Image

CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

IL CYBERSPACE: LA SOVRANITÀ NEL QUINTO DOMINIO

Il presente articolo ha ad oggetto lo studio del cyberspace, quale nuovo fronte per l'esercizio della sovranità statale. Lo scopo è quello di ricercare, grazie ad un'analisi sugli aspetti basilari e strutturali del cyberspazio, i diritti che ciascuno Stato ha nell'esercizio della sovranità nel cosiddetto "quinto dominio". Verrà affrontata l'incidenza del principio di sovranità territoriale e le difficoltà insite nell'applicazione dello stesso a un ambiente digitale, caratterizzato da una forte dematerializzazione e transnazionalità. L'analisi è svolta individuandone in breve i limiti, le possibili evoluzioni e riportando un caso di specie, al fine di stimolare una riflessione critica sulla inevitabilità di disporre un quadro normativo che regoli le attività nel cyberspazio.

di **Federica Mercurio**
IUS/13 - DIRITTO INTERNAZIONALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Mercoledì 30 Ottobre 2024

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

This article deals with the study of cyberspace, as a new front for the exercise of state sovereignty. The aim is to research, thanks to an analysis of the basic and structural aspects of cyberspace, the rights that each State has in the exercise of sovereignty in the so-called "fifth domain". This work will address the impact of the principle of territorial sovereignty and the difficulties inherent in its application to a digital environment, characterized by strong dematerialization and transnationality. The analysis is carried out by briefly identifying its limits, possible evolutions and reporting a specific case, in order to stimulate a critical reflection on the inevitability of having a regulatory framework that regulates activities in cyberspace.

Sommario: 1. Breve introduzione al mondo di internet; 2. Il Cyberspace: individuazione e caratteristiche; 3. Il Cyberspace tra sovranità interna ed esterna; 4. Un caso pratico: gli USA e il blocco della piattaforma tiktok; 5. Conclusioni.

1. Breve introduzione al mondo di internet

Dare una definizione chiara ed indipendente alla dimensione del cyberspace può sembrare un atto scontato, viste le quotidiane attività riguardanti il mondo informatico. In realtà, a partire dagli anni 90 quando la rete si era oramai rafforzata e stabilita in tutto il mondo, fu inevitabile l'adozione di una definizione che circoscrivesse il cyber-spazio. Inizialmente si pensava che questo mondo fosse totalmente indipendente rispetto alle politiche governative dei singoli Stati, tutt'oggi non può esser dichiarato lo stesso vista la portata delle operazioni svolte e soprattutto le ripercussioni avutesi rispetto ad interessi di carattere primario, quali il settore dell'economia, della sanità pubblica, della privacy e della sicurezza[1]. Al fine di comprendere le caratteristiche basilari del cyberspace è necessario partire dalla sua nascita, nello specifico soffermarsi sulla storia e sui motivi che spinsero grandi scienziati ed esperti ad investire nella ricerca di Internet.

A seguito della strage di Pearl Harbour, il governo americano stanziò una notevole quantità di fondi, destinati alla ricerca, al fine di permettere all'esercito americano di trovare nuovi strumenti, per investire nella sicurezza e nell'avanzamento della difesa. Invero, nell'anno 1958 il presidente degli Stati Uniti D.D. Eisenhower fondò l'Advanced Research Projects Agency, in abbreviato Arpa, un'agenzia del Dipartimento della Difesa statunitense il cui scopo era sviluppare nuove tecnologie militari. La prima vera scoperta di Internet vi fu pochi anni dopo, circa gli anni 60 del 900, per opera dell'Arpanet. L'Arpanet non fu altro che un progetto figlio del progetto Arpa, creato per permettere agli scienziati di scambiarsi informazioni anche da remoto.

CamminoDiritto.it
ISSN 2421-7123

L'Arpa fu guidata da personaggi illustri ed esperti del settore informatico, quale Joseph Licklider, un importante psicologo ed informatico americano, Ivan Sutherland e Robert Taylor, due professori universitari nonché pionieri dell'informatica[2]. A seguito dell'allontanamento di Licklider dal progetto, questo fu concluso da Ivan Sutherland e Robert Taylor[3]. Nel febbraio del 1967, Robert Taylor permise all'Arpa di ricevere un finanziamento importante da investire nella creazione di un programma di rete a pacchetto. Gli studi continuarono rapidamente e divennero così importanti tanto da richiedere il coinvolgimento di altri scienziati e di esperti provenienti dal settore delle comunicazioni. Infatti, nel 1967 nacque il primo router, cioè un dispositivo in grado di coordinare il traffico sul web e gestire i vari dati tra dispositivi su reti differenti, in questo modo fu possibile la condivisione della stessa connessione Internet da parte di più dispositivi[4].

