UNIVERSITÀ DEGLI STUDI DI GENOVA
Dipartimento di Giurisprudenza

CORSO DI DOTTORATO DI RICERCA IN DIRITTO
CURRICULUM INTERNAZIONALISTICO

L'applicazione del diritto internazionale alle operazioni cibernetiche

Tutor
Prof.ssa Ilaria Queirolo
Prof.ssa Laura Carpaneto

Candidato
Dott. Matteo Daniele

XXXIV ciclo

Indice

Abbreviazioni

Carta	Carta delle Nazioni Unite
CEDU	Convenzione per la salvaguardia dei dritti dell'uomo e delle libertà fondamentali
CGUE	Corte di giustizia dell'Unione europea
CIG	Corte internazionale di giustizia
Corte EDU	Corte europea dei diritti dell'uomo
DNC	Democratic National Committee
DNS	Domain Name System
GGE	Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security
ICT	Tecnologie dell'informazione e della comunicazione
IGF	Internet Governance Forum
ISOC	Internet Society
ITRs	International Telecommunication Regulations
ITU	Unione internazionale delle telecomunicazioni
Manuale di Tallinn	M.N. Schmitt e L. Vihul (a cura di), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017
Progetto della CDI	Nazioni Unite, Commissione del diritto internazionale, *Responsibility of States for internationally wrongful acts*, in allegato alla risoluzione 56/83 dell'Assemblea generale (12 dicembre 2001)
TPIJ	Tribunale penale internazionale per la ex Jugoslavia
WSIS	World Summit on the Information Society

Glossario*

Attacco cibernetico: azione ostile finalizzata a danneggiare la riservatezza, l'integrità e la disponibilità di dati memorizzati o elaborati da sistemi informatici.

Attacco DoS/DDoS (Denial of Service/Distributed Denial of Service): attacco informatico che mira a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. Nella versione distribuita (DDoS) l'attacco proviene da un gran numero di dispositivi ed è diretto verso un target. Le botnet sono uno strumento per condurre un attacco DDoS.

Botnet: rete di computer utilizzata per attacchi da remoto, o per altre finalità, formata da computer infetti (bot o zombie) che, all'insaputa dei legittimi utenti, sono controllati da un utente malevolo (il *botmaster*).

CERT (Computer Emergency Response Team): unità organizzativa deputata a coordinare la risposta a incidenti informatici, a mitigarne gli effetti ed a prevenire il verificarsi di ulteriori eventi.

Difesa cibernetica: L'insieme della dottrina, dell'organizzazione e delle attività volte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti nel e tramite lo spazio cibernetico ovvero in danno di uno o più dei suoi elementi costitutivi.

Exploit: termine che si riferisce sia ad un mezzo informatico (in genere software) impiegato per lo sfruttamento di vulnerabilità di un sistema al fine di accedervi abusivamente o porre in essere azioni malevoli e sia alla vulnerabilità stessa.

Firewall: sistema di sicurezza perimetrale (ossia collocato nel punto in cui due reti entrano in contatto, tipicamente posto tra la rete esterna e quella interna ad una organizzazione) che protegge i dispositivi dislocati a valle del firewall da accessi non consentiti.

Indirizzo IP: codice univoco, composto, nella versione 4 del protocollo IP (IPv4), da quattro set di cifre comprese tra 0 e 255 che indentifica ogni dispositivo connesso ad una rete informatica che utilizza l'Internet Protocol.

Malware: contrazione di *malicious* software. Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

Minaccia cibernetica: espressione impiegata per indicare l'insieme delle condotte controindicate che possono essere realizzate nel e tramite lo spazio cibernetico ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici: azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare l'integrità e la riservatezza di dati/informazioni.

Phishing: attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false

email generiche a un gran numero di indirizzi. Le email sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Il *phisher* utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Ransomware: malware che cifra i file presenti sul dispositivo della vittima, richiedendo il pagamento di un riscatto per la relativa decodifica. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti che paiono legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

Sicurezza cibernetica: insieme delle misure - fisiche, logiche e procedurali - finalizzate a garantire riservatezza, integrità e disponibilità delle informazioni elaborate tramite sistemi informatici.

Spazio cibernetico: insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi.

Trojan: tipologia di malware che cela le proprie funzionalità (ad es. accesso non autorizzato, furto di credenziali, sabotaggio del sistema target) all'interno di un software legittimo (il nome deriva dal mitico Cavallo di Troia). A tale attacco sono spesso associate tecniche di ingegneria sociale, che inducono il target a scaricare/installare il software contenente il trojan.

Spoofing: tipologia di attacco informatico impiegata per falsificare (dall'inglese *to spoof*) diversi tipi di informazione come, ad esempio, il mittente di un messaggio, così da trarre in inganno il destinatario, facendogli credere che provengano da soggetti noti, attendibili o che non generino sospetti. Tale tipologia di attacco fa solitamente leva su tecniche di ingegneria sociale.

Virus: tipologia di malware capace, una volta attivato, di danneggiare documenti e file eseguibili. Il virus è caratterizzato dalla presenza di istruzioni che ne consentono la replicazione e la conseguente diffusione, che avviene durante il trasferimento del file infetto da un computer a un altro. Si differenzia dal worm, che è in grado di propagarsi autonomamente mediante diffusione dentro reti di computer o tramite email.

URL: acronimo di Uniform Resource Locator. Stringa di caratteri alfanumerici che identifica in maniera univoca l'indirizzo web di una risorsa in Internet.

World Wide Web: sistema informatico che consente la navigazione di documenti e altre risorse online, identificate tramite URL e contenente collegamenti ipertestuali. Accessibile tramite la rete Internet per mezzo di specifiche applicazioni software (cd. web browser).

[*] Le definizioni sono tratte da Presidenza del Consiglio dei Ministri, *Il linguaggio degli organismi informativi – Glossario intelligence*, maggio 2019, www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/06/glossario-intelligence-2019.pdf.

Plug me right in, jump through the screen
Final frontier, I can be anything
Maddening scenes, Anthropocene
Blink and you'll miss us like we were a dream
Baby, A.I. is the messiah
My machine's learned all my kinks and desires
Virtual porn, airbrush my jaw
Are we having fun yet?

BASTILLE, *Plug In…* (2022)

INTRODUZIONE

Connessione

1. La nascita del Web e il funzionamento di Internet

Trent'anni fa il CERN[1] prese una decisione destinata a rivoluzionare il modo di comunicare. Con la dichiarazione che rilasciò il 30 aprile 1993, la tecnologia del World Wide Web diventava gratuita e accessibile a tutti. E così è rimasta sino ai giorni nostri.

Il progetto "World Wide Web" (W3), che il suo inventore Tim Berners-Lee aveva così chiamato ispirandosi alla struttura operativa del CERN, simile a una rete le cui interconnessioni erano destinate a evolvere nel tempo, nacque nel 1989, quando si rese necessaria la creazione di un sistema di documenti collegati insieme e accessibili via Internet ai fisici e agli ingegneri del CERN. Il primo sito mai realizzato era dedicato proprio al progetto W3 e descriveva le funzioni principali del Web (come accedere ai documenti delle altre persone e come configurare il proprio server).

