esecuzione e il comportamento dei belligeranti una volta che la violenza bellica avesse avuto inizio[412]. A questo sistema sono stati introdotti dei correttivi, divenuti assai rilevanti nel periodo tra le due guerre. Il riferimento è alla Convenzione dell'Aja del 1907 sulla limitazione dell'uso della forza per il recupero dei debiti contrattuali[413], al Patto della Società delle Nazioni del 1919[414] e al Patto Briand-Kelog del 1928[415].

Tuttavia, è solo successivamente alla Seconda guerra che la Comunità Internazionale disciplina in maniera più articolata il ricorso

[412] In particolare, la II° Convenzione internazionale dell'Aja 1899 concernente le leggi e gli usi della guerra terrestre e la IV Convenzione dell'Aja 1907 concernente le leggi e gli usi della guerra per terra

[413] Il primo di essi può essere individuato nella La Convenzione dell'Aja sulla limitazione dell'uso della forza per il recupero dei debiti contrattuali del 1907, c.d. Convenzione Drago-Porter, pur essendo limitata negli scopi, poneva l'obbligo del non ricorso alla forza armata a carico dello Stato creditore nel caso in cui lo Stato debitore avesse accettato mezzi pacifici di risoluzione delle controversie.

[414] Il Patto della Società delle Nazioni del 1919 non stabiliva un obbligo assoluto di rinuncia alla guerra e non istituiva meccanismi di attuazione coercitiva del diritto nei confronti dello Stato membro che contravveniva alle disposizioni del Patto. Questo stabiliva all'art. 10 l'obbligo per gli Stati Membri a rispettare e proteggere, contro ogni aggressione esterna, l'integrità territoriale e l'indipendenza politica degli altri Membri e a non ricorrere in dati casi alle armi. Il *Convenant* sanciva il dovere per gli Stati di risolvere pacificamente le controversie internazionali, obbligandoli a ricorrere ad un tribunale arbitrale, alla Corte Permanente di Giustizia Internazionale o al Consiglio della Società delle nazioni. Era inoltre previsto un periodo di tre mesi dalla pronuncia del Tribunale arbitrale, della Corte Permanente o del Consiglio, decorso il quale era lecito ricorrere alla guerra. Era previsto un divieto generale di muovere guerra a uno Stato che si fosse conformato alla decisione degli organismi indicati, purché fosse stata approvata all'unanimità. Il sistema, tuttavia, non vietava le misure coercitive diverse dalla guerra e non era previsto alcun meccanismo istituzionalizzato per l'attuazione coercitiva del diritto.

[415] Il Patto di Parigi del 1928, c.d. Patto Briand-Kellog sanciva, in due soli articoli la rinuncia incondizionata alla guerra come strumento di politica internazionale e ne condannava il ricorso come strumento per la soluzione delle controversie internazionali. L'uso della forza era consentito solo se esercitato nei confronti di uno Stato che si fosse reso colpevole di una violazione del diritto internazionale e non avesse acconsentito a ripararla. Il Patto lasciava comunque ampie zone grigie, consentendo, ad esempio, i procedimenti di autotutela diversi dalla guerra (rappresaglie armate) e non contemplava misure sanzionatorie.

alla forza armata nelle relazioni internazionali inserendolo all'interno di un più articolato sistema di sicurezza collettiva incentrato sulle norme della Carta delle Nazioni Unite.

L'art. 1 della Carta individua, tra gli scopi dell'organizzazione, quello del mantenimento della pace e della sicurezza internazionali, per il cui perseguimento la Carta sancisce, all'art. 2, par. 4 il divieto dell'uso e della minaccia dell'uso della forza armata nelle relazioni internazionali, salva l'ipotesi prevista dall'art. 51 della legittima difesa individuale e collettiva. Allo stesso modo, infine, l'art. 24 attribuisce al Consiglio di Sicurezza la responsabilità principale nel mantenimento della pace e della sicurezza internazionali.

Entro questo quadro occorre dunque ricondurre le principali problematiche connesse all'uso della forza nel cyberspace.

Nel presente paragrafo pertanto verrà discusso se e quando una cyber operation costituisce un uso illecito della forza armata; se e quando lo Stato leso può invocare il diritto all'autodifesa;

Cyber operation quale uso della forza

Cardine del sistema di sicurezza collettiva delineato dalla Carta delle Nazioni Unite è l'art. 2, par. 4 il quale, riflettendo il diritto internazionale consuetudinario[416], afferma che *"all Member shall refrain in their international relation from threath or use of force against the territorial integrity or political indipendence of any state, or in any other manner inconsistent with the Purposes of United Nations".*

La norma individua tre condizioni di carattere generale applicabili anche alle cyber operation secondo cui quest'ultime devono essere attribuibili ad uno Stato e consistere nella minaccia o nell'uso della forza armata esercitate nella condotta delle relazioni internazionali.

Rispetto alla prima questione posta, se e quando una cyber operation costituisce un uso illecito della forza armata, occorre osservare come non vi sia una chiara indicazione rispetto al concetto di uso della forza.

[416] CORTE INTERNAZIONALE DI GIUSTIZIA, *Military and paramilitary activities in and against Nicaragua*, 1986, par.187-190; *Legal Consequences of the construction of a wall in the occupied Palestinian territory* ,2005, par. 87.

L'art. 2, par. 4 non fornisce infatti, una definizione di "forza"[417]. Tuttavia, come è noto, gli Stati partecipanti alla Conferenza di San Francisco hanno respinto un emendamento del Brasile, inteso ad includere nell'art. 2, par. 4, anche le misure di coercizione economica in contrasto con i fini dell'ONU. Inoltre, le Dichiarazioni dell'Assemblea Generale sulle relazioni amichevoli (1970), sulla definizione di aggressione (1974) e sul non uso della forza (1987) sembrano supportare la prospettiva secondo cui l'art. 2, par. 4 si riferisce alla sola forza armata, differentemente dal principio di non intervento che fa riferimento ad altre forme di coercizione[418].

Il problema che si pone è dunque quello di determinare se e quando una cyber operation raggiunge il livello di utilizzo della "forza armata".

Problema al quale possono essere date risposte differenti a seconda dell'adesione alle diverse prospettive basate, rispettivamente, sugli obiettivi perseguiti, sugli strumenti utilizzati, o sugli effetti conseguiti[419].

Entro la prima prospettiva le operazioni cyber costituiscono un caso di uso della forza armata quando sono condotte contro infrastrutture critiche nazionali a prescindere dalla natura dell'operazione e dagli effetti determinati sugli obiettivi.

Il secondo approccio pone attenzione, oltre alla sussistenza dell'intento coercitivo[420], agli strumenti utilizzati per compiere l'operazione cyber e corrisponde al tradizionale approccio seguito per distinguere la forza armata dalla coercizione politica o economica. Entro questa prospettiva è stato osservato che *"armed force in the sense of Article 2(4) could be defined as the form of intervention by a State to exercise coercion on another State that involves the use of instruments (weapons) capable of producing violent consequences"*[421]

---

[417] La Carta delle Nazioni Unite utilizza l'espressione "forza" nel Preambolo e negli articoli 41 e 46 dove è preceduta dall'aggettivo "armata", mentre solo nell'art 44 la Carta si riferisce espressamente alla "forza armata".

[418] MARCO ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2014, pp. 45 e seguenti; MICHAEL N. SMITH, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Columbia Journal of Transnational Law 37 (1998-99), pp. 906-908.

[419] MARCO ROSCINI, *Cyber operation as a use of force*, in NICHOLAS TSAGOURIAS, RUSSELL BUCHAN, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017

[420] Occorre osservare come l'intento coercitivo costituisce un fattore necessario ma non sufficiente a identificare e distinguere una cyber operation come uso della forza armata. Tale intento può infatti essere presente anche in azioni diplomatiche o economiche.

[421] MARCO ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2014, pp. 50

Infine, la teoria basata sugli effetti prodotti permette di evidenziare come l'uso della forza armata, differentemente da altre forme di coercizione, determini effetti distruttivi diretti sulle persone e sulle proprietà allo stesso modo delle armi cinetiche (c.d. dottrina dell'equivalenza cinetica).

Ciò, tuttavia, porta ad escludere l'applicazione della norma della art.2, par. 4 rispetto a tutta una serie di operazioni informatiche che pur non raggiungendo la soglia della forza, sono comunque in grado di determinare rilevanti conseguenze in ragione del carattere integrato e pervasivo delle tecnologie ITC rispetto alla società attuale.

Rispetto a quest'ultimo problema sono stati elaborati una serie di parametri e fattori in base ai quali stabilire quando la portata e l'effetto delle operazioni informatiche che producono conseguenze pregiudizievoli di natura non fisica assomigliano sufficientemente a quelle di un uso cinetico della forza.

Tali criteri, non esaustivi e non vincolanti, sono: gravità, immediatezza, precisione, invasività, misurabilità degli effetti, carattere militare, coinvolgimento degli Stati, legalità[422]

Tale ultimo approccio, c.d. *scale and effect*, è ripreso dal Manuale di Tallinn 2.0 il quale prevede che "*a cyber operation constitutes a use of force when its scale and effects are comparable to noncyber operations rising to the level of a use of force"*[423],

Il commento del Manuale d Tallinn 2.0 sottolinea come nel contesto cyber non sia lo strumento usato a determinare se è stato oltrepassato il limite del divieto dell'uso della forza quanto piuttosto le conseguenze dell'operazione e le specifiche circostanze.

Tuttavia, come è stato osservato, la distinzione tra le teorie basate sugli strumenti utilizzati per la cyber operation e sugli effetti di quest'ultime viene meno ove si consideri che *"it is the instrument used that defines armed force, but the instrument is identified by its (violent) consequences"*[424]. Con riferimento all'art. 2, par. 4 della Carta ONU la Corte Internazionale di Giustizia, inoltre, ha osservato che esso si applica a *"any use of force, regardless of weapons employed"*[425]

---

[422] MICHAEL N. SMITH, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Columbia Journal of Transnational Law 37 (1998-99), pp. 906-908; TALLINN MANUAL 2.0, Commento alla *Rule 69, Definition of use of force*

[423] TALLINN MANUAL 2.0, vedi comento introduttivo al *Cap. 14 The use of force*, pag. 328.

[424] MARCO ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2014, pp. 50

[425] CORTE INTERNAZIONALE DI GIUSTIZIA, *Legality of the threat or use of nuclear weapons, advisory opinion, 8 july 1996, par. 39.*

Entro questa prospettiva gli strumenti informatici possono essere considerati quali armi in ragione della loro capacità di determinare rilevanti conseguenze tanto nel funzionamento delle infrastrutture quanto nelle persone verso le quali sono utilizzate.

Tuttavia, in ragione degli scopi perseguiti e dei caratteri delle singole armi informatiche utilizzate occorre valutare singolarmente le differenti cyber operation. In termini generali si può osservare come ricadano entro la previsione dell'art. 2, par. 4, gli attacchi cyber progettati per causare danni fisici alla proprietà, l'uccisione o il ferimento di persone. Vi rientrano inoltre gli attacchi cyber in grado di rendere inoperanti e inutilizzabili le infrastrutture critiche o di causare significanti interruzioni di servizi essenziali anche senza danneggiare fisicamente le infrastrutture. Diversamente, ove tali conseguenze non si verifichino, le cyber operation determinano una violazione del principio di non intervento qualora caratterizzate da un chiaro intento coercitivo. Aspetto questo che esclude le operazioni meramente volte alla raccolta di informazioni quand'anche relative ad attività ed elementi aventi carattere di interesse nazionale per lo Stato oggetto dell'attività informatica.

2.1.4 La legittima difesa ai sensi dell'art. 51 Carta delle Nazioni Unite nel dominio informatico;

Il sistema di sicurezza collettivo trova il suo secondo riferimento normativo nella norma dell'art. 51 della Carta delle Nazioni Unite la quale prevede che *"nothing in the present Charter shall impair the inherent right of individual or collettive self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security"*.

Nel Sistema della Carta il diritto all'autodifesa costituisce un'eccezione al divieto di uso della forza previsto dall'art. 2, par. 4 e consente agli Stati, individualmente e collettivamente, di rispondere ad un attacco armato. Risposta attuabile fintantoché il Consiglio di Sicurezza delle Nazioni Unite non adotti le misure necessarie per il mantenimento della sicurezza e della pace internazionali.

Il collegamento con la norma dell'art. 2 par. 4 permette di evidenziare presupposti e limiti per l'esercizio del diritto di autodifesa che può essere invocato solo a fronte di un attacco armato consistente

nell'uso della forza armata. Allo stesso modo l'uso della forza armata per autodifesa è legittimo nella misura in cui non superi le limitazioni imposte dal diritto internazionale.

Nel contesto del cyberspace si pongono, da un lato, il problema di definire quando una cyber operation costituisce un *attacco armato* legittimante l'esercizio del diritto di autodifesa.

Dall'altro, il problema della definizione dei limiti dell'uso della forza armata per autodifesa.

Rispetto al primo quesito si può rilevare come la nozione di *attacco armato*, al pari di quella di uso della forza, non trovi una chiara definizione. La Corte Internazionale di Giustizia nella caso Nicaragua ha evidenziato come non esista all'interno della Carta delle Nazioni Unite e nel diritto convenzionale una nozione di attacco armato[426].

Nella prospettiva volta a valorizzare lo strumento utilizzato per l'attacco armato si sostiene che anche un attacco condotto con strumenti cyber può essere considerato un *attacco armato*[427]. Muovendo dalle osservazioni della Corte Internazionale di Giustizia nel caso Armi Nucleari secondo cui l'art. 51 si applica a *"any use of force, regardless of the weapon employed"*[428] si sostiene che le cyber operation possono costituire un attacco armato anche se non utilizzano armi convenzionali. In questa prospettiva è stato osservato che *"it is neither the designation of a device, nor its normal use, which make it a weapon but the intent with which it is used and its effect. The use of any device, or a number of device which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfill the conditions of an armed attack"*[429].

Tuttavia, affinché una cyber operation costituisca un attacco armato è comunque necessario che essa sia qualificabile come un caso di uso della forza. In altri termini essa deve causare, o poter ragionevolmente causare, rilevanti danni fisici alle persone o alle proprietà o danneggiare gravemente infrastrutture critiche. Diversamente una cyber operation non può essere considerata un attacco armato e quindi legittimare l'esercizio del diritto di autodifesa.