Lo scopo primario, adoperato dall'Arpa, fu trovare un meccanismo che potesse tempestivamente e in modo sicuro mettere in connessione le forze militari, così da garantire accesso diretto alle comunicazioni anche a seguito di un eventuale attacco nucleare. La scoperta della rete Internet è quindi legata ad un campo prettamente militare. Tale rete qualche tempo dopo fu adoperata anche nell'ambito civile, in considerazione della sua portata e le innumerevoli prospettive di crescita[5]. Per essere più tecnici, se volessimo risalire ad una delle prime definizioni di Internet sicuramente dovremmo parlare di «una tecnica di trasmissione di dati», ovverosia un sistema che permette a più punti di poter essere connessi tra loro. Invero, la traduzione dall'inglese corrisponderebbe ad «una rete tra reti», in gergo l'abbreviazione del termine completo Inter-network. In origine il suo significato era pressoché legato ai computer, solo nell'epoca recente questo termine è stato affiancato anche ad altri dispositivi, quali cellulari, televisioni o console di videogiochi. Inoltre, la sua complicata struttura, priva di un fondamento gerarchico e di un punto centrale o di vertice impedisce che ci sia una struttura fissa, che segni una netta connessione tra le infinite macchine collegate tra loro per scambiarsi informazioni[6].

Delineati i profili storici che hanno portato all'affermazione di Internet, lo scopo di questo lavoro consisterà nell'analizzarne gli attuali risvolti, le relative caratteristiche e le possibilità di accesso al cosiddetto «cyberspazio». Oggi rispetto al passato, la portata e la frequente utilizzazione di Internet e di tutti gli accessi connessi ha portato ad un effetto quasi contrario, scatenando la diffusione di una conoscenza che se sperimentata nel modo sbagliato può portare a conseguenze di non poco conto e permettere a chi vi si pone come artefice, di nascondersi dietro l'ignoto e contemporaneamente agire nell'ignoto.

2. Il cyberspace: individuazione e caratteristiche Al fine di comprendere l'ambito di operatività entro il quale è possibile parlare di cyberspace, è necessario definire il suo significato e perimetrare i suoi confini. A tal proposito è fondamentale il riferimento al

CamminoDiritto.it
ISSN 2421-7123

concetto di sovranità in genere così come previsto dal diritto internazionale.

La sovranità statale rappresenta un principio fondamentale del diritto Internazionale consuetudinario. Quest'ultima obbliga lo Stato a non esercitare il suo potere di governo all'interno del territorio di un altro Stato, senza il suo rispettivo consenso. Tale principio, infatti, vieta allo Stato di compiere azioni che abbiano una natura coercitiva o che vengano attuate coercitivamente nel territorio di un altro Stato[7]. Nella sentenza arbitrale relativa al caso dell'Isola di Palmas nell'anno 1928, l'espressione sovranità, relativamente ai rapporti tra Stati, veniva associata alla loro "indipendenza". Nello specifico, l'indipendenza «rispetto ad una porzione del globo è il diritto di esercitarvi, con esclusione di qualsiasi altro Stato, le funzioni di uno Stato»[8]. Sono numerosi i principi e le norme di diritto internazionale consuetudinario che discendono direttamente dalla sovranità, ad esempio l'obbligo di rispettare l'immunità degli altri Stati o il rispetto della dovuta diligenza[9].

Più volte, è stato definito il termine territorio, anche in relazione al senso attribuito al concetto di sovranità. A questo punto è doveroso porsi una domanda e chiedersi "Quante implicazioni può avere la parola territorio? Quale può essere la sua interpretazione in relazione alle operazioni informatiche?". Il termine "territorio" quindi, assumerà vesti differenti in base al contesto nel quale verrà inserito e avrà una portata diversa rispetto al principio di sovranità, nello specifico in relazione al cyberspace. Il concetto di territorialità è quindi «al centro del principio di sovranità[10]» ma non sarà di certo il solo a regnarvi.

Nel mondo del cyber spazio, lo Stato può esercitare prerogative sovrane anche giurisdizionali, ad esempio su strutture informatiche o attività informatiche anche estere ed allo stesso modo ciò è concesso alle persone incaricate in queste attività[11]. Varie sono le operazioni informatiche condotte dagli Stati, nel rispetto del principio di sovranità, ma al fine di comprendere a pieno che cosa si intenda per cyber spazio, è necessario apportare delle precisazioni.