Da archivio virtuale consultabile solo da gruppi ristretti di persone, il Web si è trasformato in «un grande catalogo globale in cui tutte le informazioni prodotte dal genere umano fossero messe in correlazione fra loro per creare a loro volta nuova conoscenza»[2].

Rolf Heuer, Direttore Generale del CERN, ha dichiarato che l'invenzione del Web ha trasformato ogni settore della società, dalla ricerca all'impresa all'educazione. Il Web ha rimodellato il modo in cui noi comunichiamo, lavoriamo, innoviamo e viviamo. Esso offre una chiara dimostrazione di come la ricerca di base possa beneficiare il genere umano[3].

Web e Internet vengono spesso utilizzati come sinonimi, ma non sono la stessa cosa. Il Web è solo un servizio di Internet, uno spazio digitale per la pubblicazione di

---

[1] L'Organizzazione europea per la ricerca nucleare, comunemente conosciuta come CERN (acronimo del francese "Conseil européen pour la recherche nucléaire", il consiglio provvisorio fondato nel 1952 con il compito di allestire un'organizzazione di ricerca di fisica fondamentale in Europa) è un ente internazionale istituito con la convenzione firmata a Parigi il 1° luglio 1953 da 12 Stati europei, fra cui l'Italia. Il laboratorio del CERN, il più grande al mondo di fisica delle particelle, si trova al confine tra Svizzera e Francia vicino a Ginevra, nel comune di Meyrin.

[2] F. Caccavella, *Il CERN festeggia i 20 anni del Web e rimette on line la prima home page*, 30 aprile 2013, www.repubblica.it/tecnologia/2013/04/30/news/il_cern_festeggia_i_20_anni_del_web_e_rimette_on_line_la_prima_home_page-57805889/.

[3] Cfr. M. Giampietro, *Twenty years of a free, open web*, 30 aprile 2013, home.cern/news/news/computing/twenty-years-free-open-web.

contenuti multimediali. Internet, invece, è una rete universale di reti. Più propriamente, Internet è "la Rete".

Potremmo immaginare la rete Internet come un'enorme ragnatela che avvolge tutto il mondo: i fili di questa ragnatela rappresentano le singole sottoreti di apparecchi collegati che la compongono, e i ragni che la attraversano costituiscono i dati che vengono trasferiti da un punto all'altro, mentre i nodi che si formano quando i fili s'incrociano sono i punti in cui le diverse reti s'incontrano.

I vari dispositivi (non solo computer, ma anche televisioni, smartphone, console per videogiochi) hanno la possibilità di comunicare fra loro grazie a un segnale che può viaggiare attraverso mezzi differenti, come i cavi per le comunicazioni telefoniche e le fibre ottiche, o nell'etere, come nel caso delle connessioni Wi-Fi. La circostanza che la Rete è suddivisa in sezioni indipendenti l'una dall'altra implica che «nessuna sottorete è in grado di controllare tutta la Rete, né, d'altro canto, la rottura o il blocco di una sottorete comporta la perdita di funzionalità del meccanismo complessivo di trasmissione dei dati»[4].

L'interconnessione delle reti è resa possibile da un pacchetto di protocolli di comunicazioni, conosciuto come "suite di protocolli TCP/IP" (Transmission Control Protocol/Internet Protocol): quelli di base sono l'FTP (File Transfer Protocol) per trasferire i file da una macchina all'altra, la posta elettronica per scambiare messaggi, l'HTTP (Hypertext Transfer Protocol) per il funzionamento del World Wide Web. Tali protocolli costituiscono il codice di comunicazione, un insieme di regole pubbliche aperte a tutti in base a cui macchine fra loro molto diverse riescono a dialogare, indipendentemente dall'hardware e dal software che esse utilizzano. Il c.d. "instradamento dei dati" funziona in questo modo: essi vengono smembrati in gruppi elementari chiamati pacchetti (o *datagram*) e dopo aver viaggiato autonomamente nella Rete, indirizzati da apparecchiature riservate a questo scopo (gateway, router, switch), vengono ricomposti dalla macchina di destinazione.

[4] G.M. Ruotolo, *Internet-ional law. Profili di diritto internazionale pubblico per la Rete*, Bari, 2012, pag. 25.

2. Gli orientamenti sulla disciplina dello spazio cibernetico

In passato si è svolto un dibattito in merito al modo migliore per dettare compiutamente ed efficacemente una disciplina giuridica per lo spazio cibernetico. In dottrina si rinvenivano due orientamenti principali.

Il primo sosteneva l'inapplicabilità del diritto come strumento di regolazione dello spazio cibernetico e dei comportamenti che vi si svolgono. Tale tendenza è ben sintetizzata dalla Dichiarazione di indipendenza dello spazio cibernetico[5], che si rivolge direttamente agli Stati:

> You are not welcome among us. You have no sovereignty where we gather. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders.

Questo approccio proponeva di utilizzare dei meccanismi di disciplina autonomi, sviluppati spontaneamente dagli stessi internauti: le nuove regole farebbero parte di un nuovo *genus* di diritto, né statale né internazionale, la c.d. *cyber-law*. In questo modo, lo spazio cibernetico verrebbe a configurarsi come uno "spazio senza legge"[6], sottratto alla giurisdizione statale, alla stregua dell'alto mare o dello spazio extra-atmosferico, e, a differenza di questi ultimi, immune anche alle norme di diritto internazionale.

L'altro orientamento, più tradizionalista, si fondava sul presupposto che la Rete costituisse semplicemente un nuovo mezzo di comunicazione, e che, in quanto tale, potesse essere giuridicamente regolabile attraverso l'armonizzazione fra i vari ordinamenti statali. Questa visione prevedeva che i vari legislatori nazionali si occupassero di adottare le normative di dettaglio all'interno di un quadro giuridico comune, formatosi in seguito alla definizione di alcuni concetti generali ad opera del diritto internazionale. Le norme di diritto internazionale pubblico si rivelano, infatti, le più adatte alla disciplina della gestione dello spazio cibernetico come infrastruttura, mentre quelle di diritto internazionale privato provvederebbero a individuare la giurisdizionale nazionale competente a dirimere

[5] La Dichiarazione di indipendenza dello spazio cibernetico è stata scritta da John Perry Barlow, uno dei fondatori della Electronic Frontier Foundation, e pubblicata online l'8 febbraio 1996, in risposta alla conversione in legge negli Stati Uniti del Telecommunications Act. La Dichiarazione è pubblicata integralmente all'indirizzo projects.eff.org/~barlow/Declaration-Final.html.

[6] L'espressione è di A. Gigante, *Blackhole in Cyberspace: The Legal Void in the Internet*, in *John Marshall Journal of Computer and Information Law*, 1997, pag. 413 ss.

una controversia relativa a una fattispecie che abbia luogo online, e il diritto applicabile alla medesima.