---

[426] CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenza caso Nicaragua*, par. 176

[427] MARCO ROSCINI, *Cyber operations and the use of force in international law*, Oxford University Press, 2014, pag. 71

[428] CORTE INTERNAZIONALE DI GIUSTIZIA, *Parere sulla liceità della minaccia o dell'uso delle armi nucleari*, par. 39

[429] KARL ZEMANEK, *Armed Attack*, Max Planck Encyclopedia of Pubblic International Law, 2012.

Quest'ultimo aspetto viene valorizzato entro la prospettiva maggiormente attenta alle conseguenze dell'azione armata. Approccio seguito dal Manuale di Tallinn 2.0 che alla Rule 71 si occupa del diritto di autodifesa contro un attacco armato. Il Manuale rileva che *"A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects"*.

Nel commento alla regola gli Esperti che hanno redatto il Manuale di Tallinn prendono una chiara posizione evidenziando come il fattore critico non consista nelle armi utilizzate quanto piuttosto negli effetti di una operazione informatica che ritengono debbano essere analoghi a quelli che risulterebbero da un attacco armato di tipo cinetico.

Al riguardo la Rule 71, nel secondo comma, fa esplicito riferimento al criterio *scale and effects* elaborato dalla Corte Internazionale di Giustizia che, nel caso *Nicaragua*, vi fa riferimento per distinguere le forme più gravi di uso della forza consistenti in un attacco armato diversamente da quelle meno gravi, senza tuttavia fornire indicazioni sui parametri da utilizzare.

Nel contesto del cyberspace, date le caratteristiche delle operazioni informatiche e dei loro obiettivi, ciò determina un ulteriore fattore di incertezza. Da una parte, possono costituire un caso di uso della forza anche azioni che, pur non causando seri danni fisici, possono comunque determinare l'inoperatività di infrastrutture critiche per la sicurezza dello Stato. Dall'altra, l'anonimato, i problemi di attribuzione e l'immediatezza delle azioni informatiche, incidono sui tempi e sulle modalità di reazione all'attacco informatico.

Entro tale contesto viene in rilievo il dibattito sul problema se l'auto difesa preventiva sia permessa in risposta a un mero rischio di attacco informatico o contro un attacco che non oltrepassa la soglia dell'uso della forza.

La Corte Internazionale di Giustizia nel caso Nicaragua[430] si è astenuta dal pronunciarsi mentre nel caso Attività Armate in Congo[431] ribadisce i limiti dell'auto difesa posti dall'art. 51 della Carta ONU.

Tuttavia, la Corte, chiamata ad esprimersi sulla liceità dell'uso dell'arma atomica, considerati i suoi caratteri, non raggiunge una

[430] CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenza caso Nicaragua*, par. 194

[431] CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenza caso Armed Activities on the Territory of the Democratic Republic of Congo v Uganda*, par. 143 e 148

conclusione definitiva sulla legalità o illegalità dell'uso di tale arma nel caso in cui sia a rischio la sopravvivenza dello Stato[432].

Allo stesso modo in cui l'arma atomica ha ridefinito i parametri dell'uso della forza, le tecnologie del cyberspace ne determino un'ulteriore rielaborazione. La pervasività e l'integrazione rispetto alla società delle tecnologie ITC fa emergere nuovi rischi alla sopravvivenza dello Stato. Rischi legati non alla distruzione fisica totale conseguente all'arma atomica, ma al collasso delle strutture e delle dinamiche sociali, politiche, economiche essenziali alla sopravvivenza dello Stato.

Le problematiche poste dal progresso tecnologico rispetto all'auto difesa preventiva spingono taluni Stati a riconoscerne la legittimità enfatizzando la necessità di tale forma di reazione nel dominio informatico. Altri, evidenziando i problemi di attribuzione, tendono a non ampliare l'area di azione dell'auto difesa nel timore che finisca per costituire uno strumento di aggressione.

L'art. 51 prevede chiaramente che l'esercizio del diritto di auto difesa sia legittimo *"nel caso che abbia luogo un attacco armato"*.

Secondo un primo orientamento interpretativo la norma proibisce l'autodifesa preventiva. Altri valorizzando il concetto di rischio imminente ne sostengono la legittimità.

In generale tuttavia, è stato osservato che, *"it seems that the international community does not accept anticipatory self-defence as a general rule, but could see it a a justification on a case-by-case basis. The general rule is thus that anticipatory self-defence is prohibited and that its permissibility depends on the reaction of the international community as a whole in each case"*[433].

Entro questa prospettiva acquisiscono maggior rilevanza le ricostruzioni del criterio *scale and effects* e in particolare quelle ricostruzioni che includono gli effetti determinati sul piano politico/istituzionale, industriale ed economico[434] in ragione dei caratteri del cyberspace e delle azioni condotte tramite le tecnologie informatiche.

---

[432] CORTE INTERNAZIONALE DI GIUSTIZIA, *Advisory Opinion, Legality of Threat or Use of Nuclear Weapons*, par. 97.

[433] CARLO FOCARELLI, *Self-defence in cyberspace*, in, a cura di, NICHOLAS TSAGOURIAS, RUSSELL BUCHAN, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017, pag.272.

[434] AVRA CONSTANTINOU, *The right of sel-defence under costumary international law and article 51 of UN Charter*, Bruylant, 2000.

Posto che un attacco cyber in grado di compromettere gravemente il funzionamento di infrastrutture critiche per la sicurezza nazionale potenzialmente può essere considerato un attacco armato, ciò tuttavia, non legittima automaticamente lo Stato vittima ad usare in ogni caso la forza per auto difesa.

Vien qui in rilievo il secondo problema indicato relativo ai limiti dell'uso della forza ex art. 51 Carta Nazioni Unite. In particolare, la giurisprudenza della Corte Internazionale di Giustizia ha evidenziato come nel caso di legittima difesa l'esercizio della forza debba rispettare i requisiti di necessità e proporzionalità[435].

In termini generali per necessità si intende l'impossibilità di ricorrere a strumenti diversi dall'uso della forza per rispendere effettivamente ad un attacco o per prevenire una minaccia o un attacco imminente qualora sia permesso l'esercizio anticipato del diritto di autodifesa[436]. Rispetto agli attacchi informatici non si pongono particolari problemi. Lo Stato che intende esercitare il diritto all'autodifesa è obbligato a porre in essere attività informatiche difensive di tipo sia attivo che passivo al fine di bloccare l'attacco informatico, oltre che a dimostrare che tali attività siano insufficienti rispetto agli scopi difensivi.

Diversamente maggiori problemi si pongono con riferimento all'applicazione del principio di proporzionalità nel cyberspace.

Tale principio trova il suo fondamento nella norma dell'art 51 del I Protocollo addizionale alla Convenzione di Ginevra del 1977 il quale prevede che *"la popolazione civile e le persone civili godranno di una protezione generale contro i pericoli derivanti da operazioni militari"*.

Conseguentemente la stessa norma prevede al punto 5 let. b) che "*saranno considerati indiscriminati gli attacchi dai quali ci si può attendere che provochino incidentalmente morti e feriti fra la popolazione civile, danni ai beni di carattere civile, o una combinazione di perdite umane e di danni, che risulterebbero eccessivi rispetto al vantaggio militare concreto e diretto previsto".*

La violazione del principio di proporzionalità trova protezione anche nello Statuto della Corte Penale Internazionale che, all'art 8 dello Statuto considera come sproporzionati i danni eccessivi rispetto al *"vantaggio militare complessivo previsto"*.

---

[435] Nicaragua par. 194 merito; oil platform par. 161, 183, 196-198.

[436] CARLO FOCARELLI, *Self-defence in cyberspace*, in NICHOLAS TSAGOURIAS, RUSSELL BUCHAN, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017, pag. 273

Il principio di proporzionalità persegue dunque lo scopo di proteggere i civili durante un conflitto armato imponendo un bilanciamento tra il vantaggio militare derivante dall'attacco armato e l'esigenza umanitaria che l'attacco non causi vittime e/o danni eccessivi rispetto ai vantaggi militari che può determinare.

Secondo alcuni manuali militari il bilanciamento tra i due interessi in conflitto deve essere affidato all'aspettativa, in buona fede, che l'attacco porti un rilevante contributo militare[437]. Per quanto riguarda l'Italia il *Codice di comportamento delle Forze armate italiane in operazioni*[438], emanato dal Dipartimento di diritto umanitario e delle operazioni militari dell'ISSMI, evidenzia come il bilanciamento debba essere affidato al buon senso del Comandante.

Nel contesto dei moderni conflitti asimmetrici caratterizzati da un sempre maggior coinvolgimento di attori non statali, si tratta di un bilanciamento di difficile definizione data anche l'assenza di una scala di valutazione che porta a procedere caso per caso.

Una complessità che aumenta nel contesto del cyberspace ove gli obiettivi degli attacchi informatici possono essere costituiti tanto da infrastrutture essenziali per la vita cittadina quanto dai dispositivi informatici dei cittadini stessi. Occorre infatti osservare come il principio di proporzionalità tuteli i civili rispetto alle conseguenze fisiche di attacchi cinetici, mentre restano esclusi danni "minori" legati all'impossibilità di accedere a servizi essenziali, quali i servi elettrici, idrici o sanitari, o comunque legati alla piena esplicazione dell'individuo permessa dalle tecnologie di telecomunicazione. Situazioni che nel contesto del cyberspace acquisiscono una sempre maggior rilevanza.

In tale contesto i principali problemi derivano dal carattere dual use delle tecnologie ITC che, comportando effetti indiretti per i civili, complicano la valutazione di proporzionalità che i comandi militari sono chiamati ad effettuare[439].

---

437 CANADA, *Manuale "Law of Armed Conflict"* del 2001 https://www.fichl.org/fileadmin/_migrated/content_uploads/Canadian_LOAC_Manual_2001_English.pdf

438 GIOVANNI BARBERINI, *Diritto internazionale umanitario nelle operazioni militari. Convenzioni, protocolli, norme di comportamento*, Centro Alti Studi per la Difesa, Istituto Internazionale di Diritto Umanitario di Sanremo, 2012.

439 ERIC BOYLAN, *Applying the Law of Proportionality to Cyber Conflict: Suggestion for Practitioners*, Vanderbilt Journal of Transnational Law, Jan 2017, Vol 50, Issue I, p. 217 - 244

3. La sicurezza dello spazio informatico.

La seconda direttrice lungo la quale si sviluppa l'azione delle Nazioni Unite rispetto alle problematiche del Cyberspace attiene alle problematiche della sicurezza delle infrastrutture e al contrasto all'uso illecito delle tecnologie ITC al fine di rendere lo spazio informatico fruibile e sicuro per gli utenti finali.

Il tema della sicurezza informatica può essere suddiviso in due aree, la cybersecurity e il cybercrime che, seppur distinte, presentano punti di contatto e di sovrapposizione. Aspetto questo particolarmente evidente nel contesto europeo.

Il concetto di cybersecurity è comunemente legato alla sicurezza delle infrastrutture informatiche, mentre il cybercrime attiene ai crimini perpetrati attraverso le tecnologie informatiche a danno degli utenti, persone fisiche o giuridiche.

Con riferimento alle problematiche della cybersecurity si può inizialmente osservare come il relativo quadro giuridico si presenti frammentato, essendo riferibile principalmente all'azione sviluppata da organizzazioni regionali. Particolarmente rilevanti appaiono le iniziative della NATO, della ASEAN e dell'Unione Europea, oltre all'azione svolta dalle Nazioni Unite precedentemente osservata.

In materia di criminalità informatica si registra un eguale disomogeneità della disciplina giuridica sia internazionale che nazionale, in ragione soprattutto delle diverse sensibilità culturali e del diverso grado di sviluppo tecnologico. Tuttavia, si può fin d'ora notare come un punto di riferimento sempre più rilevante è costituito dalla Convenzione sul Cybercrime del Consiglio d'Europa (Convenzione di Budapest).

Nei paragrafi seguenti verranno d'dapprima tratteggiate le principali iniziative in materia di cybersecurity intraprese nei fori internazionali indicati. In secondo luogo, verranno indicate i principali aspetti caratterizzanti la Convenzione di Budapest in quanto principale strumento giuridico di contrasto al fenomeno della criminalità informatica.

3.1 La cybersecurity nel contesto NATO.

Lo sviluppo della strategia NATO in materia di cybersecurity prende avvio nel 2008 con la *NATO Policy on Cyber Defence*, successivamente rivista nel 2011, volta a rispondere ai nuovi caratteri e strumenti dei conflitti contemporanei.

A livello internazionale essa costituisce la prima azione intrapresa in materia e mira a rispondere alle evoluzioni dei conflitti fino ad allora registrate[440]. In particolare, l'attacco condotto contro le infrastrutture informatiche dell'Estonia nel 2007 e contro i siti governativi e di informazione della Georgia nel 2008 spinsero gli Stati Membri a riconoscere che le attività informatiche *"can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability"*.

In questi termini si esprime il documento *Strategic Concept for the Defence and Security of the Members of the north Atlantic Treaty Organization* del Novembre 2010. Nello stesso anno la Dichiarazione finale del Summit Nato di Lisbona conferisce nuovo stimolo all'azione dell'Alleanza prevedendo per l'anno successivo una revisione del suo Concetto Strategico. Come è stato osservato *"the Action Plan is a living document that is continuously update to ensure that NATO is at the forefront of developments in cyberspace and maintains the necessary flexibility to meet the challenges which they pose"*[441].

Su questa base, nel successivo Summit di Chicago del 2012 gli Stati Membri implementano nuovamente le capacità di cybersecurity dell'Alleanza dando avvio allo sviluppo di una struttura centralizzata di coordinamento degli strumenti predisposti a livello nazionale.

Vengono quindi sviluppate strutture, tanto di natura militare quanto tecnica, tra loro coordinate e sottoposte all'indirizzo politico del Consiglio.

Il North Atlantic Council è il principale organo politico decisionale all'interno del quale il Defence Policy and Planning Committee, composto da delegati nazionali, coordina l'attività di cybersecurity dell'Alleanza. Tale attività si sviluppa attraverso diversi organismi volti ad affrontare i diversi aspetti della sicurezza informatica.

---

[440] Nel 1999 si era registrato un primo attacco cyber durante le operazioni delle forze alleate in Kosovo che portarono ad una prima implementazione delle capacità di cyberwarfare della NATO con la creazione del NATO Computer Incident Response Capability (NCIRC) durante il Summit di Praga del 2002.