Il cyber spazio è caratterizzato da tre distinte componenti: le componenti fisiche della rete (elemento materiale) come un hardware, che può essere associato al corpo di un computer; le connessioni tra i vari dispositivi di rete (elemento logico) come dati, protocolli o applicazioni che permettono lo scambio dei dati; il livello sociale che è rappresentato dalle persone fisiche che svolgono attività informatiche[12]. Nel linguaggio odierno il cyber spazio è stato qualificato anche come di "dominio globale" o anche "quinto dominio" in quanto di natura virtuale, quindi, mancando di una vera e propria fisicità. Alcuni studiosi, invece lo ritenevano alla portata di tutti, di «comune globale»[13]. Il cyberspace fu definito come un dominio esterno rispetto all'area di sovranità degli Stati,

CamminoDiritto.it
ISSN 2421-7123

quasi come se fosse della collettività in genere e considerato come un mezzo utile a tutti[14] . Altri ancora non credevano che questo fosse un quinto dominio, essendo i vari domini della terra, concretamente e materialmente visibili o raggiungibili[15].

Ad esempio, differentemente rispetto alla terra, il mare, l'area e lo spazio, non è possibile per gli esseri umani fare una passeggiata nel cyberspazio. Oppure, secondo altre teorie, se si volesse lanciare un missile, sicuramente quest'ultimo potrebbe mirare a colpire oggetti o entità presenti sulla terra, nel mare o nello spazio, ma difficilmente mirerebbe a qualcosa localizzato nello spazio informatico. Ripercorrendo questa tesi, un caso tipico potrebbe riguardare, al massimo, la rottura di un computer con all'interno un "oggetto informatico", ma non tutti credono che un tale episodio sia qualificabile nel cyberspazio.

Altri studiosi lo definiscono non quale quinto dominio, bensì come un dominio presente in tutti e quattro gli spazi terrestri. Secondo questa tesi, lo spazio cibernetico viene individuato in relazione alla sua presenza in tutti e quattro gli ambienti in cui l'uomo esercita le sue azioni quotidiane[16].

Il mondo cibernetico è formato da una rete interdipendente di infrastrutture informatiche, cioè comprensiva di internet, reti di telecomunicazioni e sistemi informatici[17]. Il Gruppo Internazionale di Esperti (G.I.E)[18], che si occupa di studiare questo fenomeno, ha deciso di non partire da questa definizione, inquanto troppo distaccata e surreale rispetto all'esplicazione del principio di sovranità ma per identificare il cyber spazio è necessario riferirsi ad attività informatiche che si svolgono su di un territorio che siano reali e determinate o condotte da persone fisiche o giuridiche.

Anche se può sembrare un mondo tutto nuovo, rispetto alla normale circoscrizione geografica che si definisce sotto la giurisdizione di uno Stato, il cyberspace non costituisce un nuovo ambito giuridico, tanto è vero che nessuno potrà ostacolare il diritto internazionale dalla sua applicazione[19]. Proprio per questo, il riferimento al termine cyberspace non è un vocabolo di origine scientifica o tecnica ma è stato utilizzato per la prima volta da William Gibson, uno scrittore di fantascienza[20].

Gibson fu uno dei primi ad aver utilizzato il termine cyberspazio all'interno di un libro, pubblicato nell'estate del 1982, in Burning Chrome. Una bellissima descrizione di questo termine fu fatta nel 1984, nel romanzo Neuromancer, all'interno del quale veniva descritto come una «una rappresentazione grafica di dati estratti dalle banche di ogni computer nel sistema umano. Complessità impensabile. Linee di luce spaziate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci della città, che si allontanano»[21]

CamminoDiritto.it
ISSN 2421-7123

3. Il Cyberspace tra sovranità interna ed esterna Le operazioni informatiche coinvolgono oggetti, sono sviluppate su determinati territori e possono essere adottate da persone o anche entità, sui quali gli Stati sono in grado esercitare la loro sovranità. In molti casi, non è che detto che le operazioni informatiche si sviluppino in luoghi precisi attribuibili senza dubbio ad uno Stato ma potrebbero essere condotte in acque o spazi aerei internazionali o potrebbero raggiungere più frontiere. Tuttavia, qualsiasi attività informatica deve essere necessariamente condotta da soggetti o entità appartenenti alla giurisdizione di uno o più Stati[22]. In genere, salvo che non sia vietato secondo una norma di diritto internazionale, ciascuno Stato può all'interno del proprio territorio, condurre una qualsiasi attività o operazione informatica[23]. In questo caso parleremo del libero esercizio che lo Stato ha della propria sovranità interna.

Ad esempio, uno Stato costiero, che ha il controllo sul fondale del suo mare territoriale, ha di certo il controllo su ogni cavo di comunicazione localizzato al disotto di quest'ultimo, quale cavo sottomarino. Questo diritto è fondamentale, visto che, proprio attraverso i canali sottomarini vi è il passaggio delle maggiori comunicazioni di carattere internazionale[24]. Inoltre, oltrepassando la sovranità fisica, ciascuno Stato ha il diritto di organizzare o, meglio, gestire, i vari strati logici del cyberspace, per regolamentarli. Si veda il caso in cui uno Stato possa liberamente legiferare sulla normativa relativa a determinati servizi informatici, richiedendo degli specifici obblighi. Qualsiasi Stato può disporre particolari obblighi di crittografia legati alla firma elettronica, includendo dei dati che possano fornire una maggiore garanzia, a tutela dell'individuo che fruisce del servizio. Tutto ciò sempre ai fini di una maggiore sicurezza[25].