A metà strada tra i due orientamenti appena illustrati, s'inseriva una terza modalità di lettura del problema in questione. Secondo questo approccio, lo spazio cibernetico sarebbe compiutamente regolabile dal suo codice informatico, che ne determina accidentalmente la natura. Esso è composto dall'insieme delle apparecchiature (hardware) che la compongono e del software che ne consente l'uso. Ai legislatori internazionali spetterebbe unicamente il compito di dettare norme giuridiche uniformi che fissino i valori da assumere come parametro di riferimento del suddetto codice.

Oggi la questione della disciplina dello spazio cibernetico è risolta sia nella letteratura accademica sia nella prassi degli Stati: l'applicabilità del diritto internazionale allo spazio cibernetico e alle operazioni cibernetiche è stata riconosciuta nei rapporti consensuali del gruppo degli esperti governativi incaricati dalle Nazioni Unite di esaminare lo sviluppo dell'informatica e delle tecnologie nel contesto della sicurezza internazionale (GGE)[7], e molti Stati hanno confermato questo orientamento nei propri commenti al Segretario generale delle Nazioni Unite e nelle strategie nazionali sulla difesa e sulla sicurezza cibernetiche. Il dibattito si è pertanto concentrato sull'interpretazione e sulla concreta applicazione delle norme di diritto internazionale allo spazio cibernetico. Le sfide da considerare in questo ambito sono tre: in primo luogo, l'applicazione del diritto internazionale alle operazioni cibernetiche richiede un certo grado di adattamento; in secondo luogo, i soggetti di diritto internazionale, e in particolare gli Stati, possono avere interpretazioni diverse delle specifiche norme di diritto internazionale[8]; in terzo luogo, lo sviluppo dello spazio cibernetico mette alla prova norme di diritto internazionale che già affrontano un certo grado di incertezza e contestazione sia nel loro contenuto che nella loro applicazione.

[7] Nazioni Unite, Assemblea generale, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 giugno 2013); Id., *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 luglio 2015).

[8] Nel 2017, il quinto GGE non ha adottato il rapporto finale perché gli esperti governativi provenienti dalla Cina, Da Cuba e dalla Russia si sono opposti al paragrafo 34 della sua bozza, che precisava come applicare alcune norme di diritto internazionale alle tecnologie dell'informazione e della comunicazione.

3. Le norme specificamente applicabili allo spazio cibernetico

È difficile credere che il diritto internazionale generale possa contenere norme applicabili esclusivamente allo spazio cibernetico, «non tanto per il breve lasso di tempo intercorso dalla sua diffusione su base globale, che può datare, al massimo, agli ultimi due/tre anni del secolo scorso, ma soprattutto per il contenuto materiale che norme siffatte dovrebbero avere, eccessivamente complesso e dettagliato per essere oggetto di una norma consuetudinaria»[9]. Appare anzi evidente l'assenza di norme di diritto internazionale generale specificamente volte a limitare la *domestic jurisdiction* degli Stati in queste materie, come attesta una dichiarazione del governo statunitense che riconosce esplicitamente l'esistenza di un interesse comune a tutti gli Stati alla permanenza della funzionalità della Rete[10].

D'altra parte, gli strumenti più adatti per la disciplina di Internet e di tutti gli altri fenomeni transnazionali sembrano essere i trattati internazionali. Le considerazioni espresse all'interno del dibattito sulle norme più efficaci per la tutela ambientale, di fatto, si rivelano azzeccate anche per lo spazio cibernetico e la sua regolazione:

> Sono le norme pattizie quelle davvero in grado di imporre determinati comportamenti agli Stati, conferire loro diritti verso altri Stati e, al loro interno, stabilire omologhe relazioni giuridiche nei confronti dei soggetti sui cui gli Stati stessi esercitano il loro potere normativo[11].

Le convenzioni internazionali non sono del tutto prive di aspetti negativi. Specialmente i c.d. grandi trattati, che vogliono dettare regole applicabili a un gran numero di Stati, soffrono alcuni limiti: l'esigenza di radunare molti Stati all'interno di un forum negoziale allunga i tempi di gestazione del trattato, e la difficoltà di trovare valori comuni costringe ad adottare soluzioni di compromesso, ovvero norme di carattere procedurale e strumentale.

[9] G.M. Ruotolo, op. cit., p. 56.

[10] Stati Uniti, Department of Commerce, National Telecommunications and Information Administration, *U.S. Principles on the Internet's Domain Name and Addressing System*, 30 giugno 2005, www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system.

[11] F. Munari e L. Schiano di Pepe, *Tutela transnazionale dell'ambiente*, Urbino, 2012, pag. 53.

3.1. La Convenzione sulla criminalità informatica di Budapest

Ad oggi, la Convenzione sulla criminalità informatica[12] non è soltanto il primo trattato internazionale sui reati commessi via Internet, ma è anche l'unico in vigore che si occupi esplicitamente di fattispecie generali collegate alla Rete intesa come infrastruttura. La Convenzione è stata promossa dal Consiglio d'Europa ed è stata aperta alla sottoscrizione degli Stati a Budapest il 23 novembre 2001. Essa si prefigge di perseguire una politica criminale comune finalizzata alla protezione contro il crimine cibernetico, fornendo un quadro normativo attraverso cui gli Stati membri possano procedere all'armonizzazione del diritto penale nazionale in materia di reati commessi via Internet (violazione del diritto d'autore, frodi telematiche, pedofilia, attentati all'integrità delle reti).

Il preambolo della Convenzione, nel ricordare l'esigenza di trovare un compromesso tra gli interessi dell'azione repressiva e il rispetto per i diritti umani, richiama esplicitamente la Convenzione per la salvaguardia dei dritti dell'uomo e delle libertà fondamentali (CEDU) del 1950, il Patto sui diritti civili e politici del 1966 e gli altri trattati internazionali applicabili sui diritti umani.

Il trattato è composto da quattro capitoli divisi in sezioni: uso dei termini, provvedimenti da adottare a livello nazionale (diritto penale sostanziale, diritto procedurale, competenza), cooperazione internazionale (principi generali, disposizioni specifiche), disposizioni finali. Il primo capitolo consta del solo art. 1 e contiene la definizione di alcuni concetti fondamentali per il funzionamento della Rete:

> a. "sistema informatico" indica qualsiasi apparecchiatura[13] o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati;
> b. "dati informatici" indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione;
> c. "service provider" (fornitore di servizi), indica:
> i. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico;

[12] Il Parlamento italiano ha autorizzato la ratifica della Convenzione con legge 18 marzo 2008, n. 48, *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, in GU 4 aprile 2008, n. 80. La Convenzione, a norma dell'art. 36, paragrafo 4, della stessa, è entrata in vigore il 1° ottobre 2008.

[13] Il termine "apparecchiatura" non si riferisce ai soli oggetti fisici, ma può ricomprendere anche programmi informatici. La stessa Convenzione, in base all'art. 6, fa rientrare un "programma per computer" tra le apparecchiature che possono essere utilizzate per scopi vietati.

ii. qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;

d. "trasmissione di dati" indica qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo di servizio.