[441] Katharina Ziolkowski, NATO and cyber defence, in a cura di Nicholas Tsagourias, Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Pubblishing, 2017, pag. 430.

Il *NATO Cyber Defence Management Board* (CDMB) svolge un'azione di coordinamento tra le strutture militari e civili della NATO. La sua attività segue gli indirizzi dell' *Emerging Security Challenges Division* (ESCD), creato nel 2010 e finalizzato al contrasto delle emergenti problematiche di sicurezza quali il terrorismo, la proliferazione di armi d distruzioni di massa e la sicurezza energetica. Sul piano tecnico, il principale organismo di consultazione e sviluppo delle capacità di difesa informatica, è rappresentato dal *NATO Consultation, Control and Command* (NC3). Mentre, sul piano militare e operativo rilevano le agenzie *NATO Military Authority* (NMA) e *NATO Communications and Information* (NCI). Infine, i diversi strumenti di cybersecurity predisposti a livello nazionale sono stati integrati all'interno del *NATO Defence Planning Process* (NDPP) la cui attività è volta ad individuare tempestivamente i rischi informatici e a definire il livello di risposta adeguato delle varie forze nazionali.

I diversi organismi indicati svolgono la loro azione entro i quadro strategico dell'Organizzazione focalizzato sulla prevenzione degli attacchi informatici e sullo sviluppo delle capacità di resilienza delle infrastrutture sulla base di una chiara ripartizione delle responsabilità e dell'area di azione dell'Organizzazione e degli Stati Membri.

Coerentemente con i fini statutari spetta all'Organizzazione predisporre, anche in materia di sicurezza informatica, le strutture e i meccanismi decisionali e di coordinamento così come assicurare il funzionamento e la sicurezza delle infrastrutture di comunicazione dell'Alleanza. Allo stesso modo gli Stati Membri sono responsabili per i sistemi e i network informatici nazionali. Tuttavia, l'Organizzazione è chiamata fornire il proprio supporto agli Stati nello sviluppo e nell'esercizio di attività di cybersecurity al fine di contrastare gli effetti che un attacco cyber a livello nazionale può determinare per l'Organizzazione stessa o per gli altri Stati Membri.

In questa prospettiva diviene centrale il ruolo dell'Organizzazione nella fase di gestione delle crisi, nello sviluppo di processi di consultazione, di metodologie e strumenti finalizzati all'azione di autodifesa collettiva. Parimenti rilevante è il supporto che l'Organizzazione può offrire rispetto ad attività informatiche malevole che, seppur di carattere civile e non militare, presentano caratteri di rilevante interesse nazionale. Infine, l'Organizzazione svolge un'importante funzione nello sviluppo delle capacità nazionali di contrasto ai rischi informatici attraverso le attività di ricerca, formazione, esercitazione e cooperazione.

3.2 L'approccio dell'ASEAN alla sicurezza informatica.

I temi della sicurezza delle infrastrutture informatiche sono parte dell'azione dell'Association of Southeast Asian Nations (ASEAN). Entro questo contesto lo sviluppo di capacità di cybersecurity, diversamente dalla NATO, non trova origine in problematiche di sicurezza prettamente militare. Essa piuttosto trova fondamento nella volontà, espressa nella *Dichiarazione di Bangkok* del 1967[442] di garantire la sicurezza degli Stati firmatari rispetto alle interferenze esterne e di tutelare la loro sicurezza e stabilità politica interna.

Finalità che si pongono alla base del successivo *Trattato di Cooperazione e Amicizia nel Sud Est Asiatico* del 1976 in cui viene evidenziato l'intento di cooperare al fine di implementare la sicurezza dei suoi Membri. Intenti nuovamente ribaditi nella *Carta dell'ASEAN* adottata nel 2007.

Entro questo quadro l'azione dell'ASEAN in materia di cybersecurity risponde in primo luogo alla necessità di sviluppare la cooperazione tra gli Stati Membri e, in secondo luogo, all'obiettivo di implementare la sicurezza rispetto all'attività di attori esterni.

La cooperazione nello sviluppo della sicurezza delle infrastrutture nazionali si sviluppa a partire dall'azione dell' *ASEAN Telecommunications and IT Ministers* (TELMIN) che, nel 1999, adotta un primo documento in materia, *e-ASEAN Iniziative*, che costituisce la base per il *e-ASEAN Framework Agreement del 2001*. Documento quest'ultimo che mira allo sviluppo di infrastrutture in grado di assicurare l'interconnetività e l'interoperabilità tra i sistemi informatici degli Stati Membri. .

Nel 2003 la *Dichiarazione di Singapore* spinge gli Stati Membri dell'ASEAN alla creazione *Computer Emergency Response Teams* (CERTs) in funzione dei quali verrà sviluppato un comune framework regionale per l'implementazione dell'operatività e della sicurezza delle infrastrutture ITC.

I successivi sviluppi sono legati, da una parte, all'*ASEAN ICT Masterplan 2015* (adottato nel 2011), e al *Mactan Cebu Declaration*, adottato nel 2012, entrambi nel contesto TELMIN. Quest'ultimo in

[442] La Dichiarazione di Bangkok del 1967 è stata sottoscritta da Indonesia, dalla Malesia, dalle Filippine, dalla Tailandia e da Singapore.

particolare mira a sviluppare la cooperazione e la partecipazione nella costruzione e nella promozione di un ambiente informatico sicuro; ad armonizzare le normative relative alle tecnologie ITC, a consolidare la resistenza e la resilienza delle infrastrutture informatiche e a sviluppare la cooperazione e la condivisone di informazioni e best practices.

Differentemente da esperienze quali quella dell'Alleanza Nord Atlantica e, come vedremo, dell'Unione Europea, la sicurezza delle infrastrutture informatiche nel contesto dell'ASEAN poggia sull'azione nazionale degli Stati. Nonostante le iniziative volte a sviluppare un framework comune per la cybersecurity, il sistema di sicurezza risente della frammentazione nazionale e delle diverse prospettive geopolitiche degli Stati.

3.3 Sicurezza informatica e sviluppo sociale nell'Unione Europea.

L'azione dell'Unione Europea rispetto alla sicurezza informatica trova il suo principale riferimento nel documento strategico adottato nel 2013, al quale segue, nel 2019, l'adozione del *Cyber security Act*.

I tratti caratteristici dell'azione europea vengono tuttavia delineati a partire dai documenti elaborati nei primi anni 2000[443] entro il quadro generale predisposto dalla strategia di Lisbona del 2000, nei quali l'attenzione viene posta sui temi del cybercrime e della protezione dei dati personali e delle infrastrutture critiche. Tali documenti rispondono allo scopo di far diventare l'Europa l'economia basata sulla conoscenza "*più competitiva e più dinamica del mondo"*[444] entro il 2010 attraverso lo sviluppo di servizi pubblici digitali e di un'affidabile infrastruttura di protezione dell'informazione[445].

Sul piano delle strutture istituzionali un ruolo centrale viene affidato nel 2004 all'*Agenzia europea di sicurezza delle reti e dell'informazione* (EISA) il cui compito consiste, inizialmente, nell'assistere la

---

[443] COMMISSIONE EUROPEA, *eEurope. Una società dell'informazione per tutti*, [COM (2000) 130], 8 marzo 2000; *eEurope 2005: una società dell'informazione per tutti*, [COM (2002) 263], 28 maggio 2002.

[444] COMMISSIONE EUROPEA, [COM (2002) 263], 28 maggio 2002, pag. 7

[445] Rispondono a tale obiettivo la *Direttiva 2002/21/CE* che instituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica; la *Direttiva 2002/19/CE*, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime; la *Direttiva 2002/20/CE* relativa alle autorizzazioni per le reti ed i servizi di comunicazione elettronica. Successivamente abrogate con la Direttiva 2009/140/CE del 25 novembre 2009.

Commissione e gli Stati Membri nell'implementazione delle proprie capacità in materia di cybersecurity[446]. L'importanza dell'Agenzia viene successivamente consolidata dalla Commissione nel 2013[447], la quale le attribuisce il compito di sviluppare linee guida e best practices sia per le istituzioni pubbliche sia per il settore privato entro una prospettiva temporale che si estende al 2020.

La promozione della cooperazione tra attori pubblici e privati nel settore della cybersecurity costituisce uno dei tratti caratteristici dell'azione dell'Unione Europea che, come ribadito nel 2006, si prefigge l'obiettivo di *"realizzare una Società dell'Informazione Sicura"*[448].

Entro questa prospettiva si inseriscono i successivi interventi volti, da una parte, alla definizione e alla protezione delle infrastrutture critiche[449] e, dall'altra, alla definizione delle fattispecie di reato lesive della sicurezza delle infrastrutture informatiche.

La Relazione sull'attuazione della Strategia europea in materia di sicurezza, presentata dal Consiglio dell'Unione Europea nel 2008 lega il concetto di Cybersecurity alle problematiche del terrorismo e della criminalità organizzata.

Nella costruzione del sistema europeo di sicurezza informatica, un'ulteriore rilevante documento è rappresentato dal Framework per le reti e i servizi di comunicazione elettronica[450] che obbliga gli Stati

---

[446] *Regolamento (CE) n. 460/2004* del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[447] *Regolamento (UE) 526/2013* del 21 maggio 2013 concernente l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (EINSA). L'atto, inoltre, abroga il precedente Regolamento (CE) n. 460/2004, 2013

[448] COMMISSIONE EUROPEA, *Una strategia per una società dell'informazione sicura. "dialogo, partenariato e responsabilizzazione*", [COM, (2006) 251], 12 dicembre 2006.

[449] COMMISSIONE EUROPEA, *Comunicazione relativa a un programma europeo per la protezione delle infrastrutture critiche*, [COM (2006) 786], 12 dicembre 2006; CONSIGLIO DELL'UNIONE EUROPEA, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione*, [S407/08], 11 dicembre 2008; *Direttiva 2008/114/CE* relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione; *Direttiva 2009/140/CE* del 25 novembre 2009; COMMISSIONE EUROPEA, *Proteggere le infrastrutture critiche informatizzate. Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberpertubazioni*, [COM (2009) 149, 30 marzo 2009; COMMISSSIONE EUROPEA, *Commission Staff Working Document on a new approach ti the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure* [SWD (2013) 318], 28 agosto 2013.

[450] COMMISSIONE EUROPEA, *Direttiva 2009/140/CE* del 25 novembre 2009 recante modifica delle direttive 2002/21/CE, 2002/19/CE e 2002/20/CE.

Membri ad adottare una serie di misure nazionali volte a garantirne l'attuazione.

Su di un piano più prettamente giuridico, la Commissione presenta nel 2010 una proposta volta a definire le *"fattispecie di reato nel settore degli attacchi contro i sistemi i informazione e norme minime per le relative sanzioni nonché disposizioni comuni per impedire tali attacchi e migliorare la cooperazione giudiziaria penale europea in questo campo"*[451]. Le fattispecie individuate si riferiscono i) all'accesso illecito ai sistemi di informazione; ii) l'interferenza illecita rispetto ai sistemi; iii) l'interferenza illecita rispetto ai dati; l'intercettazione illecita.

Nello stesso anno vengono pubblicati due ulteriori documenti il primo dei quali, *Agenda digitale europea*[452], si propone lo scopo di sviluppare un mercato digitale unico basato sulla rete internet veloce e su applicazioni interoperabili al fine di ottenere vantaggi socioeconomici sostenibili. L'attenzione della Commissione Europea è in questo momento rivolta ai temi mercato digitale unico e dell'interoperabilità e dei relativi standard.

Diversamente con il secondo documento, *La strategia di sicurezza interna dell'UE*[453], la Commissione rivolge la sua attenzione alle principali minacce informatiche individuando cinque momenti di sviluppo della sua azione: i) smantellare le reti criminali internazionali; prevenire il terrorismo e contrastare la radicalizzazione e il reclutamento; iii) aumentare i livelli di sicurezza per i cittadini e le imprese nel cyberspace; iv) rafforzare la sicurezza attraverso la gestione delle frontiere; v) aumentare la resilienza dell'Europa alle crisi e alle calamità.

Al fine di realizzare i punti indicati, in particolare la sicurezza dei cittadini e delle imprese, il documento strategico prevede una serie di azioni e, per il loro sviluppo, individua specifiche autorità e procedure. Vengono quindi delineati i) il centro europeo per il cybercrime; ii) un meccanismo di *incident reporting*; iii) l'European Cyber Crime Centre (EC3) nell'ambito dell'Europol a cui spetta un ruolo di coordinamento delle investigazioni a livello europeo.

---

[451] COMMISSIONE EUROPEA, *Proposta di direttiva relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio*, [COM (2010) 517], 30 settembre 2010, art. 1; 3; 6.

[452] COMMISSIONE EUROPEA, *Un'agenda digitale europea*, [COM (2010) 245 f/2], 26/08/ 2010.

[453] COMMISSIONE EUROPEA, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, [COM (2010) 673], 22 novembre 2010.

L'azione dell'Unione Europea trova un rinnovato indirizzo con l'adozione della *Strategia dell'Unione Europea per la cyber sicurezza* adottata il 7 febbraio 2013[454].

La Strategia si propone di incrementare l'accessibilità, la fruibilità e la sicurezza del cyberspace attraverso strumenti volti alla tutela dei dati e delle informazioni. Allo stesso tempo intende promuovere l'applicazione nel dominio informatico di principi norme e valori riconosciuti nel mondo fisico al fine di riaffermare i diritti fondamentali, la democrazia e lo stato di diritto.

In particolare, il riferimento è ai principi di i) protezione dei diritti fondamentali, delle libertà di espressione, dei dati personali e della privacy; ii) l'accesso alla rete gratuito per tutti; iii) lo sviluppo di sistemi di governance multistakeholder democratica ed efficiente; iv) di condivisione della responsabilità tra tutti gli attori coinvolti.

Il rispetto di tali principi è considerato essenziale al fine di raggiungere cinque obiettivi prioritari: i) lo sviluppo di capacità di cyber resilienza; ii) la drastica riduzione del cybercrime; iii) lo sviluppo di una politica e di una capacità di cyber difesa collegate alla Politica di sicurezza e di difesa comune (PEDC); iv) lo sviluppo delle risorse industriali e tecnologiche per la cyber sicurezza; v) la definizione e l'attuazione di una politica internazionale coerente dell'Unione Europea in materia di cyberspace e la promozione dei valori costitutivi dell'Unione Europea.