In aggiunta, la dimensione sociale del cyberspace include la possibilità per uno Stato di regolare e limitare l'accesso al mondo del cyberspace da parte dei suoi cittadini, le persone o entità, come le persone giuridiche che si trovino sul suo territorio. Per questo è legittimato agli Stati, nell'esercizio della propria sovranità interna, di disporre la censura di un contenuto condiviso da una piattaforma informatica, da un'applicazione o da un social media. Ragion per cui è del tutto lecito che lo Stato possa censurare un contenuto di natura terroristica trasmesso attraverso i social media o tramite siti web. In questo modo il diritto lecitamente esercitato dallo Stato dovrà comunque rispettare le norme di diritto internazionale applicabile, ad esempio diritti che riconoscono la libertà di espressione. Precisamente, i limiti imposti sulla possibilità di visionare un contenuto online non dovranno essere discriminatori e dovranno garantire non solo il libero esercizio della libertà di espressione ma tutti i diritti disposti dal diritto internazionale ed internazionale umanitario[26].

A questo punto è necessario porsi un interrogativo: "È possibile che un'operazione informatica determinata da uno Stato contro un altro Stato, possa costituire una violazione della sua sovranità?" Questa domanda di certo genera più di una risposta, per fare

CamminoDiritto.it
ISSN 2421-7123

chiarezza è opportuno analizzare il principio della sovranità esterna e le sue sfaccettature.

Per sovranità esterna si intende l'indipendenza dello Stato nelle sue relazioni esterne intraprese con altri Stati, inclusa la libertà di concludere accordi internazionali o di condurre operazioni informatiche, sempre nel rispetto delle norme di diritto internazionale [27]. In genere, salvo che non sia vietato da una norma di diritto internazionale, ciascuno Stato può all'interno del proprio territorio condurre una qualsiasi attività o operazione informatica, indipendentemente dal carattere pubblico o privato che la sua infrastruttura possa avere[28]. Allo stesso tempo, ai sensi dell'articolo 2 para.1 della Carta delle Nazioni Unite[29] ciascuno Stato è tenuto a rispettare l'integrità territoriale, la personalità e l'indipendenza politica degli altri Stati, non tralasciando il rispetto dei propri obblighi internazionali[30]. Quindi ogni Stato ha il diritto di intraprendere attività o operazioni informatiche con altri Stati ma nessuno Stato potrà prevalere sull'altro[31].

Si avrà quindi una violazione della sovranità il caso in cui un'operazione informatica determinata da uno Stato nel territorio di un altro Stato, ne impedisca l'esercizio delle sue funzioni sovrane; salvo in casi d'eccezione in cui è lo stesso diritto internazionale a consentirlo. Ad esempio, rappresenta un'eccezione alla violazione della sovranità l'autorizzazione del Consiglio di Sicurezza, in quanto organo esecutivo delle Nazioni Unite e responsabile del mantenimento della pace e della sicurezza internazionali[32].

Per la conduzione di un'attività informatica non è sempre necessaria la presenza fisica di un agente all'interno di un altro Stato, perché nell'ambito del cyberspace la maggioranza delle attività informatiche si svolge a distanza. Le attività di questo genere permettono di operare da qualsiasi parte del mondo contro un qualsiasi software[33] o dispositivo che si voglia alterare, controllare o danneggiare. In questo caso il G.I.E, ha valutato la presenza di determinate condizioni, affinché un'azione informatica possa violare la sovranità. Questi sono rispettivamente 1) il danno fisico, 2) la perdita di funzionalità e 3) violazione dell'integrità territoriale al di sotto della soglia di funzionalità[34].

Si veda ad esempio il caso del virus Shamoon, un virus che ha attaccato la compagnia petrolifera Saudi Aramco situata in Arabia Saudita nel 2012, a seguito dell'attacco è stato necessario riparare e sostituire migliaia dei dischi della compagnia petrolifera in oggetto. Un ulteriore requisito, che rientra tra i più importanti nell'identificazione di una effettiva violazione, corrisponde all'interferenza di un'operazione informatica contro funzioni o attività intrinsecamente governative di uno Stato. Per funzioni di questo tipo il G.I.E ha convenuto rientrassero l'interferenza con dati riguardanti: la fornitura di servizi sociali, le elezioni politiche, riscossione di tasse, sicurezza e difesa nazionale o dati riguardanti la diplomazia[35]. In questo caso la gravità dell'azione informatica svolta non sta

CamminoDiritto.it
ISSN 2421-7123

esclusivamente nella mera «invasione territoriale» dello Stato ma nelle gravissime conseguenze di natura governativa ed interna che quest'ultima possa realmente comportare. Un'attività che possa recare danni alle strutture o funzioni intrinsecamente governative può rappresentare un'arma a doppio taglio per chi la detiene, in quanto recante effetti pregiudizievoli non solo immediati ma anche futuri.