Benché la dottrina giuridica abbia spesso trascurato le norme definitorie contenute nella Convenzione sulla criminalità informatica – per dedicarsi alla disciplina dei comportamenti statali o individuali che hanno luogo sul Web e che lo utilizzano come mezzo – esse sono determinanti nel processo di creazione di un quadro giuridico di diritto internazionale per lo spazio cibernetico, in quanto si tratta delle uniche norme comuni di definizione degli elementi tecnici di Internet e sarebbero idonee a produrre i loro effetti anche al di fuori del sistema della Convenzione.

3.2. Soft law e codici di autoregolamentazione

Le fonti di *soft law*, come le risoluzioni del Parlamento europeo o dell'Assemblea generale, sono «atti e manifestazioni della prassi, i quali hanno in comune un elemento di carattere negativo, che consiste nell'assenza di effetti giuridici vincolanti»[14]. Esse prendono la forma di raccomandazioni, norme programmatiche o proposizioni che orientano il comportamento degli attori del diritto internazionale e provengono da soggetti privi del potere di emanare regole di condotta vincolanti.

La loro mancanza di obbligatorietà produce alcuni effetti rilevanti: da una parte, è più facile costruire la regola, dal momento che non si pone il problema di imporne l'effettiva applicazione; dall'altra, la sua applicazione su base volontaristica fornisce delle indicazioni in merito alla necessità di rapide correzioni, nonché alla possibilità della sua trasformazione in regola precettiva, da norma esortativa qual è. Questi atti hanno anche il pregio di trasferire a livello di opinione pubblica riflessioni organizzate su un determinato problema. La loro flessibilità è particolarmente richiesta in quei settori ritenuti sensibili dai legislatori statali o a uno stato non definitivo di sviluppo. Accade frequentemente, dunque, che questi documenti costituiscano «l'antecedente necessario rispetto a

[14] R. Luzzatto, *Il diritto internazionale generale e le sue fonti*, in S.M. Carbone, R. Luzzatto, A. Santa Maria (a cura di), *Istituzioni di diritto internazionale*, Torino, 2011, pag. 83.

norme cogenti, che riescono poi a trovare applicazione e consenso in quanto preventivamente discusse e testate su base volontaristica»[15].

Relativamente alla disciplina dello spazio cibernetico, questo tipo di strumenti giuridici è stato utilizzato soprattutto per la fissazione di principi generali di tipo materiale e per l'adozione di norme di contenuto procedimentale. Nel loro complesso, ribadiscono l'esistenza dell'interesse di tutti i soggetti coinvolti a una gestione comune della Rete. Questi atti sono stati adottati in primo luogo nell'ambito del World Summit on the Information Society (WSIS), come la Dichiarazione di Ginevra e l'Agenda di Tunisi, ma anche l'Assemblea generale delle Nazioni Unite ha provveduto ad adottare una risoluzione in cui sottolinea l'importanza del coinvolgimento dei soggetti non statali nei vari forum negoziali[16]. Nello specifico, l'Assemblea generale incoraggia una cooperazione rafforzata e continua fra i diversi portatori d'interesse, al fine di assicurare l'effettiva implementazione dei risultati delle fasi di Ginevra e Tunisi del WSIS, attraverso la promozione di associazioni e piattaforme nazionali, regionali e internazionali, in un dialogo che includa anche i Paesi meno sviluppati e gli attori nel settore delle tecnologie dell'informazione e della comunicazione.

All'interno della variegata tipologia di norme di *soft law* rientrano anche i c.d. codici di condotta, con cui si definiscono «quei complessi di disposizioni non vincolanti con i quali soggetti tra loro omogenei e che sono al contempo i destinatari delle indicazioni ivi contenute, provvedono ad auto-definire certi standard (linee guida) che devono guidare il loro stesso comportamento in un determinato settore»[17]. A differenza dei codici di autoregolamentazione applicabili nel "mondo reale", tuttavia, quelli destinati allo spazio cibernetico, come le linee di condotta o le condizioni d'uso di Facebook, Twitter, LinkedIn, YouTube, Vimeo ed eBay, non sono quasi mai adottati dagli stessi soggetti ai quali si impongono, bensì dai gestori dei siti che offrono servizi online (social network, video-hosting, transizioni commerciali). Le linee guida di comportamento imposte da detti codici contemperano, generalmente, l'esigenza di garantire la libertà di espressione degli utenti con la necessità di rispettare la privacy e i diritti di proprietà intellettuale.

A favore dall'autoregolamentazione si sono espresse le istituzioni europee, che già a partire dal 1999 hanno sottolineato la necessità «di analizzare il contributo che i

[15] F. Munari e L. Schiano di Pepe, op. cit., p. 66.

[16] Risoluzione 64/187 dell'Assemblea generale, *Information and communication technologies for development*, A/RES/64/187 (9 febbraio 2010).

[17] G.M. Ruotolo, op. cit., p. 72.

sistemi di autoregolamentazione potrebbero fornire ai nuovi servizi nel settore dei media; di bilanciare i punti di forza e di debolezza dei sistemi di autoregolamentazione; di approfondire l'analisi degli eventuali contributi, in particolare attraverso consultazioni pubbliche; di tener conto degli interessi dei terzi, in particolare dei consumatori, nell'esaminare l'autoregolamentazione nei nuovi servizi nel settore dei media»[18].

4. Ambito, scopo e contributo della ricerca†

Muovendo dalla constatazione della crescente militarizzazione dello spazio cibernetico e delle possibili conseguenze degli attacchi cibernetici sulla sicurezza degli Stati, la tesi analizza come il diritto internazionale possa, e debba, regolare l'impiego di strumenti, programmi e tecniche che producono effetti nello spazio cibernetico o tramite esso.

Dopo una breve panoramica dei casi in cui un'operazione cibernetica può costituire un illecito internazionale (Capitolo zero), la tesi ne scompone il processo di attribuzione, soffermandosi sulle ipotesi in cui è possibile ricondurre alla condotta di uno Stato il comportamento di un attore non statuale (Capitolo I). L'indagine prosegue con l'esame delle conseguenze che discendono dall'esecuzione di un'operazione cibernetica internazionalmente illecita (Capitolo II), incluso il caso in cui l'operazione integri gli estremi di un attacco armato (Capitolo III).

Lo scopo della ricerca è determinare se l'attuale quadro normativo, e in particolare il regime sulla responsabilità internazionale degli Stati e lo *jus ad bellum*, sia adeguato a disciplinare lo spazio cibernetico. A tal fine, sarà considerata la reinterpretazione delle norme di diritto internazionale proposta dal Manuale di Tallinn, un lavoro scientifico non legalmente vincolante che identifica il diritto internazionale applicabile allo spazio cibernetico[19].

Il risultato atteso è un compendio degli strumenti giuridici a cui gli Stati possono ricorrere ogniqualvolta siano lesi da un'operazione cibernetica. L'immediata rilevanza della ricerca appare ancora maggiore dal momento che l'esame delle diverse fattispecie

[18] Conclusioni del Consiglio, del 27 settembre 1999, sul ruolo dell'autoregolamentazione alla luce dello sviluppo di nuovi servizi nel settore dei media, in GUCE L 283, del 6 ottobre 1999.