L'azione europea per la sicurezza del cyberspace viene ulteriormente sviluppata nel dicembre del 2018 con l'approvazione del *Cybersecurity Act*[455] elaborato dalla Commissione Europea. Il documento implementa le descritte linee d'azione, in particolare attraverso il rafforzamento dell'European Cybersecurity Agency e degli strumenti di sicurezza informatica per il settore privato.

Per quanto riguarda l'Agenzia, il documento rende permanente il suo mandato e aumenta le risorse di cui può usufruire mentre, sul piano delle competenze le viene attribuito un ruolo centrale nello sviluppo delle capacità di sicurezza informatica dei privati.

---

[454] COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Joint communication to the European Parliament, the council, the european economic commitee of the regions, Cybersecurity Strategy af the European Union: an open and secure cyberspace*, [JOIN (2013) 1 final

[455] PARLAMENTO EUROPEO, CONSIGLIO DELL'UNIONE EUROPEA, *Regulation on ENISA (The European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, Regolamento 2019/881 del 17 aprile 2019

La definizione di un framework per la certificazione europea di cybersecurity per i prodotti, i processi e i servizi costituisce il secondo elemento di novità introdotto dalla direttiva. Si tratta di una novità particolarmente importante nella prospettiva dello sviluppo delle tecnologie dell'Internet of Things e dei processi di Industry 4.0 rispetto ai quali introduce una serie di requisiti di sicurezza in grado di incidere sulla progettazione e sullo sviluppo delle nuove tecnologie (c.d. security by design).

Scopo delle norme introdotte dal Cybersecurity Act è dunque quello, da una lato, di aumentare la sicurezza e la fiducia degli utenti favorendo lo sviluppo del mercato digitale. Dall'altro, la certificazione di sicurezza informatica mira a facilitare le industrie del settore che possono ora accedere ad una certificazione unica per il mercato europeo.

3.4 Il Cybercrime nella Convenzione di Budapest.

I lavori delle Nazioni Unite in materia di cybercrime hanno sottolineato come i principali aspetti problematici siano legati alla novità della materia, alla sua transnazionalità, alle differenze tra le culture giuridiche degli Stati, oltre che all'assenza di una chiara definizione delle fattispecie criminali nel contesto del cyberspace.

Rispetto a tali problematiche l'azione svolta in ambito europeo rappresenta un momento fondamentale dell'azione di contrasto al crimine informatico a livello internazionale.

La Convenzione sul Cybercrime del Consiglio d' Europa, firmata a Budapest nel 2001, costituisce il principale strumento normativo per il contrasto delle problematiche a livello internazionale.

Il processo di elaborazione della Convenzione ha infatti registrato la partecipazione, in qualità di osservatori[456], di Stati che non sono parti del Consiglio d'Europa. Inoltre, il Trattato permette, all'art. 37, l'adesione degli Stati non Membri del Consiglio d'Europa[457].

Tali caratteristiche rendono la Convenzione di Budapest il principale framework internazionale per la cooperazione tra Stati volta a favorire

[456] Il Consiglio d'Europa ha invitato a partecipare alla redazione della Convenzione, in qualità di Osservatori, il Canada, il Giappone, il Sud Africa e gli Stati Uniti.

[457] Alla data del 8 settembre 2020, sono sessantacinque gli Stati che hanno proceduta alla ratificato o hanno aderito alla Convenzione. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

la convergenza delle politiche di contrasto ala criminalità, l'armonizzazione delle legislazioni nazionali oltre che lo sviluppo delle capacità necessarie ai fini indicati.

La convenzione si compone di quattro part dedicate i) alla definizione dei termini impiegati, ii) alle misure di livello nazionale, iii) alla cooperazione internazionale oltre ad iv) una serie di norme finali.

Vengono quindi previsti una serie di reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici quali: l'accesso illegale ad un sistema informatico (art. 2),l'intercettazione abusiva (art3), l'attentato all'integrità dei dati (art 4) e di un sistema (art. 5). Vengono considereati reati informatici in senso stretti quelli di falsificazione informatica (art. 7) e frode informatica (art. 8).

Maggiore interesse ricopre la previsione dei reati relativi ai contenuti tra cui l'art 9 annovera i reati relativi alla pornografia infantile mentre l'art. 10 si occupa dei reati contro la proprietà intellettuale.

Le norme indicate si caratterizzano per il loro forte valore simbolico, restando in capo agli Stati parti della Convenzione l'elaborazione di specifiche legislazioni in materia di criminalità informatica. La Convenzione, tuttavia, da una parte indirizza l'azione legislativa nazionale, dall'altra ne costituisce un forte stimolo allo sviluppo nella misura in cui pone l'attenzione su determinate problematiche[458].

Sul piano della cooperazione internazionale, l'art. 23 ne individua i principi generali prevedendo che *"le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale"*.

Le successive norme delineano strumenti e procedure volte a facilitare la cooperazione per quanto attiene, in particolare, lo svolgimento delle indagini, la raccolta, conservazione e trasmissione delle prove raccolte e per l'estradizione dei criminali informatici.

La Convenzione, infine, è stata integrata da un I Protocollo relativo all'uso dei sistemi informatici per attività di propaganda xenofoba e razzista. Occorre tuttavia rilevare come la Convenzione non copra tutti

---

[458] *NANCY MARION, The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation, International Journal of Cyber Criminology, Vol. 4 Issue 1&2 January – July 2010 / July – December 2010*

i reati informatici restandone esclusi, in particolare, l'adescamento di minore per fini sessuali o le attività c.d. di spam delle mail.

4. La duplice dimensione dei Diritti Umani nel Cyberspace.

Il sistema dei diritti umani costituisce un elemento fondamentale per la definizione di una disciplina giuridica applicabile al cyberspace nel quale, tuttavia, se da una parte conserva i suoi originali caratteri e funzioni, dall'altra è chiamato a confrontarsi con nuove dinamiche determinate dalle peculiarità dello spazio informatico i quali, incidendo sulle relazioni sociali e sulle strutture economiche, pongono il sistema dei diritti umani di fronte a nuove esigenze di tutela che, si sostiene, possono determinarne un ulteriore momento di evoluzione.

Nei successivi paragrafi verranno presi in considerazione alcuni aspetti del rapporto tra diritti umani e cyberspace a partire dai documenti ONU precedentemente presi in considerazione.

In primo luogo, verrà rilevata l'applicabilità del sistema dei diritti umani ai vari ambiti del cyberspace. In particolare, con riferimento alle aree tematiche lungo le quali si sviluppa l'azione delle Nazioni Unite verrà evidenziata l'applicabilità di specifici settori del sistema dei diritti umani.

In secondo luogo, verrà evidenziata, con riferimento agli interessi rilevanti nelle diverse aree tematiche indicate, la funzione attribuita alle norme e ai principi dei diritti umani. In particolare, verrà evidenziato come all'originaria funzione strumentale al mantenimento della pace e delle relazioni internazionali si affianchi la necessità di sviluppare una funzione volta a delineare i caratteri propri della persona umana al fine di delineare un limite all'incidenza del progresso tecnologico sull'uomo. In questo senso la funzione che i diritti umani sono chiamati a svolgere risponde al problema di evitare *"un uso umano dell'essere umano"*. La definizione dei caratteri propri dell'essere umano, degli aspetti che lo qualificano, la cui affermazione è funzionale a promuovere e tutelare la dignità della persona, risponde alla necessità di definire un equilibrio tra gli sviluppi tecnologici e l'uomo che mantenga il rapporto di strumentalità delle "macchine" rispetto all'uomo e ai suoi principi, valori e aspirazioni al fine di tutelare la dignità umana all'interno della Società dell'Informazione.

4.1 Applicabilità del sistema dei Diritti Umani ai vari ambiti del Cyberspace.

L'analisi svolta con riferimento all'azione delle Nazioni Unite rispetto all'emergere del cyberspace e delle sue problematiche ha evidenziato la centralità di tre aree tematiche relative: i) al rapporto tra nuove tecnologie e la sicurezza internazionale; ii) allo sviluppo di una cultura della cybersicurezza tanto delle persone quanto delle infrastrutture; iii) al rapporto tra le tecnologie della comunicazione e la promozione e il rispetto dei diritti dell'uomo.

Inoltre, i documenti presi in considerazione ribadiscono tutti l'applicabilità dei diritti umani alle questioni inerenti il cyberspace. In termini generali può qui richiamarsi l'affermazione contenuta nel Rapporto del Gruppo di Esperti Intergovernativi istituito rispetto alla sicurezza internazionale e presentato nel 2013. In esso si ribadisce che *"les action entreprise par les Etats pour assurer la sécurité informatique doivent se faire dans le respect des droits de l'homme et des libertés fondamentales énoncés dans la Declaration universelle des droit de l'homme et dans les autres instruments internationaux"*[459].

Alla generale applicabilità del sistema internazionale dei diritti umani corrisponde tuttavia la differente rilevanza dei vari diritti dell'uomo internazionalmente riconosciuti.

Entro la prima area tematica, il rispetto delle libertà fondamentali e dei diritti dell'uomo costituisce, nella prospettiva del Gruppo di Esperti Intergovernativi, un limite alle attività che gli Stati possono porre in essere al fine di assicurare la sicurezza dei propri sistemi ITC esposti ai rischi derivanti dalle azioni di altri soggetti Statali.

Le caratteristiche dell'azione conflittuale condotta attraverso le tecnologie che compongono il cyberspace sono riconducibili, come abbiamo visto, alla tipologia delle Information Operation volte, sostanzialmente, ad incidere sulla percezione della realtà e sui processi decisionali degli attori. Tale tipologia di azioni riposa sui mutamenti determinati dalle tecnologie ITC rispetto ai fattori della potenza.

Aspetti questi che possono essere chiariti richiamando le posizioni espresse dalla Federazione Russa[460]. In esse si rileva come la Rivoluzione dell'Informazione incida su tutti i domini di attività dell'uomo offrendo nuove prospettive di cooperazione internazionale e,

[459] ASSEMBLEA GENERALE, *Rapporto* GGE A/68/98, paragrafo 21
[460] ASSEMBLEA GENERALE, *Documento* A/56/213

al contempo, attribuendo un nuovo valore all'informazione, la quale diviene un elemento esternamente prezioso della ricchezza e delle risorse strategiche degli Stati. Ciò determina il rischio che i progressi nel dominio dell'informazione possano essere utilizzati a fini contrari al mantenimento della sicurezza e della pace internazionali.

L'informazione diviene infatti un'arma attraverso la quale è possibile, tra l'altro, influenzare le strutture di base di un altro Stato e il suo sistema sociale e politico; svolgere attività di manipolazione psicologica della popolazione ai fini destabilizzatori; manipolare i flussi di informazione e disinformazione al fine di mettere in pericolo l'ambiente spirituale e psicologico di un paese così come incidere sui suoi tradizionali valori spirituali, etici, estetici, morali e culturali.

Entro questa prospettiva diviene centrale il rispetto della libertà fondamentali e dei diritti umani sanciti dalla Carta delle Nazioni Unite, dalla Dichiarazione Universale e, in particolare, dai Patti sui diritti civili e politici ed economici, sociali e culturali.

All'interno dei lavori del Gruppo di Esperti l'applicabilità di tale insieme di diritti è stata più volte ribadita evidenziando una comune visione degli Stati Membri sulla questione.

Diversamente non si registra l'emergere di una visione comune rispetto all'applicabilità del diritto internazionale umanitario. Ciò in ragione del fatto che la sua rilevanza viene in discussione durante il momento conflittuale, rispetto al quale sussistono tra gli Stati divergenze in ordine alla sua disciplina in ragione della pluralità di interessi e dei diversi livelli di sviluppo tecnologico. Cionostante l'applicabilità del diritto internazionale umanitario è riconosciuta rispetto alla connessa problematica dello sviluppo dei sistemi d'arma autonomi letali.

In questo senso già il Gruppo di Esperti Informale istituito dalle Alte Parti Contraenti la Convenzione CCW nel 2013[461] sosteneva la compatibilità delle armi autonome con il diritto internazionale attuale e, in particolare, l'applicabilità dei principi di distinzione, proporzionalità e precauzione propri del diritto internazionale umanitario, rilevando inoltre l'applicabilità delle Convenzioni di Ginevra del 1949 così come della clausola di Martens e del diritto consuetudinario. Il potenziale offensivo dei sistemi d'arma letali autonomi determina inoltre la rilevanza del rispetto dei diritti umani sotto il profilo del rispetto della dignità umana, del diritto alla vita, del

[461] ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/MSP/2014/3

diritto di essere protetti contro tutti i trattamenti inumani e il diritto ad un equo processo. Tali affermazioni verranno ribadite nei successivi report redatti dai Gruppi di Esperti Governativi i quali evidenzieranno ulteriormente la centralità che ricoprono in questo ambito i principi di umanità, di proporzionalità e di discriminazione volti a tutelare gli individui da lesioni superflue e sofferenze inutili oltre che a garantirne la tutela in funzione della posizione assunta nel corso di un conflitto.

La seconda area tematica oggetto dell'azione delle Nazioni Unite prende in considerazione i problemi della sicurezza legati all'uso delle tecnologie ITC per fini criminali, alla sicurezza delle attività delle persone all'interno dello spazio informatico e, infine alla sicurezza delle infrastrutture.

Rispetto alle problematiche indicate emerge la centralità della promozione e della tutela del diritto alla vita privata riconosciuto dalla Dichiarazione Universale e dal Patto sui diritti Civili e politici. Il diritto alla privacy acquisisce all'interno del cyberspace un ruolo centrale che verrà approfondito con riferimento all'ultima linea d'azione delle Nazioni Unite specificatamente volta alla tutela dei diritti umani.

Rispetto alle tre problematiche legate alla sicurezza dello spazio informatico si può qui osservare come tale diritto venga in rilievo con riferimento alla tutela di altri specifici diritti.

Il contrasto delle attività criminali condotte nel cyberspace richiede l'utilizzo di strumenti giuridici propri del diritto penale. In questa prospettiva viene ribadita la necessità di proteggere le libertà individuali e la privacy, preservando al contempo i poteri delle autorità pubbliche funzionali al contrasto del fenomeno criminale. Il rispetto di diritti umani viene qui in rilievo in relazione alle problematiche dell'individuazione delle fattispecie incriminanti e della definizione di prova informatica e delle modalità di raccolta ed utilizzo di tali elementi probatori.