La violazione di suddette funzioni comporterà l'inosservanza del principio di sovranità, a prescindere dal luogo in cui sia stata compiuta. La loro pericolosità non può non essere sottovalutata. A seguito di un'attenta analisi sugli elementi costituenti un'invasione di sovranità, il G.I.E ha rilevato che il dolo, quale elemento intenzionale, è irrilevante ai fini della definizione di una violazione, ciò che conta sono gli effetti provocati. Quindi a prescindere dalle finalità che possano spingere uno Stato a determinare un'azione informatica contro un altro Stato, saranno gli effetti e le conseguenze recate a rilevare quale violazione per il diritto internazionale[36].

Un altro punto su cui è opportuno soffermarsi riguarda tutte quelle operazioni informatiche dirette a colpire il mercato economico nazionale, tali da comportare anche gravi perdite economiche. In questo caso non c'è conformità di opinioni nella comunità internazionale, in quanto si tratta di azioni che non comporterebbero un'alterazione o un danneggiamento di funzioni intrinsecamente governative ma che comunque potrebbero recare conseguenze ingenti all'interno della società. Si pensi all'installazione di un virus che indotto all'interno di strutture informatiche, controllanti il mercato azionario, determini rilevanti perdite finanziarie. La prassi statale è più propensa a ritenere che questo caso rappresenti una violazione della sovranità lex lata (cioè la norma così com'è) ma il G.I.E è di diversa opinione[37]. Per concludere la trattazione delle varie fattispecie oggetto della ricerca, si pensi al compimento di operazioni informatiche su o contro un veicolo, un aeromobile o una nave, che gode di immunità statale, è evidente in questo caso che le attività compiute contro di essi si intenderanno concluse contro lo Stato stesso [38].

4. Un caso pratico: gli USA e il blocco della piattaforma tiktok

Un esempio attuale, che ha ad oggetto l'azione promossa da uno Stato nel controllo di operazioni informatiche nell'esercizio della sua sovranità interna, riguarda la proposta di blocco della piattaforma social TikTok, approvata da parte del senato statunitense. Sono tante le motivazioni che hanno portato in questi anni a ridefinire l'approccio dei giovani verso questa piattaforma a causa della dipendenza creata da quest'ultima. Nello specifico, il pericolo legato all'utilizzo dei dati da parte di tiktok comporta una riproduzione di contenuti tale da creare dipendenza nei giovani e non solo. Secondo un'opinione già da tempo smentita, il motivo per cui l'attuale Presidente Joe Biden abbia deciso di proporre il

CamminoDiritto.it
ISSN 2421-7123

blocco della piattaforma riguarderebbe il pericolo di accesso, utilizzo e diffusione dei dati dei cittadini americani, da parte del governo cinese.

La causa di questo assunto è legata all'origine cinese dell'azienda che controlla il social cioè ByteDance[39]. Il timore che le informazioni potessero essere sfruttate dal governo cinese risultava apparentemente fondato. In realtà, uno studio più approfondito ha affermato che seppur di origine cinese, i dati dei circa 170 milioni di cittadini americani associati a tiktok vengono controllati e gestiti da Oracle, una società americana che agisce sul territorio americano.

Vista questa constatazione, non dovrebbe esserci il pericolo di condivisione delle informazioni dei cittadini americani. La paura che i propri dati non fossero al sicuro è stata posta anche da parte di alcuni Stati europei. A tal proposito, un ulteriore studio ha confermato che le informazioni personali relative ai cittadini europei, vengono conservate in Norvegia e in Irlanda, e tenute sotto il controllo di una società britannica[40]. Di conseguenza, anche se non sono pochi i dubbi e le preoccupazioni legate a questa tesi, non sono state rilevate prove sull'effettivo utilizzo che il governo cinese possa aver determinato dei dati legati ai profili degli utenti associati[41].

Ritornando alla proposta di legge americana, le tempistiche apposte per la sua entrata in vigore non saranno brevi. Inoltre, la proposta di legge prevede che sarà necessaria la cessione della piattaforma ad una società di origine americana a meno che la ByteDance non decida di concludere definitivamente il suo lavoro sul territorio degli Stati Uniti, prevendendo un periodo di 270 giorni per la cessione[42]. A tal riguardo, Shou Zi Chew, quale amministratore delegato della piattaforma, ha già annunciato che faranno ricorso contro la legge che prevede la cessione di tiktok[43].