[19] Il Manuale di Tallinn è stato scritto da un gruppo internazionale di esperti, a titolo personale, su invito del Cooperative Cyber Defence Centre of Excellence della NATO. La prima versione del Manuale, pubblicata nel 2013, trattava le operazioni cibernetiche più gravi. La seconda versione del Manuale (2017), a cui si fa riferimento, considera le norme di diritto internazionale regolanti gli incidenti cibernetici che si presentano agli Stati quotidianamente senza superare la soglia dell'uso della forza.

di operazioni cibernetiche fornirà l'occasione per affrontare alcuni degli aspetti più controversi del diritto internazionale contemporaneo, come la legittima difesa preventiva, la legittima difesa in risposta ad attacchi di attori non statuali e le questioni giuridiche connesse con la guerra automatizzata.

[†] Le idee espresse nella presente tesi sono riconducibili interamente all'autore.

CAPITOLO ZERO

La liceità delle operazioni cibernetiche

Nel diritto internazionale non vi è alcun divieto generale a eseguire operazioni cibernetiche. Benché il Manuale di Tallinn non includa nessun riferimento esplicito all'assenza di tale divieto, essa può innanzitutto desumersi dalla sua regola 3:

> A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.

Nonostante l'assenza di un divieto generale a eseguire operazioni cibernetiche, queste, analogamente alle attività di spionaggio, incluso quello cibernetico[20], possono comunque costituire atti ostili[21] o violare specifiche norme di diritto internazionale.

Le operazioni cibernetiche possono, per esempio, violare la sovranità territoriale dello Stato che ne è il bersaglio. Dall'applicazione del principio generale della sovranità statale nello spazio cibernetico[22] consegue infatti che uno Stato ha il diritto esclusivo di esercitare prerogative sovrane sulle infrastrutture e sulle attività cibernetiche localizzate all'interno del suo territorio[23]. La mera penetrazione in un sistema informatico localizzato sul territorio di uno Stato estero[24], o a bordo di una piattaforma, ovunque localizzata, che gode dell'immunità statale[25], sarebbe sufficiente a costituire una violazione della sovranità, indipendentemente dalla natura del sistema infettato. È opportuno sottolineare che il tema dell'estensione della sovranità sulle infrastrutture cibernetiche localizzate nel territorio di uno Stato, contro cui non sembrano registrarsi obiezioni da parte degli Stati, è da

[20] Cfr. regola 32 del Manuale di Tallinn, pag. 168 ss.

[21] Un atto ostile è un comportamento di uno Stato, consistente in un'azione o in un'omissione, che, senza essere contrario al diritto internazionale, arreca uno svantaggio o una scortesia a un altro Stato, e costituisce pertanto una rottura delle relazioni amichevoli. Dal momento che gli atti ostili sono leciti, essi non configurano un diritto a ricorre ad atti illeciti, come le contromisure o l'autotutela. Lo Stato vittima di un atto ostile può adottare ritorsioni, a dimostrazione che può reagire soltanto con altri atti ostili.

[22] Cfr. regola 1 del Manuale di Tallinn, pag. 11 ss.

[23] Cfr. regola 2 del Manuale di Tallinn, pag. 13 ss.

[24] Cfr. regola 4 del Manuale di Tallinn, pag. 17 ss.

[25] Cfr. regola 5 del Manuale di Tallinn, pag. 27 ss.

non confondere, per quanto in parte correlato, con l'importante dibattito, emerso negli ultimi anni, che ruota intorno alla questione di chi controlla Internet[26].

Le operazioni cibernetiche possono inoltre violare alcune norme in materia di diritti umani[27], a partire dal diritto alla privacy. La natura extraterritoriale delle operazioni cibernetiche, per cui i titolari dei diritti violati possono trovarsi al di fuori del territorio dello Stato responsabile, rende tuttavia difficile invocarne la responsabilità.

Dal momento che la maggior parte delle operazioni cibernetiche contro uno Stato sono condotte primariamente ai fini di coercizione, la base principale per determinare l'illiceità di un'operazione è generalmente il principio di non intervento[28]. Lo sviluppo dello spazio cibernetico e la possibilità di colpire infrastrutture critiche, dal cui funzionamento dipendono il mantenimento di servizi vitali per la società e la protezione della popolazione da importanti fattori di rischio, ha infatti offerto nuove modalità d'intervento negli affari interni ed esterni degli Stati.

[26] Sulla governance di Internet, v. *infra* appendice I.

[27] Sul rapporto tra la Rete e i diritti fondamentali, v. *infra* appendice II.

[28] Cfr. regole 66-67 del Manuale di Tallinn, pag. 313 ss.

CAPITOLO I

L’attribuzione delle operazioni cibernetiche

Presupposto necessario per determinare le risposte giuridiche a un’operazione cibernetica internazionalmente illecita è la sua attribuzione, il processo che consiste nell’identificazione degli autori dell’operazione e nella riconducibilità della loro condotta a uno Stato o a un altro soggetto di diritto internazionale. L’attribuzione di un’operazione cibernetica si compone di tre dimensioni distinte: l’attribuzione alla macchina impiegata per la creazione, il lancio o il transito dell’operazione; l’attribuzione alla persona che l’ha eseguita; l’attribuzione all’entità aggregata per conto della quale l’autore può aver agito. L’attribuzione a uno Stato dipende dalle prove fattuali disponibili, e quindi anche, ma non necessariamente, dall’identificazione della macchina o della persona responsabili, a sua volta basata su evidenze forensi. Anche se strettamente connesse l’una con l’altra, le diverse dimensioni dell’attribuzione di un’operazione cibernetica restano indipendenti l’una dall’altra: l’impossibilità d’identificare la macchina da cui è stata lanciata l’operazione non impedisce infatti l’attribuzione di quest’ultima ai suoi responsabili, a cui possono condurre elementi di contesto e intelligence che non rientrano nell’ambito cibernetico.

1. L’attribuzione a una macchina

La macchina da cui è originata un’operazione cibernetica può essere identificata attraverso il numero di serie[29], l’indirizzo MAC[30] o l’indirizzo IP.

Gli indirizzi IP sono la fonte più spesso utilizzata ai fini dell’attribuzione. Sono infatti generalmente distribuiti in blocchi a fornitori di servizi Internet, società, università, governi e altri enti che tengono pubblici registri in cui è possibile rintracciare un indirizzo. L’indirizzo IP identifica ogni dispositivo (host) connesso a Internet o a una rete che usa il suo protocollo. Poiché ogni indirizzo IP appartiene a una specifica rete di computer,

[29] Il numero di serie è un numero unico attribuito dal creatore di un prodotto per identificarlo all’interno di una serie. Il numero di serie di un computer è inciso sul suo hardware e incorporato nel codice che lo fa funzionare.

[30] L’indirizzo MAC (Media Access Control) è un numero di identificazione unico assegnato a ogni scheda di rete dal suo produttore. La scheda di rete è il componente hardware che connette un computer a una rete di computer. Un computer può essere identificato da più di un indirizzo MAC: uno per ogni sua scheda di rete.

ogni computer ha un indirizzo IP per ciascuna rete a cui è connesso. L'intestazione dei pacchetti di dati che transitano su Internet incorpora gli indirizzi IP del mittente e del destinatario.