La rilevanza di questi aspetti è legata alle conseguenze che da essi discendono sull'incriminazione e quindi sul concreto esercizio dei poteri pubblici rispetto alle libertà fondamentali e ai diritti umani. Problemi che trovano origine nella stessa struttura delle norme sui diritti umani. Come rilevato dal Report del Gruppo di Esperti istituito in materia nel 2012, la disciplina delle fattispecie incriminanti, delle indagini e delle prove processuali, pone problemi di tutela delle libertà fondamentali e dei diritti umani rispetto l'esercizio dei pubblici poteri in ragione del fatto che la disciplina internazionale sui diritti umani lascia agli Stati uno spazio di discrezionalità nella determinazione dei

limiti delle forme di espressione accettabili in considerazione delle culture e delle tradizioni giuridiche degli Stati.

Il tema della cyber sicurezza come visto è stato declinato in una prospettiva più ampia in termini di costruzione di una cultura globale della sicurezza che coinvolga, in base ai rispettivi ruoli, governi, imprese, organizzazioni sociali e singole persone, nella realizzazione di attività volte ad aumentare la sicurezza dello spazio informatico. Un'azione questa che si colloca all'interno del più ampio processo di edificazione di una Società della Conoscenza incentrata sulla persona e sulla sua possibilità di accedere, utilizzare e condividere informazioni.

In questa prospettiva i diritti umani vengono in rilievo al fine di orientare l'adozione delle diverse misure di sicurezza sulla base di criteri etici che prendano in considerazione gli interessi dei diversi soggetti coinvolti. In particolare, vengono qui in rilievo i diritti e le libertà più strettamente legati al principio democratico, quali la libertà di informazione, di opinione e di espressione, la cui tutela deve essere garantita rispetto alle misure di sicurezza adottate.

Nell'ambito della sicurezza delle infrastrutture delle tecnologie ITC, in particolare Internet, il problema dei diritti umani viene in rilievo sotto il profilo della tutela del diritto alla vita privata nel contesto delle nuove tecnologie dell'Internet of Things, delle tecnologie 5G, dei Big Data e dell'Intelligenza Artificiale. Tali progressi tecnologici incidono sulla vita delle persone secondo modalità non ancora chiaramente delineate. Viene qui in evidenza il problema di tutelare il diritto alla privacy sotto il profilo della tutela dei dati personali, compresi i dati biometrici, che vengono raccolti sostanzialmente da tutti i dispositivi informatici che le persone utilizzano nella loro quotidianità.

Il diritto alla privacy costituisce il perno intorno al quale si sviluppa la terza linea d'azine delle Nazioni Unite volta ad affrontare le diverse problematiche legate al rapporto tra tecnologie informatiche e diritti umani. Tali problematiche vengono individuate nelle modalità con cui le autorità pubbliche tutelano il diritto alla privacy soprattutto in relazione alle attività di sorveglianza che le stesse autorità, così come soggetti privati, pongono in essere al fine di rispondere ad esigenze di carattere securitario.

La centralità del diritto alla vita privata è determinata dai suoi legami con altri diritti. Vengono nuovamente in rilievo il diritto a cercare, ricevere e condividere ogni tipo di informazione e idea attraverso Internet funzionali alla libertà di opinione e di espressione a loro volta funzionali all'esercizio delle libertà democratiche. Inoltre, la

funzionalità della raccolta e analisi dei dati alla ricerca e alla cattura di persone o all'utilizzo dei droni, evidenzia il legame tra la tutela del diritto alla privacy e il diritto alla vita e a non subire atti di tortura o trattamenti pregiudizievoli. Infine, le possibilità offerte dalle nuove tecnologie evidenziano l'ulteriore legame tra il diritto alla privacy e il diritto alla salute in ragione sia della raccolta di dati di natura medica, sia dell'utilizzo di dispositivi medici di natura tecnologica alla cui sicurezza è legata la salute stessa della persona che ne fa utilizzo. In questo contesto i documenti presi in considerazione ribadiscono inoltre, la generale applicabilità alle attività condotte nel cyberspace, di tutti i diritti delle persone godute offline. Allo stesso modo vengono ribaditi i limiti ai poteri pubblici derivanti dai principi di legalità, di necessità e proporzionalità dell'esercizio dei poteri pubblici.

4.2 La funzione dei Diritti dell'Uomo nel Cyberspace.

È stato precedentemente osservato come l'articolata azione condotta dalle Nazioni Unite poggi sul riconoscimento di una serie di interessi riconducibili alla Comunità Internazionale.

In questo senso si può richiamare la prima risoluzione adottata dall'Assemblea Generale nel 1998 nella quale da un lato, veniva riconosciuto il contributo che le tecnologie della comunicazione e dell'informazione possono fornire al generale progresso dell'uomo e, dall'altro, i rischi che le stesse tecnologie pongono sul piano delle relazioni internazionali in ragione della pervasività e dell'integrazione di tali tecnologie. Considerazioni peraltro comuni a tutti i documenti presi in considerazione.

Entro questa prospettiva sussiste un interesse riconducibile alla Comunità Internazionale non soltanto rispetto all'uso dello spazio informatico e dei suoi strumenti nei rapporti tra soggetti statali. Interessi di natura internazionali emergono anche rispetto alle problematiche del contrasto alla criminalità, la cui dimensione globale, può avere ripercussioni, ad esempio, sui sistemi finanziari e produttivi così come sulla fiducia degli utenti, in misura tale da incidere sulle relazioni internazionali.

Allo stesso modo, le questioni poste dalla possibilità di influenzare l'opinione pubblica di un paese, il funzionamento delle sue strutture istituzionali e le sue procedure politiche, costituiscono elementi di criticità nelle relazioni interstatali.

Entro questa prospettiva risulta abbastanza agevole sostenere la persistenza dell'originaria funzione strumentale dei diritti umani rispetto al mantenimento della pace e della sicurezza internazionale. L'affermazione e la tutela dei diritti umani rilevanti nei diversi ambiti e rispetto ai vari profili permettono infatti di riconoscere in essi un fattore di limitazione e al contempo un parametro di controllo dell'azione degli attori nel cyberspace. Promozione e tutela dei diritti umani rispondono all'esigenza di individuare dei limiti alle nuove possibilità di azione offerte dalle tecnologie dell'informazione. Allo stesso tempo, attraverso la normativa derivata, essi costituiscono un parametro di controllo dell'attività degli Stati nei diversi ambiti e nella sua dimensione applicativa.

Il cyberspace, tuttavia, non rappresenta solo uno spazio, dai caratteri peculiari, entro cui si svolge l'azione degli attori internazionali.

Come si è tentato di evidenziare, il carattere unitario del cyberspace, permette di qualificarlo quale fattore di progresso delle relazioni umane. Le modalità di raccolta, conservazione, manipolazione ed elaborazioni dei dati sorreggono lo sviluppo di nuovi progressi scientifici e tecnici grazie alla possibilità di estrapolare dai dati informazioni che possono trovare applicazione nei più svariati campi.

I dati, quali risorsa essenziale per lo sviluppo dei sistemi informatici, del cyberspace, si pongono alla base di una nuova dinamica economica il cui fattore di crescita è dato dalla capacità di estrapolare da essi informazioni di tipo predittivo sulla base delle quali strutturare i processi commerciali o la fornitura di servizi.

Tuttavia, dal punto di vista economico, le maggiori possibilità di crescita sono legate alla possibilità di predeterminare il comportamento delle persone, così come di strutturare i sistemi produttivi, in funzione delle previsioni elaborate attraverso l'utilizzo dei dati.

L'incidenza di tale dinamica sulle dinamiche sociali può essere riconosciuta nei mutamenti avvenuti nel settore musicale o nell'utilizzo dei robot in un numero crescente di attività in precedenza svolte dall'uomo. Allo stesso modo l'influenza dei processi di elaborazione dati può essere riscontrata nei diversi settori della medicina e, in particolare, delle biotecnologie dove si pongono alla base dei processi di manipolazione, ad esempio del DNA dell'uomo.

Rispetto a questi ambiti i diritti umani mutano la loro funzione.

La promozione e la tutela dei singoli diritti non rispondono alla sola necessità di limitare l'esercizio dei poteri pubblici bensì risponde alla

necessità di definire limiti al progresso tecnologico nella misura in cui il suo sviluppo incide sull'attività dell'uomo.

Si pone, in altri termini il problema di definire i caratteri qualificanti dell'Uomo al fine di preservare il carattere strumentale delle tecnologie rispetto alle attività e alle finalità determinate dall'uomo.

In questa prospettiva i diritti umani sono chiamati a tutelare la dignità umana rispetto non solo all'azione dei pubblici poteri, attraverso il riconoscimento di un bene della vita quale diritto umano, perciò, sottratto alla loro azione, bensì rispetto alle caratteristiche e alla funzionalità della tecnologia, individuando e tutelando i fattori che qualificano l'agire dell'uomo nelle sue molteplici attività.

I diritti umani sono dunque chiamati a definire i caratteri qualificanti della dignità umana al fine di determinare il limes del progresso tecnologico delineandone, al contempo, i valori e i principi di riferimento per il suo sviluppo.

Bibliografia

Libri; articoli su rivista e documenti di analisi; documenti nazionali; documenti internazionali; documenti Nazioni Unite; documenti Unione Europea; giurisprudenza; articoli di giornale.

Libri

ALPA GUIDO, ANDENAS MADS, *Fondamenti del diritto privato europeo*, Giuffré, 2005

BERNERS-LEE TIM, *Weaving the web. The original ultimate destiny of the world wide web*, HarperCollins Publisher, New York, 2000

BOSTROM NICK, *Superintelligenza. Tendenze, pericoli, strategie*, Bollati Boringhieri, Torino, 2018;

BRACKEN PAUL, *the Command and Control of Nuclear Forces*, New, Yale University Press, 1983

BROUSSEUA ERIC, MARZOUKI MERYEM, MÉADEL CÉCILE, *Governance, Regulations and Power on the Internet*, Cambridge University Press, 2015.

BRYNJOLFSSON E., MCAFEE A., *Race against the machine: how the digital revolution is accelerating innovation, driving productivity, and irreversibly trasforming employment nd the economy*, Digital Frontier Press, 2011;

BRYNJOLFSSON E., MCAFEE A., *the second machine age: work, progress and prosperity in a time of brilliant technologies*, W. W. Northon & Co. Press, 2014

CASSESE ANTONIO, *International Law*, Oxford University Press Second Edition, 2004.

CASSESE ANTONIO, *L'apertura degli ordinamenti nazionali all'ordinamento della Comunità Internazionale*, collana Lezioni Magitrali dell'Università degli Studi Suor Orsola Benincasa, Facoltà di Giurisprudenza, Edizione Scientifiche, Napoli.

CASSESE SABINO, *La crisi dello Stato*, Bari-Roma 2002

CASSESE SABINO, *Lo spazio giuridico globale*, Bari- Roma 2003

CERUZZI,PAUL E. A history of modern computing, The MIT Press, 2nd ed., 2003

CHOUCRI NAZLI, *Cyberpolitics in International Relation*, The MIT Press, 2012

CIPRIANI ALBERTO, GRAMOLATI ALESSIO, MARI GIOVANNI, *Il lavoro 4.0. La quarta Rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018

CODECASA MARIA SILVIA, *La rotta di Glauco. Viaggi per terra e per mare*, Exorma edizioni, 2011

CONFORTI BENEDETTO, *Diritto Internazionale*, Editoriale Scientifica, Napoli, 2002

CONSTANTINOU AVRA, *The right of sel-defence under costumary international law and article 51 of UN Charter*, Bruylant, 2000

CONTRAMMIRAGLIO VANNUTELLI. *Il Mediterraneo fonte risorgente della civiltà mondiale*, Cappelli, Bologna 1932

CYPRIAN BROODBANK, *Il Mediterraneo. Dalla preistoria alla nascita del mondo classico*, Einaudi, 2015

DENNING,DOROTHY *Information Warfare and Security*, Addison-Wesley Longman Ltd. Essex, UK, 1999

DETTI TOMMASO, LAURICELLA GIUSEPPE, *The Origin Of Internet*, Bruno Mondatori, Milano, 2013

DI NOLFO ENNIO, *Storia delle relazioni internazionali. Dal 1918 ai giorni nostri*, Editori Laterza Roma-Bari 2011

FERNAND BRAUDEL, *Civiltà e imperi del Mediterraneo nell'età di Filippo II,* Einaudi, 2010

FLORIDI LUCIANO, *La quarta Rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Ed., Milano 2017

FLORIDI LUCIANO, *La rivoluzione dell'informazione*, Codice edizioni, Torino, 2012

FOCARELLI CARLO, *Diritto Internazionale*, CEDAM, Milano, 2019

GENTILE EMILIO, *Ascesa e declino dell'Europa nel mondo 1898-1918*, Garzanti 2018

GIACONI MARCO, *Spazio e potere. Modelli di geopolitica*, FrancoAngeli, 2003

GIANNINI MASSIMO SAVERIO, *Il pubblico potere*, Bologna 1985

GIBSON WILLIAM, *Neuromante*, Ace Book, 1986

GLOBAL COMMISSION ON INTERNET GOVERNANCE, *Who runs the Internet? The global Multi-stakeholder model of Internet governance, Research Volume Two*.

GORI UMBERTO E LISI SERENA, *Information Warfare 2012. Armi cibernetiche e processo decisionale*, Franco Angeli, Milano, 2013

GRECO PIETRO, *La scienza e l'Europa. Il primo Novecento*, L'Asino d'oro edizioni, Roma, 2018

HARRISON JEFFREY S., BARNEY JAY B., FREEMAN R. EDWARD AND PHILLIPS ROBERT A., *The Cambrige Handobook of stakeholder theory*, Cambridge University Press, 2019

HOBSBAWM, *Age of extremes. The short twentieth century 1914-1991*, Penguin Books, 1994

HORDEN PEREGRINE, PURCELL NICHOLAS, *The Corrupting Sea*, Wiley-Blackwell, 2010.