La modalità di azione dell'algoritmo di tiktok[44], ha rappresentato il principale motivo di preoccupazione legato alla sua diffusione. Difatti quest'ultimo, a causa della ripetizione dei contenuti preferiti e specifici dei suoi utenti, può "promuovere o censurare" degli "argomenti" in modo da suggestionare realmente i cittadini americani. Sono tanti i profili che hanno smosso l'opinione pubblica, soprattutto sugli effetti legati all'utilizzo di questa piattaforma. Infatti, la proposta di legge non rappresenta la prima misura adottata dagli Stati Uniti. Un esempio è la legge del Montana, già adottata lo scorso anno e poi bloccata che aveva negato l'accesso della piattaforma nel territorio dello Stato[45]. L'attuale situazione presente negli Stati uniti permette di comprendere la modalità attraverso cui uno Stato possa, nei limiti del rispetto della normativa internazionale, agire per tutelare i propri cittadini. Questo avviene nel caso in cui lo stesso reputi che ci sia un utilizzo dannoso di una piattaforma. Ma quali posso essere i suoi limiti ed entro quanto lo stato potrà spingersi sorretto dall'esigenza di tutelare la sua popolazione? Quando si parla

CamminoDiritto.it
ISSN 2421-7123

di sovranità interna, si fa espresso riferimento a tutti i diritti che lo Stato ha, di poter accedere, gestire e organizzare, nel modo più idoneo, il mondo del cyberspace, anche a coloro i quali si trovino sul suo territorio.

Ovviamente, questo diritto dovrà essere esercitato nel rispetto di tutte le norme di diritto internazionale applicabili al riguardo, quali ad esempio la libertà di espressione, come già esposto in precedenza. Quindi, le eventuali limitazioni determinate, anche sulle piattaforme social, dovranno comunque rispettare i diritti ad esse connesse, e non creare discriminazioni[48]. Concludendo, si può affermare che, la sovranità non solo attribuisce diritti, ma soprattutto, prescrive obblighi giuridici. Ad esempio, è una responsabilità dello Stato, l'esercizio della dovuta diligenza, nelle azioni riguardanti la gestione o la limitazione delle operazioni informatiche presenti sul suo territorio, imponendone, se dannose, la loro fine[47].

5. Conclusioni

«Il cyber-space, complessità impensabile. Linee di luce spaziate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci della città, che si allontanano».

William Gibson

Alla luce di quanto fin qui esposto, è possibile desumere la complessità e la tecnicità dell'argomento trattato.

Nonostante i vari orientamenti e riferimenti svolti, sono ancora tanti i dubbi in merito all'individuazione delle varie attività informatiche, al controllo che ne hanno gli Stati al riguardo e ancor più la liceità delle azioni da questi esperibili. Il fine di questa ricerca è trovare una tra le soluzioni possibili, rispetto ad un'esigenza sempre più attuale, invero, spingere la collettività a coltivare la conoscenza del cyberspace, oltre i limiti entro i quali oggi viene utilizzato. Se si acquisisse una maggiore conoscenza informatica, si potrà tendere ad un livello di sicurezza più elevato, e di conseguenza anche ad un uso delle piattaforme più consapevole. Inoltre, si potrà capire in che modo agire per difendersi, in caso di violazione dei propri diritti.

La necessità di cooperare per la protezione comune non è solo un dato lampante, che permette di evidenziare i risvolti negativi dell'avanzamento tecnologico, in un mondo diventato ormai iperconnesso, ma rappresenta anche il frutto di un settore, che è in costante crescita e che soprattutto si trova alla portata di tutti.

CamminoDiritto.it
ISSN 2421-7123

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] A. STIANO, Attacchi informatici e responsabilità internazionale dello Stato, 1. La dimensione giuridica nel cyberspazio: brevi cenni, Cultura giuridica e scambi internazionali, 9, Edizioni scientifiche italiane, Napoli, 2023, 2.

[2] F. VILLA, La storia di ARPANET. Joseph Licklider fu a capo dei programmi di Scienze Comportamentali e di Comando e Controllo dell'ARPA.

[3] Ibidem.

[4] A. RUGOLO, difesaonline.it.

[5] A. STIANO, Attacchi informatici e responsabilità internazionale dello Stato, 1. La dimensione giuridica nel cyberspazio: brevi cenni, Cultura giuridica e scambi internazionali, 9, Edizioni scientifiche italiane, Napoli, 2023, 2.2 ss, cfr., G. DELLA MORTE, Big Data e protezione internazionale dei diritti umani. Regole e conflitti, Napoli, 2018, 31.