Le operazioni cibernetiche contro il Democratic National Committee (DNC)[31] offrono un'illustrazione dell'utilizzo dell'indirizzo IP ai fini dell'attribuzione. Gli autori dell'hackeraggio hanno impiegato indirizzi IP che, secondo una relazione del governo statunitense[32], erano già stati utilizzati in precedenti operazioni attribuite a due agenzie d'intelligence russe. Questa circostanza indurrebbe a credere che esse siano responsabili anche delle intrusioni nei sistemi informatici del DNC. È tuttavia importante non escludere la possibilità che gli autori possano aver agito "sotto falsa bandiera" per addossare la colpa a qualcun altro. La pratica di utilizzare un indirizzo IP contraffatto è una delle forme più comuni di *spoofing* e ha due obiettivi principali: impedire la localizzazione della fonte dell'operazione e aggirare un firewall che consente il traffico in ingresso soltanto ai dati provenienti da specifiche reti[33].

Alcune delle tecniche utilizzate per rintracciare la fonte di un'operazione cibernetica implicano la penetrazione di altri sistemi. Qualora questi siano localizzati in un paese straniero, la penetrazione può costituire un'illecita violazione della sovranità territoriale dello Stato estero. L'illiceità della penetrazione può tuttavia essere esclusa sulla base dello stato di necessità[34], laddove la violazione sia l'unico mezzo per proteggere un interesse essenziale dello Stato minacciato dall'operazione cibernetica iniziale e non leda gravemente un interesse essenziale dello Stato nei confronti del quale sussiste l'obbligo del rispetto della sovranità territoriale.

Il processo di attribuzione si complica quando le operazioni si svolgono in più fasi. L'autore di un attacco DDoS (Distributed Denial of Service), per esempio, può usare contro il suo obiettivo vari computer "zombie" riuniti in una *botnet* e controllare quest'ul-

[31] Il 22 luglio 2016, alcuni giorni prima della Democratic National Convention a Philadelphia, WikiLeaks ha pubblicato 19.252 e-mail di dirigenti del DNC, l'organo direttivo del Partito Democratico, dalle quale emerge che la leadership del comitato aveva lavorato per avvantaggiare Hillary Clinton su Bernie Sanders.

[32] Stati Uniti, Department of Homeland Security e Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, 29 dicembre 2016, www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

[33] Cfr. F. Delerue, *Cyber Operations and International Law*, Oxford, 2020, pagg. 67-69.

[34] V. *infra* cap. II.

tima tramite server C&C (Command and Control). Al fine di risalire all'autore dell'attacco è pertanto necessario operare un'attribuzione a cascata, identificando preliminarmente i computer zombie e, a seguire, almeno un server C&C.

Benché non sia un prerequisito per identificare l'autore di un'operazione cibernetica e, tantomeno, lo Stato per conto del quale egli può aver agito, l'identificazione della macchina da cui è stata lanciata l'operazione può essere utile ai seguenti fini[35]:

a. prevenzione, ove l'identificazione, precedendo il lancio dell'operazione, consenta alla potenziale vittima di adattare la protezione del sistema a cui l'attacco è diretto;
b. mitigazione degli effetti dell'operazione, ove l'identificazione sia contestuale al verificarsi dell'operazione;
c. invocazione dell'obbligo di diligenza[36] dello Stato dal cui territorio l'operazione è stata lanciata.

2. L'attribuzione a una persona

Le operazioni cibernetiche, incluse quelle che prevedono un elevato livello di automazione, implicano sempre il coinvolgimento di una persona, anche quando sono sponsorizzate da Stati, che, in quanto enti astratti, devono avvalersi di uomini che agiscano per loro conto.

La persona responsabile di un'operazione può essere individuata grazie all'identificazione della macchina da cui l'operazione è stata lanciata, che può rivelare la località dell'autore. Qualora l'autore sia localizzato in un altro Stato, dove lo Stato vittima non ha giurisdizione[37], questo può richiedere la cooperazione del primo, senza alcuna garanzia che quello dia seguito alla richiesta. Quando, per esempio, l'Estonia ha richiesto alla Federazione Russa di collaborare all'identificazione degli autori degli attacchi DDoS che Tallinn ha subito nel 2007[38], Mosca si è astenuta. L'unico responsabile facilmente identificato e contro il quale è stato possibile raccogliere prove che hanno condotto alla sua condanna è stato Dmitri Galushkevich, che ha agito dal territorio estone.

---

[35] Cfr. F. Delerue, op. cit., pagg. 56-57.

[36] V. *infra*.

[37] Sull'applicazione, all'ambito cibernetico, delle norme di diritto internazionale sulla giurisdizione statale e sull'immunità degli Stati, v. regole 8-13 del Manuale di Tallinn, pag. 51 ss.

[38] Nell'aprile 2007, l'Estonia ha dovuto far fronte a duri scontri di piazza scatenati da una minoranza di origine russa dopo la decisione di rimuovere la statua di bronzo di un soldato sovietico risalente alla Seconda guerra mondiale. Contemporaneamente, il paese ha sperimentato molteplici operazioni cibernetiche,

Informazioni sull'identità della persona responsabile possono essere fornite anche dal modo in cui l'operazione è stata eseguita, come illustra l'esempio di BadRabbit, un ransomware identificato per la prima volta il 24 ottobre 2017 che si presentava come un aggiornamento di Adobe Flash Player. L'analisi del suo modus operandi suggerirebbe che i suoi autori siano gli stessi di NotPetya[39], che più Stati (Australia[40], Nuova Zelanda[41], Regno Unito[42]) hanno attribuito alla Federazione Russa, la quale risulta tra le principali vittime di BadRabbit. Tre ipotesi alternative possono spiegare quest'apparente contraddizione[43]:

a. i responsabili di BadRabbit, che non hanno agito per conto della Federazione Russia, hanno riutilizzato gli strumenti che NotPetya aveva reso di pubblico dominio;
b. il gruppo Sandworm (anche noto come TeleBots e BlackEnergy), autore di NotPetya e presumibilmente di BadRabbit, ha agito per conto della Federazione Russia nel tentativo di confondere le prove che le attribuivano la responsabilità di NotPetya;
c. i responsabili di BadRabbit hanno fatto ricorso agli stessi strumenti utilizzati dai servizi di intelligence russi al fine di sviare le indagini e attribuire falsamente la responsabilità delle operazioni alla Federazione Russa[44].

in particolare attacchi DDoS su larga scala ai siti web e ai server di enti pubblici e privati. Il governo estone ha accusato la Federazione Russa di essere la responsabile degli attacchi; la Federazione Russa ha negato qualsiasi coinvolgimento.

[39] Quando BadRabbit era avviato sul computer di una vittima, la sua componente "*worm*" tentava di propagarsi impiegando EternalRomance, un *exploit* che si ritiene sia stato sviluppato dalla National Security Agency prima di essere stato rubato e poi diffuso online. EternalRomance era stato precedentemente utilizzato anche da NotPetya, il malware che a partire dal 27 giugno 2017 ha colpito principalmente le reti e i sistemi ucraini.