JEAN CARLO e TREMONTI GIULIO, *Guerre stellari. Società ed economia nel cyberspazio*, Franco Angeli editore, Milano 2000

JEAN CARLO, *Geopolitica del mondo contemporaneo*, Laterza, 2012

JEAN CARLO, *Geopolitica del XXI secolo*, Laterza, 2014

JEAN CARLO, *Manuale di geopolitica*, Editori Laterza, 2010

JGLEICEMES K, *L'informazione. Una storia. Una teoria. Un diluvio*, Feltrinelli 2015

JUNGK ROBERT, *Gli apprendisti stregoni*, Einaudi Editore, 1958

KANDINSKY WASSILY, *Lo spirituale nell'arte*, SE, Milano 2005

KAPLAN JERRY, *Le persone non servono. Lavoro e ricchezza nell'epoca dell'Intelligenza Artificiale*, LUISS University Press, Roma, 2016

KENNEDY PAUL, *Il parlamento dell'uomo. Le Nazioni Unite e la ricerca di un governo mondiale*, Garzanti, 2007

KEOHANE ROBERT O., NYE JOSEPH S., *Power and Interdependence*, Boston: Little Brown, 1977

KEYNES JOHN MAYNARD, *Economic Possibilities four our Grandchildren*, Conferenza tenuta da Keynes a Madrid nel giugno del 1930. Ora nel nono volume dei suoi Collected Writings intitolato *Essay in Persuasion*, traduzione italiana, *La fine del laissez faire ed altri scritti*, Bollati Boringhieri, Torino 1991.

KRAMER FRANKLIN D, STARR STUART H., AND WENTZ LARRY K., *Cyber power and National Security*, Center for technology and national security policy, National Defense University, Washington D.C., University of Nebraska Press; 1 edition, 2009

KURZWEIL RAY , *The Singularity is Near: When Humans Trascend Biology*, Viking, New York, 2005

LANIER JARON, *La dignità ai tempi di internet. Per un'economia digitale equa*, Il Saggiatore, Milano 2014

LASSWELL H. D., *Politics: who gets what, when and how*, McGraw-Hill, New York, 1958

LIBINKY M. C., *Conquest in Cyberspace. National Security and Information Warfare*, Cambrige University Press, 2007

MARTIN HENRI-JEAN, *Storia e potere della scrittura*, Editori Laterza, Bari 2009

MAYER-SCHONMERGER VIKTOR, COKIER KENNETH, *Big Data*, Garzanti, 2017

MERCEDES BUNZ, GRAHAM MEIKLE, *The internet of things*, Polity Press, Cambridge UK, 2018

MUCCIARELLI GIUSEPPE, *La psicologia nel sentiero contemporaneo,* G. D'Anna, Messina-Firenze, 1981

NORBERT WEINER, *The Human use of human beings: cybernetics and society*, Free Association Books, London, 1989 (First published 1950)

ORGANSKI A. , *World Politics*, Knopf, New York, 1968

OSULA ANNA MARIA E HENRY ROIGAS, *International cyber Norms. Legal, Policy & Industry Perspective*, NATO CCDCOE COE Pubblications, Tallin, 2016

PICONE PAOLO, *L'applicazione extraterritoriale delle regole sulla concorrenza e il diritto interno e internazionale*, Padova, 1989

PIKETTY THOMAS, *Capitale e ideologia*, La nave di Teseo editore, Milano, 2020

QUADRI ROLANDO, *Diritto internazionale pubblico*, V° Ediz. Napoli 1968

QUINTARELLI STEFANO, *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Bollati Boringhieri, Torino 2019

RATTRAY GREGORY, *Strategic Warfare in Cyberspace*, MIT Press, Cambridge, MA, 2001

REINHARD WOLFGANG, *Storia del potere politico in Europa*, Il Mulino, 2001

ROMANO SANTI, *Discorso inaugurale dell'anno accademico 1917-1918*

ROMEO FEDERICO, *Storia della Guerra fredda. L'ultimo conflitto per l'Europa*, Einaudi 2009

ROSCINI MARCO, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, 2014

ROSSI PAOLO, *Clavis universalis. Arti della memoria e logica combinatoria da Lullo a Leibniz*, Il Mulino, 2000

RUGGE FABIO, *Confronting an "Axis of Cyberspace"? China, Iran, North Korea, Russia in Cyberspace*, ISPI, Ledizioni LediPublishing, Milano, 2018.

SCHMITT MICHAEL N., LIIS VIHUL, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*, Cambridge University press, 2017

SCHMITT MICHAEL N., *Tallinn Manual on the International law applicable to cyber warfare*, Cambridge University Press, 2013

SCHWARTAU WINN, *Information Warfare: Chaos on the Electronic Superhigway*, Thunder's Mouth, New York, 1994

SCHWARTAU WINN, *Information Warfare: Chaos on the Electronic Superhigway*, Thunder's Mouth Press, 2° Ed., 1996

SKINNER BURRHUS FREDERIC , *About Behaviorism*, Vintage Books, 1974

STEVENS TIM, *Cybersecurity and the Politics of Time*, Cambridge University Press, 2017

TETI ANTONIO, *Il potere delle informazioni. Comunicazione globale, Cyberspazio, Intelligenze della conoscenza*, Gruppo 24 Ore, 2004

TETI ANTONIO, *Lavorare con i Big Data. La guida completa per il Data Scientist*, pag. XXI Tecniche nuove, 2017

TETI ANTONIO, *PsycoTech. Il punto di non ritorno. La tecnologia che controlla la mente*, Springer, Italia, 2011

TEUBNER GUNTHER, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Armando Editore, Roma, 2005

THALER RICHARD H., *Misbehaving. La nascita dell'economia comportamentale*, Giulio Einaudi Editore, Torino 2018

TIZZANO ANTONIO, ADAM ROBERTO, *Manuale di diritto dell'Unione Europea,* G. Giappichelli Editore, 2017

TOFFLER ALVIN, The Third Wave, William Morrow and Comp. inc., New York, 1980

TSAGOURIAS NICHOLAS, BUCHAN RUSSELL, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017

TURING A. M., a cura di GABRIELE LOLLI, *Intelligenza Meccanica*, Bollati Boringhieri, Torino,1994

VESPASIANO FRANCESCO, *La società della conoscenza come metafora dello sviluppo*, Franco Angeli editore, 2005

WALLACE RUSSEL, *The wonderful century*, Dodd, Mead and Company, New York, 1899 consultabile in archive.org all'indirizzo web https://archive.org/details/wonderfulcentury028485mbp/page/n8

WALTZ EDWARD, *Information Warfare: Principle and Operations*, Artech House, Inc. Norwood, MA, USA, 1998

WEINER NORBERT *Introduzione alla cibernetica. L'uso umano degli esseri umani*, Bollati Boringhieri, Torino, 2012

WEINER NORBERT, *Introduzione alla cibernetica. L'uso umano degli esseri umani*, Bollati Boringhieri, 2012

WIENER NORBERT, *Cybernetics, or control and communication in the animal and the machine*, prima edizione: The MIT Press, Cambridge (MA), 1948; seconda edizione: Wiley, New York, 1961 (trad. italiana: *La Cibernetica - Controllo e Comunicazione nell'animale e nella macchina*, Il Saggiatore, Milano, 1968)

ZUBOF SHOSHANA, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press

Articoli su rivista e documenti di analisi

AMERICAN LAW INSTITUTE, *Restatement of the Law. The Foreign Relations of The United States*, St. Paul Minn., 1987 Vol I

ANDREI NECULAI, *Modern Control Theory – A historical perspective*, Scieri Matematice

BARAN PAUL, *On a Distribuited Command and control System Configuration*", USAF, Project RAND, Research Memorandum RM-2632, 31 December 1960

BARBERINI GIOVANNI, *Diritto internazionale umanitario nelle operazioni militari. Convenzioni, protocolli, norme di comportamento*, Centro Alti Studi per la Difesa, Istituto Internazionale di Diritto Umanitario di Sanremo, 2012.

BATTINI STEFANO, *L'impatto della globalizzazione sulla pubblica amministrazione e sul diritto amministrativo: quattro percorsi*, Giornale di diritto amministrativo n. 3/2006

BATTINI STEFANO, *La globalizzazione del diritto pubblico*, Riv. Trim. Dir. Pubb. N. 2/2006

BENNET S., *A Brief history of Automatic control*, IEEE Control System Society, June 1996

BORGIA ELEONORA, *The Internet of Things vision: Key features, application and open issues*, Computer Communications 54(2014)

BOYLAN ERIC, *Applying the Law of Proportionality to Cyber Conflict: Suggestion for Practitioners*, Vanderbilt Journal of Transnational Law, Jan 2017, Vol 50, Issue I, p. 217 – 244

BOYTE KENNET J., *A comparative analysis of the cyberattacks against Estonia, the United States, and Ukraine: Exemplifyng the evolution on internet-supported*

warfare, International Journal of Cyberwarfare and Terrorism, Volume 7, Issue 2 april-June 2017

CLARK DAVID, *Characterizing cyberspace: past, present and future*, MIT CSAIL, Version 1.2 of March 12, 2010

CLARK DAVID, *Characterizing the cyberspce: past, present and future*, MIT CSAIL Version 1.2 of March 12, 2010

COHEN HARLAN GRANT, *Multilateralism's Life Cycle*, The American Society of International Law, 2018, doi:10.1017/ajil.2018.11

COLAJANNI MICHELE, *Il ruolo dei Big Data Analytics e Machine Learning nella sicurezza*, GNOSIS 2/2017

COMELLA COSIMO, *Origine dei Big Data*", GNOSIS, 2/2017

CORN GARY P., TAYLOR ROBERT, *Sovereignty in the age of cyber*, in THE AMERICAN SOCIETY OF INTERNATIONAL LAW, *Symposium on Sovereignty, cyberspace and Tallinn Manual 2.0*, 2017

CORNISH P., LIVINGSTONE D., CLEMENTE D., YORKE C., *On Cyber Warfare.* A Chatham House Report,2010.

D'ORLANDO FABIO, *Problem, solutions and new problems whit the third wave of technological unemployment*, CreaM Working Papers Series Nr. 2/2018

DE ALCANTARA BRUNA TOSA, *SCO and Cybersecurity: Eastern Security Vision for Cyberspace*, International Relation and diplomacy, Volume 6, Number 10, (Serial Number 61) October 2018

DELLA CANANEA GIACINTO *Legittimazione e accountability nell'organizzazione mondiale del commercio*, Riv. Trim. Dir. Pubb. 200

DELLA CANANEA GIACINTO, *I pubblici poteri nello spazio giuridico globale*, Riv. Trim. Dir. Pubb. N 1/2003

ERSKINE TONI, CARR MADELINE, *Beyond "Quasi-Norms': The challenges and potential of engaging with norms in cyberspace*, in, a cura di, OSULA ANNA-

MARIA, ROIGAS HENRY, *International Cyber Norms: Legal, Policy & Industry Perspective*, NATO CCD COE Publications, Tallinn 2016.

EVANS DAVE, *Cisco Internet Business Solutions Group, The Internet of Things. How the next evolution changing everything*, Aprile 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

FALLIERE NICOLAS, LIAM O MURCHU, ERIC CHIEN, *W32.Stuxnet Dossier Version 1.4.* Symantec Corporation, February 2011, 7 consultabile all'indirizzo web www.symantec.com

FERNALD J. G., *Productivity and potential output before, during and after the great recession*, NBER Working Paper No 20248, 2014

FOCARELLI CARLO, *Self-defence in cyberspace*, in, a cura di, TSAGOURIAS NICHOLAS, BUCHAN RUSSELL, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017, pag.272.

GARTHOFF RAYMOND L., DIVINE ROBERT A., *The Sputnik Challenge*. *The American Historical Review*, Volume 99, Issue 2, April 1994, New York

GEORGE MARTA WHEELER, *The impact of Sputnik: Case study of American Pubblic Opinion at the Break of the space Age*, October 4, 1957: NASA Historical note 22, NASA History Offices Archive

HENRIKSEN ANDERS, *The end of the road for the UN GGE process: The future regulation of cyberspace*, Journal of Cybersecurity, 2019, p. 1-9.

HENRY BARBARA, *Scientia ficta, umani e non nati/e da donna nell'immaginario globale: trame robotiche nella letteratura disegnata*, Nuova corrente rivista di letteratura, 1/2017

HESSBRUEGGE JAN ARNO, *The historical development of the doctrines of attribution and due diligence in International Law*, New York Univ. Jour. of International Law and Politics, 2004

HOBSON JOHN M., SHARMAN JASON C., *The Enduring Place of Hierarchy and Political Change*, European Journal of International Relations 11 (1): 63-90, 2005;

HURD IAN, *Legitimacy and Authority in International Politics*, International Organization 53 (2): 379-408, 1999.

ILIAS O. PAPPAS, PATRICK MIKALEF, YOGESH K. DWIVEDI, LETIZIA JACCHERI, JOHN KROGSTIE, MATTI MÄNTYMÄKI (EDS.) *Digital Transformation for a Sustainable Society in the 21st Century. 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019 Trondheim, Norway, September 18–20, 2019*, Springer

INSTITUTE ASSER, *The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime*, Report https://www.asser.nl/about-the-institute/asser-today/the-tallinn-manual-20-and-the-hague-process-from-cyber-warfare-to-peacetime-regime/

INTERNATIONAL LAW ASSOCIATION, *Study Group on Due Diligence in International Law*, First Report (7 March 2014), Second Report (July 2016)

INTRALIGI VALERIO, NATICCHIONI PAOLO, *Cambiamento tecnologico e mercato del lavoro: una survey*, Università degli Studi di Roma Tre

J. LEWIS, K. VIGNARD, *Report of the International Security Cyber Issues Workshop Series*, UNIDIR, Center for strategic and International Studies (CSIS).