[6] Ibidem, 1, si v. G. M. RUOTOLO, Internet (diritto internazionale), in Enc. dir., 2014, 545 ss. Per maggiori approfondimenti si riveda B. CAROTTI, Il sistema di governo di internet, Milano, 2016, XIII; J. C. WOLTAG, Internet, in MPEIL, 2010

[7] B. CONFORTI. e M. IOVINE, Diritto Internazionale, XII ed., Editoriale Scientifica, Napoli, 2021, 212 ss.

[8] MICHAEL N. SCHMITT, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Part I, General international law and cyberspace, Rule 1, Sovereignty, 11 ss., per ulteriori approfondimenti si veda ISLAND OF PALMAS, arbitral award, in Reports of international arbitral awards, Netherlands, USA, 4 April 1928, Volume II, 838.

[9] Ibidem, 11-12.

[10]Ibidem.

[11] Ibidem.

[12]Ibidem.

[13] F. DELERUE, Cyber Operations and International Law, Does International law matter in cyber space?, International cyber space law, A, Cambridge University press, United Kingdom, 2020, 1.1.1.3, 10.

[14] Ibidem, 11.

[15] Ibidem, si veda anche T. RID, Cyber War Will Not Take Place, OUP, 2013, 165-166 e P. D ALLEN and D. P GILBERT, Jr, The Information Sphere Domain - Increasing Under- standing and Cooperation in Christian Czosseck and Kenneth Geers (eds), The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press, 2009, 132-142.

[16] Ibidem.

[17] Cfr. Dipartimento di Difesa americano, DoD Dictionary of Military and Associated Terms, 2010.

[18] Il termine si riferisce al Gruppo internazionale di esperti (G.I.E.) che ha lavorato alla redazione del Manuale da cui sono tratte le considerazioni ivi esposte. Nello specifico, «Il gruppo di esperti che ha redatto il Manuale ha lavorato sotto la guida del Professore Michael N. Schmitt, preside del Dipartimento di Diritto Internazionale presso lo U.S. Naval War College ed ex decano del George C. Marshall, Centro Europeo per gli studi sulla sicurezza. Il processo ha avuto inizio nel 2007 a seguito di un potentissimo attacco informatico sferrato dalla Russia a danno di siti internet di governo, banche e organismi di informazione estoni». Per ulteriori informazioni si veda F. S. DE GREGORIO, Il Manuale di Tallin 2.0, CyberLaws, 11 marzo 2019.

CamminoDiritto.it
ISSN 2421-7123

[19] F. DELERUE, Cyber Operations and International Law, Does International law matter in cyber space?, International cyber space law, A, Cambridge University press, United Kingdom, 2020, 1.1.1.3, 9.

[20] Ibidem, 10, per ulteriori approfondimenti si veda J. PRUCHER, Cyberspace, The Oxford Dictionary of Science Fiction, OUP, 2006.

[21] Ibidem, si veda inoltre, W. GIBSON, Burning Chrome, Omni, July 1984, 69, Neuromancer, Ace Books, 1984.

[22] Ibidem.

[23]MICHAEL N. SCHMITT, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Part I, General international law and cyberspace, Rule 1, Sovereignty, 13

[24] Ibidem.

[25] Ibidem, 14.

[26] Ibidem,16.

[27] Ibidem.

[28] Ibidem, 13.

[29United Nations, Charter of the United Nations, 24 Ottobre 1945, art. 2 para.1.«The Organization is based on the principle of the sovereign equality of all its members».

[30] MICHAEL N. SCHMITT, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Part I, General international law and cyberspace, Rule 1, Sovereignty, 16.

[31] Ibidem.

[32] Ibidem, 17.

[33] In informatica il termine software si riferisce all'insieme dei programmi che possono essere impiegati su un sistema di elaborazione dei dati: ad esempio un software applicativo è quello relativo ai programmi applicativi, sviluppati per una particolare funzione (scrittura, elaborazione di immagini, gestione di dati, ecc), © Istituto della Enciclopedia Italiana fondata da Giovanni Treccani.

[34] Ibidem, 21

[35]. Ibidem, 22

[36] Ibidem, 24.

[37] Ibidem, 26.

[38] Ibidem, 27.

[39] ByteDance è una società di origine cinese, è stata fondata da Zhang Yiming nel 2012, ha sede a Pechino.

[40] E. CAPONE, E se le news fossero la ragione per cui gli USA vogliono vietare TikTok? Oltre il 30% degli americani sotto i 30 anni usa TikTok per informarsi: è un valore che è triplicato in appena 3 anni, che dà fastidio a Meta e Google e viceversa potrebbe aiutare editori e giornalisti, La Repubblica, 18 marzo 2024.

[41] Ibidem.