[40] Australia, Minister for Foreign Affairs, *Attribution of a pattern of malicious cyber activity to Russia*, 4 ottobre 2018, www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-pattern-malicious-cyber-activity-russia.

[41] Nuova Zelanda, Government Communications Security Bureau, *Malicious cyber activity attributed to Russia*, 4 ottobre 2018, www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/.

[42] Regno Unito, National Cyber Security Centre, *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, 4 ottobre 2018, www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

[43] Cfr. F. Delerue, op. cit., pagg.73-76.

[44] In proposito occorre ricordare che Vault 7, la serie di documenti che WikiLeaks ha cominciato a pubblicare a partire dal 7 marzo 2012, ha svelato che UMBRAGE, un gruppo della Remote Devices Branch della CIA, si sarebbe appropriato delle tecniche cibernetiche utilizzate da altri Stati. Con UMBRRAGE, la CIA potrebbe non soltanto aumentare il numero dei tipi di attacchi, ma anche sviare le indagini mascherando gli attacchi sotto le apparenze del lavoro di un altro gruppo.

Gli autori di BadRabbit e NotPetya sono ritenuti responsabili anche delle operazioni cibernetiche che nel 2015 hanno sabotato la rete elettrica in Ucraina, provocando un blackout di un'ora per alcune migliaia di utenti a Kiev[45].

La rilevanza delle informazioni tecniche nel processo di attribuzione è stata confermata anche nel caso di Stuxnet[46]. Il percorso del suo file contiene il termine "*myrtus*", che potrebbe intendersi come riferito a Esther, la regina ebrea originariamente chiamata Hadassah ("mirto" in ebraico). Questa informazione, combinata con il numero 19790509, che appare nel codice di Stuxnet e può corrispondere al 9 maggio 1979 (giorno in cui Habib Elghanian è stato fucilato[47]), suggerirebbe il coinvolgimento di sviluppatori ebraici o israeliani, o dello stesso Stato di Israele. Il fatto che siano state impiegate due piattaforme diverse per la sua creazione[48] indicherebbe che ci abbiano lavorato due diversi gruppi di sviluppatori, corroborando l'ipotesi che Stuxnet sia stato sviluppato inizialmente dagli Stati Uniti e successivamente congiuntamente a Israele.

In altri casi, infine, la nazionalità dell'autore di un'operazione cibernetica è stata tradita dalle impostazioni del layout della sua tastiera[49] o dal suo nome utente[50].

Se l'identificazione delle persone coinvolte nell'esecuzione di un'operazione cibernetica consente di analizzare il loro rapporto con il presunto Stato responsabile, essa

[45] I sistemi di tre società di distribuzione sono stati infettati dalla terza versione di BlackEnergy, il malware che è diventato il marchio di fabbrica del gruppo Sandworm. BlackEnergy si sarebbe introdotto nei sistemi delle stazioni elettriche attraverso un file di Microsoft Office, che all'apertura ha permesso la diffusione dell'infezione e la successiva acquisizione delle credenziali per accedere ai sistemi SCADA (Supervisory Control And Data Acquisition).

[46] Stuxnet ha infettato il sistema informatico dell'impianto nucleare di Natanz in Iran e portato fuori giri le sue turbine fino alla loro distruzione.

[47] Imprenditore e filantropo ebreo di spicco, Habib Elghanian è stato il primo ebreo e il primo civile giustiziato dal governo iraniano insediatosi dopo la rivoluzione del 1979.

[48] La prima versione di Stuxnet, che colpì le valvole delle centrifughe della centrale, fu sviluppata sulla piattaforma Flame, mentre la versione successiva, che modificò la velocità delle centrifughe, fu sviluppata sulla piattaforma Tilde-d.

[49] L'indagine di Mandiant ha rivelato che gli autori di alcune attività di spionaggio cibernetico apparentemente condotte da computer e server localizzati in paesi diversi utilizzavano tastiere cinesi. Questa informazione, insieme alla scoperta che la maggior parte degli attacchi originavano da indirizzi IP localizzati a Shangai, è un forte indizio che la lingua materna degli autori sia il cinese.

[50] L'indagine condotta dal Communications Security Establishment del Canada su un malware scoperto nel 2009, inizialmente denominato "Snowglobe", ha rivelato che il suo creatore gli aveva dato il nome in codice "Babar" e che il nome utente dello sviluppatore era "titi". Il fatto che Babar sia il personaggio di un cartone animato francese e che "titi" sia il diminutivo di Thierry suggeriscono che il malware sia stato creato da un cittadino francese.

non è tuttavia un prerequisito per l'identificazione di quest'ultimo, che potrebbe riconoscere la propria responsabilità senza rivelare i nomi degli agenti che hanno operato per suo conto[51].

2.1. Le misure restrittive nei confronti di persone fisiche e giuridiche

In conseguenza delle costanti preoccupazioni per le minacce cibernetiche che provengono da attori non statuali, a livello nazionale e regionale sono stati elaborati degli strumenti volti a scoraggiare e rispondere in maniera efficace agli attacchi informatici che non siano direttamente riconducibili a uno Stato, e non integrino pertanto gli estremi di un illecito internazionale.

Nel maggio 2019, il legislatore europeo ha adottato la decisione (PESC) 2019/797 e il conseguente regolamento (UE) 2019/796, entrambi concernenti le misure restrittive contro gli attacchi informatici che costituiscano una minaccia esterna per l'Unione o i suoi Stati membri. Il regolamento si applica agli attacchi cibernetici con effetti significativi, inclusi i tentati attacchi cibernetici con effetti potenzialmente significativi, che (a) provengono o sono sferrati dall'esterno dell'Unione, (b) impiegano infrastrutture esterne all'Unione, (c) sono compiuti da una persona fisica o giuridica, un'entità o un organismo stabiliti o operanti al di fuori dell'Unione, o (d) sono commessi con il sostegno, sotto la direzione o sotto il controllo di una persona fisica o giuridica, un'entità o un organismo operanti al di fuori dell'Unione. Gli attacchi comprendono quelli che incidono su sistemi d'informazione relativi, tra l'altro, a infrastrutture critiche, servizi necessari per il mantenimento di attività sociali e/o economiche fondamentali, funzioni statali essenziali, conservazione o trattamento di informazioni classificate, o squadre di pronto intervento governative. I fattori che determinano se un attacco ha effetti significativi comprendono (a) portata, entità, impatto o gravità delle turbative causate, (b) numero di persone fisiche o giuridiche, entità o organismi interessati, (c) numero di Stati membri interessati, (d) importo della perdita economica causata, (e) vantaggio economico ottenuto dall'autore dell'atto per se stesso o per terzi, (f) quantità o natura dei dati oggetto del furto o entità delle violazioni dei dati, (g) natura dei dati sensibili sotto il profilo commerciale cui si è avuto accesso. Il regolamento prevede il congelamento di tutti i fondi e delle risorse economiche appartenenti, possedute, detenute o controllate dalle persone fisiche o giuridiche,

[51] Quando l'Iran ha sostenuto che il corpo speciale dell'esercito iraniano per la guerra elettronica aveva hackerato un RQ-170 Sentinel statunitense ha tenuto i nomi per sé.

entità o organismi che siano responsabili di questi attacchi o tentati attacchi, così come delle persone fisiche o giuridiche, entità o organismi che abbiano sostenuto o siano comunque coinvolti nella commissione o nel tentativo di commissione degli attacchi. Ove ritenuto necessario ai fini del conseguimento degli obiettivi della politica estera e di sicurezza comune, è prevista la possibilità di applicare misure restrittive ai sensi del regolamento anche in risposta ad attacchi informatici con effetti significativi nei confronti di Stati terzi od organizzazioni internazionali.