KEEN EDWARD, *A Case Study of the Construction of International Hierarchy: British Treaty-Making against the Slave Trade in the Early Nineteenth Century*, International Organization 61 (2): 1077-90, 2007;

KOANE ROBERT O., *Multilateralism: An Agenda for Research*, International Journal 45 (Autumn 1990)

KOH HAROLD HONGJU, *International law in cyberspace*, Yale Law Faculty Scholarship Series 2012;

LI S., PENG S., CHEN W., LU X., *Income: practical land monitoring in precision agriculture with sensor networks*, Comp. Commun. 36 (4) (2013)

LIBICKI MARTIN C., *What is Information warfare?*, Center for Advanced Concepts and Tecnology Istitute for National Strategic Studies, National Defense University, August 1995

LIBICKI MARTIN, *A debate on geopolitics. The emerging primacy of information*, Orbis Vol. 40, Issue 2, Spring 1996

LICKINDER JOSEPH C. R., *Man Computer Symbiosis*, Cornell University, 1960

LICKINDER JOSEPH C. R., *The Truly Sage System or Toward a Man-Machine System for Thinking*, 20 August 1957, 1-2

LYNN III WILLIAM J., *Defending e new domain. The Pentagon's cyber strategy*, Foreign Affairs, September/October 2010

MA J., ZHOU X., LI S., LIO Z., *Connecting agriculture to the internet of things through sensor networks*, in: Proceedings of Internet of Things (iThings/CPSCom), 2011

MANN, *The doctrine of Jurisdiction in International Law*, RC, 1964 I, 9

MARION NANCY, *The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation*, International Journal of Cyber Criminology, Vol. 4 Issue 1&2 January – July 2010 / July – December 2010

MARTINO LUIGI, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, Politica&Società, Il Mulino, 2018, vol. VII

MARTINO Luigi, *La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica*, CSSII – Centro studi Strategici, Internazionali e Imprenditoriali, 2012, consultabile https://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf

MASSA F., *Il caso San Bernardino: Apple vs FBI*, Sicurezza e Giustizia, Numero III del MMXVII.

MCCOLL L., *Fundamental Theory of Servomechanisms*, D. Van Nostrand Company inc., 1945

MCCULLOCH, PITTS, *On how we knok univwersal: the perception of auditory and visual forms*, Bulletin of Mathematical Biophysics, 1947, 9:127-147

MCKINSEY GLOBAL INSTITUTE analysis, *How we can recognize the real power of the Internet of Things?*

MILLER BEN, ATKINSON ROBERT D., *Are robot taking our jobs, or making them?*, ITIF – The Information Technology & Innovation Foundation, september 2013

MINDELL D. A., *Between human and machine – feedback, control and computing before Cybernetics*, The Johns Hopkins University Press, 2002

MÜLLER P. HANK, S., VERMESAN O., KEYBUS J. VAN DEN, *Automotive ethernet: invehicle networking and smart mobility*, in: Proceedings of the Conference on Design, Automation and Test in Europe (DATE'13), 2013

Neumann JOHN VON , *First Draft of a Report on the EDVAC*, 1945 consultabile all'indirizzo web http://web.mit.edu/STS.035/www/PDFs/edvac.pdf

NILS MELZER, *Cyber operations and Jus in bello*, in, a cura di TSAGOURIAS NICHOLAS, BUCHAN RUSSELL, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017

NOLTE D. , *How to compare regional powers: analytical concepts and research topics*, Rev. Int. Stud., 36 (4) (2010)

NYE .JOSEPH S. , *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance, Paper Series: no.1, May 2014, p. 9

OSULA ANNA-MARIA AND ROIGAS HENRY, *International Cyber Norma: Legal, Policy & Industry Perspective*, NATO CCD COE PUBBLICATIONS, TALLINN, 2016

PEDRESCHI DINO, *Data Science. La parola ai pionieri*; GNOSIS, 2/2017

PHILLIPPA BIGGS (ITU), JOHN GARRITY (CISCO), CONNIE LASALLE (CISCO) AND ANNA POLOMSKA (ITU), UNDER THE SUPERVISION OF DR. ROBERT PEPPER (CISCO), *Harnessing the Internet of Things for Global Development*, Report presentato alla ITU/ UNESCO Broadband Commission for Sustainable Development,

RAYMOND MARK, DE NARDIS LAURA, *Multi-stakeholderism: anatomy of an inchoate global institution*, in RAYMOND MARK, DE NARDIS LAURA, Thinking clearly about Multistakeholder Internet Governance, Paper presented at Eight Annual GigaNet Symposium, Bali, Indonesia, October 21, 2013.

ROSCINI MARCO, *Cyber operation as a use of force*, in NICHOLAS TSAGOURIAS, RUSSELL BUCHAN, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017

RUGGIE JOH GERARD, *International Regimes, Transactions, and change: Embedded Liberalism in the Post War Economic Order*, International Organization 36 (2);

RUGGIE JOHN GERARD, *Multilateralism: The Anatomy of an Institution*, International Organization, Vol. 46 no.3 (Summer, 1992) pp. 561-598, The MIT Press, 1992

SAMIH H., *Smart cities and internet of things*, Journal of Information Technology Case and Application Research, 21:1, 3-12, https://doi.org/10.1080/15228053.2019.1587572;

SCHIMTT M. N., L. VIHUL, *The Nature of International Law Cyber Norms*, in, a cura di ANNA MARIA OSULA E HENRY ROIGAS, International cyber Norms. Legal, Policy & Industry Perspective, NATO CCDCOE COE Pubblications, Tallin, 2016

SCHMITT MICHAEL N., *In defence of sovereignty in cyberspace*, Just Security, May 8, 2018, http://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

SCHMITT MICHAEL N., *In defence of Sovereignty in Cyberspace*, justsecurity.org, may 8, 2018, https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

SCHMITT MICHAEL N., *In defense of Due Diligence in cyberspace*, The Yale Law Journal Forum, June 22, 2015

SCHMITT MICHAEL N., *The Tallin Manual 2.0 on the International Law of Cyber Operation: What it is and isn't*, Just Security, 9 Feb. 2017, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

SCHMITT MICHAEL N., VIHUL LIIS, *Respect for Sovereignty in Cyberspace*, Texas Law Review, Vol. 95:1639, 2017

SCHMITT MICHAEL N., VIHUL LIIS, *Sovereignty in cyberspace: lex lata vel non?* in THE AMERICAN SOCIETY OF INTERNATIONAL LAW, *Symposium on Sovereignty, cyberspace and Tallinn Manual 2.0*, 2017;

SCHMITT MICHEL N., WATTS SEAN, *The decline of International Humanitarian Law Opinio Juris and The Law of Cyber Warfare*, Text. Int'ILJ 50, 2018, pag. 217

SCHMITT N. MICHAEL, *Computer network attack and the use of force in international law: thoughts on a normative framework*, Columbia Journal of Transnational Law, vol 37, 1999.

SHANNON CLAUDE E., *A Mathematical Theory of Communication*, Bell System Technical Journal, vol. 27, luglio e ottobre 1948

SHANNON CLAUDE ELWOOD, *Collected Papers*, a cura di Neil Sloane e Aron Wyner, IEEE Press, New York 1993

SHARMAN JASON C., *International Hierarchies and Contemporary Imperial Governance: A Tale of Three Kingdoms*, European Journal of International Relations, 19 (2): 189-207, 2013;

SHARP WALTER GARY, *Cyber Space and the Use of Force*, Aegis Research Corporation, USA, 1999

SOLOMONOF GRACE, *Ray Solomonoff and the Dartmouth Summer Research Project in Artificial Intelligence, 1956*

SPECTOR PHIL, *In defence of sovereignty, cyberspace, and Tallinn Manual 2.0*, in THE AMERICAN SOCIETY OF INTERNATIONAL LAW, *Symposium on Sovereignty, cyberspace and Tallinn Manual 2.0*, 2017

TEUBNER GUNTHER, *Breaking Frames: la globalizzazione economica e l'emergere della lex mercatoria*, in GUNTHER TEUBNER, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Armando Editore, 2005

TEUBNER GUNTHER, *Economia del dono, positività della giustizia: la reciproca paranoia di Jacques Derrida e Niklas Luhmann*, Sociologia e politiche sociali, 6, 1, 2003

TSAGOURIAS NICHOLAS, BUCHAN RUSSELL, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing Limited, 2017

Turing A. M., *On Computable Numbers, with an Application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society, Volume s2-42, Issue 1, 1937, Pages 230–265

VALJATAGA ANN, *Tracing opinio juris in National Cyber Security Strategy Documents*, NATO CCD COE, Law researcher, Tallinn, 2018

VARZI ACHILLE, *Storie di macchine*, La Rivista dei Libri, 9:11, 1999, 29-31

VENEZIANI ANDREA, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, Rivista Italiana di Informatica e Diritto, Fascicolo 1-2020;

VERONICA ZOLNERCIKOVA, *ICANN: Trasformation of approach toward Internet Governance*, Masaryk University Journal of Law and Technology, vol. 11 n. 1, Summer 2017, p. 158, HeineOnline

VIGNARD KERSTIN, *Confronting cyberconflict*, United Nations Institute for Disarmament Research, Disarmement Forum, four 2011

VINCENTELLI A. SANGIOVANNI-, *Let's get physical: adding physical dimensions to cyber systems*, in: Internet of Everything Summit, Roma, July 201

VINGE VERNOR, The Coming Technological Singularity: How to Survive in the Post-Human Era, in Vision-21: Interdisciplinary Science and Engineering in the Era of Cyberspace, 11-22, NASA Conference Publication 10129, NASA Lewis Research Center

VITALI F., *La geopolitica economica dei dati e il futuro del dominio. Dal controllo alla previsione. Il potere tra social media e manipolazione dell'azione sociale*, in *Nomos & Khaos*. *Rapporto Nomisma 2011-2012 sulle prospettive economico-strategiche*, Osservatorio Scenari Strategici e di Sicurezza, Nomisma Spa, A.G.R.A., Roma, 2012, pp. 207-231

VOULODIMOS A.S., PATRIKAKIS C.Z., SIDERIDIS A.B., NTAFIS V.A., XYLOURI E.M., *A complete farm management system based on animal identification using RFID technology*, Comp. Electron. Agricult. 70 (2) (2010) 380–388

WEBER COLF H., *Internet of Things – New security and privacy challenges*, Computer Law & Security Review 26 (2010)

WEBER COLF H., *Iternet of Things – Need for a New Legal Enviroment*, Computer Law & Security Review n. 25 (2009

WEST DARRELL M., *What appens if robots take the job? The impact of emerging technologies on employment and pubblic policy*, Center for Technology Innovation at Brookings, Octtober 2015

WIENER NORBERT, *The Extrapolation, Interpolation, and Smoothing of Stationary Time Series*, Report of the Services 19, Research Project DIC-6037 MIT, February 1942; poi New York: Wiley, 1949

WOHLSTETTER ALBERT, *The delicate balance of terror*, Foreign Affairs, January 1959, https://www.foreignaffairs.com/articles/1959-01-01/delicate-balance-terror

YAN-E D., *Design of intelligent agriculture management information system based on IoT*, in: Proceedings of International Conference on Intelligent Computation Technology and Automation (ICICTA), 2011, pp. 1045– 1049

ZEMANEK KARL, *Armed Attack*, Max Planck Encyclopedia of Pubblic International Law, 2012.

ZHAO J. CHUN, ZHANG J. FENG, FENG Y., XIN J. GUO, *The study and application of the IOT technology in agriculture*, in: Proceedings of 3rd IEEE Computer Science and Information Technology (ICCSIT), 2010, 2010, pp. 462–465

ZIOLKOWSKI KATHARINA, *NATO and cyber defence*, in a cura di TSAGOURIAS NICHOLAS, BUCHAN RUSSELL, *Research Handbook on International Law and Cyberspace*, Edward Elgar Pubblishing, 2017

Documenti nazionali

CANADA, *Manuale "Law of Armed Conflict"* del 2001

FEDERAZIONE RUSSA, *Doctrine of Information Security on the Russian Federation*, 2016

FRANCIA, *Cyberdefense Strategic Review*, 2018

ITALIA, *Relazione al Parlamento sulla politica dell'informazione per la sicurezza 2010*

USA, Memorandum from Jennifer M. O'Connor, Gen. Counsel of the Dep't of Def., *International Law Framework for Employing cyber Capabilities in Military Operation* Jan. 19, 2017

NATIONAL SECURITY COUNCIL, *National Security Decision Directive 32*, U.S. National Security Strategy, The White House, Washington, DC, 1982, Homeland Security Digital Library

NATIONAL SECURITY COUNCIL, Presidential Directive/NSC-18, U.S. National Strategy, The White House, Washington, DC, 1977, Homeland Security Digital Library

RUSSIA, CHINA, *Joint Statement on Cooperation in Information Space Development*

USA, U.S. Dep't of Def., Office of Gen. Counsel, *An assessement of international legal issue in information operations* (2nd ed 1999), in Computer Network Attack and International Law 459, 463-65, Michael N. Schmitt, Brian T. O'Donnel, 2002.

UFFICIO ESECUTIVO DEL PRESIDENTE DEGLI STATI UNITI, *Documento* Big Data and Privacy: A Technological Perspective

UK GOVERNEMENT. ATTORNEY GENERAL JEREMY WRIGHT, *Cyber and International Law in the 21st Century*,

CINA, *International Strategy of Cooperation on cyberspace*, 3 Jan. 2017

Documenti internazionali

NAZIONI UNITE *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*

NAZIONI UNITE, *Risoluzione Assemblea Generale* 2625 del 1970, *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States*

NAZIONI UNITE, HIGHT COMMISSIONER FOR HUMAN RIGHTS, Opening Remarks by MS. NAVI PILLAY, United Nations to the Side-event at 24th sessio of the UN Human Rights Council "How to safeguard the right to privacy in the digital age?", 20 Settembre 2013, Palais des Nations, Genevra,

NAZIONI UNITE, HIGHT COMMISSIONER FOR HUMAN RIGHTS, Opening Remarks by MS. NAVI PILLAY, to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Palais des Nations, Ginevra

NAZIONI UNITE, *Documento* E/CN.4/1990/72 del 1990

ITU, WORLD SUMMIT ON THE INFORMATION SOCIETY *Déclaration du SMSI+10 sur la mise en oeuvre des résultats du SMSI*

ITU, WORLD SUMMIT ON THE INFORMATION SOCIETY *Déclaration du SMSI+10 sur la mise en oeuvre des résultats du SMSI; Sez. C. Difficultés rencontrées pendant la mise en oeuvre des grandes orientations et problèmes récemment apparus par. 16*

ITU, WORLD SUMMIT ON THE INFORMATION SOCIETY Vision du SMSI+10 pour le SMSI au cours de l'après-2015 par. 11

ITU, WORLD SUMMIT ON THE INFORMATION SOCIETY, *Documento* WSIS-05/TUNIS/DOC/6(Rev. 1)-E

ITU, *Recommendation* ITU-T Y.2060, Overview of the Internet of Things, giugno 2012

ITU-T *Y-series Recommendations* – Supplement 33, gennaio 2016

INTERNET GOVERNANCE FORUM, *The Internet of Trust. Chair's Summary & IGF Messages*, Thirteenth Internet Governance Forum (IGF) 12-14 November 2018 Paris, France

WORKING GROUP ON INTERNET GOVERNANCE, *Report of the Working Group on Internet Governance*, Chateau de Bossey, 2005

ICRC, *Weapons: Statement of the ICRC to the United Nations*, 2017

G7, *Declaration on Responsible States Behavior in Cyberspace*, Lucca, 11 April 2017.