[42] E. CAPONE, Biden ha firmato la legge sul blocco di TikTok negli Stati Uniti: ora che succede? Il provvedimento è passato al Senato insieme con il nuovo pacchetto di aiuti all'Ucraina ed è arrivato sulla scrivania del presidente, che lo ha approvato rapidamente. Ma perché diventi davvero operativo dovranno passare ancora 9 mesi, La Repubblica, 24 aprile 2024.

[43] Il POST, 2024/05/07/tiktok-ricorso-agli Stati-Uniti «Il ricorso di ByteDance si basa sulla presunta incostituzionalità della legge, che violerebbe il Primo emendamento della Costituzione degli Stati Uniti, quello che tutela la libertà di espressione. Il ricorso è stato presentato alla Corte d'Appello di Washington, ma secondo molti esperti il caso probabilmente arriverà alla Corte Suprema. La legge obbliga ByteDance a vendere entro nove mesi (che possono diventare dodici) il social network TikTok e tutte le tecnologie correlate, come il suo algoritmo, a un investitore non legato al governo cinese».

[44] Il POST, Non sarà facile vietare TikTok negli Stati Uniti.

CamminoDiritto.it
ISSN 2421-7123

[45] Ibidem.

[46] MICHAEL N. SCHMITT, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Part I, General international law and cyberspace, Rule 1, Sovereignty, 15.

[47] Ibidem.

Bibliografia

ALLEN PATRICK D and GILBERT D. P , Jr, The Information Sphere Domain - Increasing Under- standing and Cooperation, in Christian Czosseck and Kenneth Geers, eds, The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press, 2009.

ASSOCIAZIONE ITALIANA DEI COSTITUZIONALISTI, Osservatorio Costituzionale, 3 ottobre 2017, f. 3/2017.

CAPONE E., Biden ha firmato la legge sul blocco di TikTok negli Stati Uniti: ora che succede? Il provvedimento è passato al Senato insieme con il nuovo pacchetto di aiuti all'Ucraina ed è arrivato sulla scrivania del presidente, che lo ha approvato rapidamente. Ma perché diventi davvero operativo dovranno passare ancora 9 mesi, La Repubblica, 24 aprile 2024.

CAPONE E., E se le news fossero la ragione per cui gli USA vogliono vietare TikTok?, Oltre il 30% degli americani sotto i 30 anni usa TikTok per informarsi: è un valore che è triplicato in appena 3 anni, che dà fastidio a Meta e Google e viceversa potrebbe aiutare editori e giornalisti, La Repubblica, 18 marzo 2024.

CARROTTI B., Il sistema di governo di internet, Milano, 2016, XIII; J. C. WOLTAG, Internet, in MPEIL, 2010

CONFORTI B. e IOVINE M., Diritto Internazionale, XII ed., Editoriale Scientifica, Napoli, 2021.

DE GREGORIO F.S, Il Manuale di Tallin 2.0, CyberLaws, 11 marzo 2019.

DELERUE F., Cyber Operations and International Law, Does International law matter in cyber space?, International cyber space law, A, Cambridge University press, United Kingdom, 2020, 1.1.1.3.

DELLA MORTE G., Big Data e protezione internazionale dei diritti umani. Regole e conflitti, Napoli, 2018, 31

DIPARTIMENTO DI DIFESA AMERICANO, DoD Dictionary of Military and Associated Terms, 2010.

GIBSON W., Burning Chrome, Omni, July 1984, 69.

GIBSON W., Neuromancer, Ace Books, 1984.

IL POST, 2024/05/07/tiktok-ricorso-agli Stati-Uniti.

IL POST, Non sarà facile vietare TikTok negli Stati Uniti.

ISLAND OF PALMAS, arbitral award, in Reports of international arbitral awards, Netherlands, USA, Volume II, 4 April 1928, 838.

JIMÈNEZ DE ARECHAGA E., in Yearbook of the International Law Commission, 1964, vol. I., 52

PRUCHER j., Cyberspace, The Oxford Dictionary of Science Fiction, OUP, 2006.

Rid T., Cyber War Will Not Take Place, OUP, 2013.

RUGOLO A., difesaonline.it.

RUOTOLO G.M., Internet, diritto internazionale, in Enc. dir., 2014, p. 545 s.

SCHMITT MICHAEL M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Part I, General international law and cyberspace, Rule 1, Sovereignty.

STIANO A., Attacchi informatici e responsabilità internazionale dello Stato, 1. La dimensione giuridica nel cyberspazio: brevi cenni, Cultura giuridica e scambi internazionali, 9, Edizioni scientifiche italiane, Napoli.

UNITED NATIONS, Charter of the United Nations, 24 Ottobre 1945, art. 2 para.1.

VILLA F., La storia di ARPANET.

YEARBOOK OF THE INTERNATIONAL LAW COMMISSION, Osservazioni dell'Olanda, 1966, Vol II.

CamminoDiritto.it
ISSN 2421-7123

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=10596