G20, *Dichiarazione finale* del G20 tenuto ad Osaka, Giappone, del 2019

G20, *Communique´ Antalya Summit, 15–16 November 2015*.

NATO, *Allied Joint Doctrine For Information Operation*, AJP-3.10, novembre 2009

SHANGAI COOPERATION ORGANIZATION, *Annex I to the agreement between the governaments of the member states of Shangai Cooperation Organization on cooperation in the field of international information security*, 16 June 2009

SHANGHAI COOPERATION ORGANIZATION (SCO), *Agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security*, 2009

ASEAN REGIONAL FORUM, *Concept Paper For the Establishment of Asean Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies (ISM on ICTs Security)*;

ASEAN REGIONAL FORUM, *Work Plan on Security of and in the Use of Information and Communication Tecnologies (ICTs)*, 7 May 2015

ORGANIZATION AMERICAN STATES, Resolution AG / RES. 2004 (XXXIV-O/04), *The Inter-American Integral Strategy to Combat Threats to Cyber Security*

CONSIGLIO D'EUROPA, *Convenzione sulla criminalità informatica*, Budapest 23/11/2001.

CONFERENZA SULLA SICUREZZA E LA COOPERAZIONE IN EUROPA, *Atto finale*, Helsinki, 1975

II CONVENZIONE INTERNAZIONALE DELL'AJA 1899 concernente le leggi e gli usi della guerra terrestre, Aja, 29 luglio 1899

IV CONVENZIONE DELL'AJA 1907 concernente le leggi e gli usi della guerra per terra, Aja, 18 ottobre 1907

PATTO costitutivo della Società delle Nazioni del 28 giugno 1919

TRATTATO di rinuncia alla guerra (c.d. Briand-Kellog), Parigi del 27 agosto 1928

STATUTO di Internet Corporation for assigned names and number

Documenti Nazioni Unite

ASSEMBLEA GENERALE, *Risoluzione* A/RES/53/70 del 1998, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/54/49, del 1999 Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/55/28 del 2000, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/55/63 del 2000, Combating the criminal misuse of information technologies

ASSEMBLEA GENERALE, *Risoluzione* A/RES/56/121 del 2001, Combating the criminal misuse of information technologies

ASSEMBLEA GENERALE, *Risoluzione* A/RES/56/19 del 2001, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/57/239 del 2002, Creation of a global culture of cybersecurity

ASSEMBLEA GENERALE, *Risoluzione* A/RES/57/53 del 2002, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/58/199 del 2003, Creation of a global culture of cybersecurity and the protection of critical information infrastructures

ASSEMBLEA GENERALE, *Risoluzione* A/RES/58/32 del 2003, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/59/61 del 2004, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/60/45 del 2005, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/61/54 del 2006, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/62/17 del 2007, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/63/37 del 2008, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/64/211 del 2009, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

ASSEMBLEA GENERALE, *Risoluzione* A/RES/64/25 del 2009, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/65/230 del 2010, Twelfth United Nations Congress on Crime Prevention and Criminal Justice : resolution / adopted by the General Assembly

ASSEMBLEA GENERALE, *Risoluzione* A/RES/65/41 del 2010, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/66/24 del 2011, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/67/27 del 2012, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/68/167 del 2013, The right to privacy in the digital age

ASSEMBLEA GENERALE, *Risoluzione* A/RES/68/243 del 2013, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/69/166 del 2014, The right to privacy in the digital age

ASSEMBLEA GENERALE, *Risoluzione* A/RES/69/28 del 2014, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/70/237 del 2015, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/73/266 del 2018, Advancing responsible State behaviour in cyberspace in the context of international security

ASSEMBLEA GENERALE, *Risoluzione* A/RES/73/27 del 2018, Developments in the field of information and telecommunications in the context of international security

ASSEMBLEA GENERALE, *Documento* A/43/40, Allegato VI

ASSEMBLEA GENERALE, *Documento* A/56/213 del 2001

ASSEMBLEA GENERALE, *Documento* A/69/723 del 2014, Letter, 9 Jan. 2015, from China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan. Transmits revised International Code of Conduct for Information Security; previously submitted in document A/66/359.

ASSEMBLEA GENERALE, *Documento* A/71/368 del 2016, Right to privacy: note by the Secretary-General

ASSEMBLEA GENERALE, *Documento* A/72/43103 del 2017, Social development: report of the 3rd Committee: General Assembly, 72nd session

ASSEMBLEA GENERALE, *Documento* A/73/45712 del 2018

ASSEMBLEA GENERALE *Rapporto GGE* A/60/202, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General

ASSEMBLEA GENERALE *Rapporto GGE* A/65/201, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General

ASSEMBLEA GENERALE, *Rapporto* A/66/290, Promotion and protection of the right to freedom of opinion and expression : note by the Secretary-General

ASSEMBLEA GENERALE, *Rapporto* GGE A/68/98 del 2013, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General

ASSEMBLEA GENERALE, *Rapporto* GGE A/70/174 del 2015, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/17/27, del 2011, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/23/40, del 2013, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/28/39, del 2014, Summary of the Human Rights Council Panel Discussion on the Right to Privacy in the Digital Age : report of the Office of the United Nations High Commissioner for Human Rights

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/31/64 del 2016, Report of the Special Rapporteur on the Right to Privacy: note by the Secretariat

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/32/38, del 2016, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression : note / by the Secretariat

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/34/60 del 2017, Report of the Special Rapporteur on the Right to Privacy : note / by the Secretariat

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/34/L.7/ Rev.1, del 2017, The right to privacy in the digital age : draft resolution / Albania, Angola, Argentina, Austria, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Chile, Congo, Croatia, Cyprus, Czechia, Denmark, Ecuador, Estonia, Finland, Georgia, Germany, Haiti, Honduras, Iceland, Ireland, Kenya, Latvia, Liechtenstein, Lithuania, Luxembourg, Mali, Mexico, Monaco, Montenegro, Netherlands, Norway, Panama, Paraguay, Peru, Poland, Portugal, Republic of Moldova, Romania, Serbia, Sierra Leone, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Timor-Leste, Tunisia, Ukraine

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/35/22, del 2017, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression : note / by the Secretariat

CONSIGLIO DEI DIRITTI DELL'UOMO, *Documento* A/HRC/37/62 del 2018, Report of the Special Rapporteur on the Right to Privacy: note by the Secretariat

CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/13/37, del 2009, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin

CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/17/27, del 201, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue

CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/23/40, del 2013, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue

CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/27/37, del 2014, The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights

CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/34/60, del 2017, Report of the Special Rapporteur on the Right to Privacy: note by the Secretariat

CONSIGLIO DEI DIRITTI DELL'UOMO, *Rapporto* A/HRC/37/62, del 2018, Report of the Special Rapporteur on the Right to Privacy: note by the Secretariat

CONSIGLIO ECONOMICO E SOCIALE, *Report* UNODC/CCPCJ/EG.4/2011/3,

UNODC, *Etude détaillée sur la cybercriminalité*, Ebauche – Février 2013,

UNODC, *Gruppo di Esperti sulla Cyber criminalità*, Report UNODC/CCPCJ/EG.4/2013/2,

UNODC, *Gruppo di Esperti sulla Cybercriminalità*, Report UNODC/CCPCJ/EG.4/2013/2,

ALTE PARTI CONTRAENTI CCW, *Documento* CCW/MSP/2013/10,

ALTE PARTI CONTRAENTI CCW, *Documento* CCW/CONF.V/2 del 2016,

ALTE PARTI CONTRAENTI CCW, *Documento* CCW/MSP/2014/3,

ALTE PARTI CONTRAENTI CCW, *Documento* CCW/MSP/2015/3,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/CONF.V/2 del 2016,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/MSP/2014/3,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/MSP/2014/3,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/MSP/2015/3,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/GGE.1/2017/CRP.1,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/GGE.1/2017/CRP.1,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/GGE.1/2018/3,

ALTE PARTI CONTRAENTI CCW, *Rapporto CCW*/GGE.1/2018/3,

ALTE PARTI CONTRAENTI CCW, *Rapporto* CCW/GGE.1/2019/CRP.1/Rev.2,

Documenti Unione Europea

COMMISSIONE EUROPEA *Direttiva 2002/19/CE*, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime.

COMMISSIONE EUROPEA *Direttiva 2002/20/CE* relativa alle autorizzazioni per le reti ed i servizi di comunicazione elettronica.

COMMISSIONE EUROPEA *Direttiva 2002/21/CE* che instituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica.

COMMISSIONE EUROPEA *Direttiva 2008/114/CE* relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

COMMISSIONE EUROPEA Direttiva 2009/140/CE del 25 novembre 2009

COMMISSIONE EUROPEA *eEurope 2005: una società dell'informazione per tutti*, [COM (2002) 263], 28 maggio 2002.

COMMISSIONE EUROPEA *Regolamento (CE) n. 460/2004* del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

COMMISSIONE EUROPEA *Regolamento (UE) 526/2013* del 21 maggio 2013 concernente l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (EINSA).

COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA, *Joint communication to the European Parliament, the*

council, the european economic commitee of the regions, Cybersecurity Strategy af the European Union: an open and secure cyberspace, [JOIN (2013) 1 final

COMMISSIONE EUROPEA, *Commission Staff Working Document on a new approach ti the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure* [SWD (2013) 318], 28 agosto 2013.

COMMISSIONE EUROPEA, *Comunicazione relativa a un programma europeo per la protezione delle infrastrutture critiche*, [COM (2006) 786], 12 dicembre 2006

COMMISSIONE EUROPEA, *Direttiva* 2009/140/CE del 25 novembre 2009

COMMISSIONE EUROPEA, *eEurope. Una società dell'informazione per tutti*, [COM (2000) 130], 8 marzo 2000

COMMISSIONE EUROPEA, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, [COM (2010) 673], 22 novembre 2010

COMMISSIONE EUROPEA, *Proposta di direttiva relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio*, [COM (2010) 517], 30 settembre 2010

COMMISSIONE EUROPEA, *Proteggere le infrastrutture critiche informatizzate. Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberpertubazioni*, [COM (2009) 149, 30 marzo 2009

COMMISSIONE EUROPEA, *Un'agenda digitale europea*, [COM (2010) 245 f/2], 26 agosto 2010

COMMISSIONE EUROPEA, *Una strategia per una società dell'informazione sicura. "dialogo, partenariato e responsabilizzazione*", [COM, (2006) 251], 12 dicembre 2006

CONSIGLIO DELL'UNIONE EUROPEA, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione*, [S407/08], 11 dicembre 2008

PARLAMENTO EUROPEO, CONSIGLIO DELL'UNIONE EUROPEA, *Regulation on ENISA (The European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, Regolamento 2019/881 del 17 aprile 2019.

Giurisprudenza

CORTE PERMANENTE DI ARBITRATO, *Sentenza caso Isola di Palmas*, 1928

CORTE PERMANENTE DI GIUSTIZIA INTERNAZIONALE, *Sentenza* caso "Lotus", Francia vs Turchia, 7 settembre 1927

CORTE PERMANENTE DI GIUSTIZIA INTERNAZIONALE, *Sentenza* relativa all'Accordo Greco-Turco, 1926

CORTE PERMANENTE DI GIUSTIZIA INTERNAZIONALE, *Parere* sull'interpretazione dell'art. 3 p.2 dell'Accordo di Losanna, 1925

CORTE PERMANENTE DI GIUSTIZIA INTERNAZIONALE, *Parere* sugli interessi della Germania nell'Alta Slesia polacca, 1926

CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenz*a caso *Gabcikovo-Nogymaras* del 1997

CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenza* sullo Stretto di Corfù, del 1949

CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenza* sul Tempio di Preah Vihear del 1960

CORTE INTERNAZIONALE DI GIUSTIZIA, *Parere* sugli effetti delle decisioni di indennizzo da parte del tribunale amministrativo delle Nazioni Unite del 1954.

CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenza* Military and paramilitary activities in and against Nicaragua, 1986

CORTE INTERNAZIONALE DI GIUSTIZIA, *Parere* Conseguenze legali della costruzione di un muro nei territori palestinesi occupati, del 9 luglio *2004*

CORTE INTERNAZIONALE DI GIUSTIZIA, *Parere* sulla liceità della minaccia o dell'uso delle armi nucleari, del 8 luglio 1996

CORTE INTERNAZIONALE DI GIUSTIZIA, *Sentenza* Attività armate nel territorio della Repubblica Democratica del Congo, del 19 dicembre 2005

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, *Sentenza* Digital Rights Ireland Ltd contro Minister for Communications, cause riunite C-293/12 e C-594/12, 8 aprile 2014

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, *Sentenza* Tele 2 Sverige AB vs. Post-och telestyrelsen, 21 dicembre 2016

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Sentenza* Weber e Saravia vs. Allemagne, del 29 giugno 2006

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Sentenza* Malone vs. Regno Unito, del 2008

CORTE EUROPEA DEI DIRITTI DELL'UOMO, Sentenza Roman Zakharov vs. Russie, 4 dicembre 2015

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI) DU MEXIQUE, *Sentenza*, Expediente PPD.0050/16 del 13/07/ 2016

Articoli di giornale

ROBERTA MADDALENA, Un'altra bocca messa a tacere: il caso wu gan e la censura in Cina, ilcaffègeopolitico.org, 23/01/2018;

ALESSANDRO IACUELLI, La censura cinese, Altrenotizie.org., 13/01/2006.

NICOLO BRUNO, Iran, i Green in piazza. Mistero sulla foto di Neda, articolo pubblicato il 10/02/2010 su SkyTg24 consultabile all'indirizzo web https://tg24.sky.it/mondo/2010/02/10/iran_proteste_neda_foto_errore.html)

Intervista rilasciata da Edward Snowden allla testata giornalistica The Gardian, consultabile all'indirizzo web https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Michael S. Rogers, A conversation whit Mike Roger's, Cybersecurity for a New America: big ideas and new voice, February 23, 2015, consultabile all'indirizzo https://www.newamerica.org/cybersecurity-initiative/events/cybersecurity-for-a-new-america/