Nella prassi, oltre alle misure a contenuto sanzionatorio, si riscontrano anche misure di tipo preventivo, come quelle con cui l'Australia e gli Stati Uniti[52], per timore di spionaggio, hanno vietato a fornitori cinesi di partecipare a gare d'appalto per l'acquisto di servizi informatici e tecnologici[53].

3. L'attribuzione a uno Stato

Affinché un'operazione cibernetica di cui è vittima uno Stato possa integrare gli estremi di un illecito internazionale[54], consentendo l'invocazione della responsabilità internazionale e producendo le conseguenze giuridiche che questa comporta[55], l'operazione deve essere attribuita a uno Stato o un altro soggetto di diritto internazionale[56].

La disciplina generale della responsabilità internazionale degli Stati è posta da regole di diritto internazionale consuetudinario di cui la Commissione del diritto internazionale delle Nazioni Unite ha curato la codificazione, sfociata nell'adozione, nel 2001,

[52] Stati Uniti, House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 8 ottobre 2012, republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[53] Sulle implicazioni commerciali delle misure di sicurezza, v. Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, in *Journal of International Economic Law*, 2015, pag. 449 ss.

[54] Cfr. regola 14 del Manuale di Tallinn, pag. 85 ss.

[55] Vedi *infra* cap. II.

[56] Sebbene questa ricerca consideri solo la responsabilità dello Stato, una responsabilità per un atto internazionalmente illecito può insorgere in capo a ogni soggetto di diritto internazionale che violi un obbligo internazionale. La questione della responsabilità delle organizzazioni internazionali per atti internazionalmente illeciti è stata oggetto di studio specifico da parte della Commissione del diritto internazionale, sfociato nell'adozione di un progetto di articoli nel 2011. La regola 31 del Manuale di Tallinn (pag. 157 ss.) enuncia il principio generale della responsabilità internazionale delle organizzazioni internazionali per operazioni cibernetiche internazionalmente illecite.

di un progetto di articoli di cui l'Assemblea generale si è limitata a prendere nota, sottoponendoli all'attenzione dei governi[57].

3.1. L'attribuzione delle operazioni condotte dagli organi dello Stato

In linea di principio, può essere riferito allo Stato solo il comportamento dei suoi organi, ossia di quelle persone e di quegli enti attraverso i quali lo Stato si organizza e agisce[58]. Rientrano tra gli organi dello Stato, oltre a quelli de jure, anche tutti gli enti e le persone che agiscono in totale dipendenza dallo Stato pur non essendo formalmente suoi organi (organi de facto)[59].

Allo stesso tempo può essere attribuita allo Stato il comportamento della persona o dell'ente che non può essere ritenuto organo dello Stato, ma che tuttavia è abilitato dal diritto interno dello Stato a esercitare prerogative dell'autorità di governo (enti parastatali)[60].

Coerentemente con quanto precede, la regola 15 del Manuale di Tallinn dispone che «le operazioni cibernetiche condotte dagli organi di uno Stato, o da persone o enti abilitati dal diritto nazionale a esercitare prerogative dell'autorità di governo, sono attribuibili a quello Stato».

La nozione di "organo dello Stato" di cui all'art. 4 del progetto della CDI è molto ampia, ricomprendendo «qualsiasi persona o ente che rivesta tale posizione secondo il diritto interno dello Stato», indipendentemente dalle funzioni esercitate (legislative, esecutive, giudiziarie o altre), dalla sua posizione nell'organizzazione dello Stato e della sua natura (organo del governo centrale o di un'unità territoriale dello Stato). Le operazioni cibernetiche condotte dagli organi militari e dalle agenzie responsabili della sicurezza sono pertanto considerate come un atto dello Stato[61].

---

[57] Risoluzione 56/83 dell'Assemblea generale, *Responsibility of States for internationally wrongful acts*, A/RES/56/83 (28 gennaio 2012).

[58] Cfr. art. 4 del progetto della CDI, ritenuto corrispondente al diritto internazionale consuetudinario dalla Corte internazionale di giustizia nella sentenza del 26 febbraio 2007 nel caso sull'*Applicazione della Convenzione per la prevenzione e la repressione del crimine di genocidio* (*Bosnia-Erzegovina* c. *Serbia e Montenegro*).

[59] Cfr. C. Focarelli, *Diritto internazionale*, 2021, cap. VIII, sez. I.

[60] Cfr. art. 5 del progetto della CDI.

[61] Il crescente interesse degli Stati per lo spazio cibernetico è stato accompagnato non soltanto da un maggiore coinvolgimento dell'esercito e delle esistenti agenzie nazionali di sicurezza e intelligence nei sistemi di difesa e offesa cibernetiche, ma anche dallo sviluppo di agenzie e organi specificamente incaricati della sicurezza cibernetica, quali lo U.S. Cyber Command, la Küberkaitseüksusla (l'unità cibernetica delle forze paramilitari estoni) e l'agenzia francese per la sicurezza dei sistemi d'informazione.

Il principale esempio di ente che esercita prerogative dell'attività di governo è costituito da una società privata che conduca operazioni cibernetiche offensive contro uno Stato per conto di un altro. Affinché sia attribuibile allo Stato, il comportamento della società deve costituire un esercizio di funzioni sovrane che lo Stato le abbia esplicitamente conferito.

Il comportamento di un organo di uno Stato o di una persona o di un ente abilitati ad esercitare prerogative dell'autorità di governo sarà considerato come un atto dello Stato ai sensi del diritto internazionale, se quell'organo, persona o ente agisce in tale qualità, anche se eccede la propria competenza o contravviene ad istruzioni[62]. Ne segue che, qualora una società privata incaricata di proteggere l'infrastruttura cibernetica governativa di uno Stato limitandosi all'impiego di misure difensive reagisca a un attacco adottando a sua volta delle misure offensive, la sua condotta sarebbe ascrivibile a quello Stato[63].

3.2. L'attribuzione delle operazioni condotte dagli organi di un altro Stato

Il comportamento di un organo di uno Stato fa sorgere la responsabilità di un altro Stato allorché venga posto a sua disposizione, esclusivamente per la condotta posta in essere nell'esercizio di prerogative dell'autorità di governo dello Stato a disposizione del quale esso è messo[64].

Nello spazio cibernetico, l'ipotesi più plausibile è la situazione in cui uno Stato metta delle unità cibernetiche a disposizione di un altro Stato per aiutare quest'ultimo a contrastare un'ondata di attacchi informatici.

3.3. L'attribuzione delle operazioni condotte da attori non statuali

Salvo talune eccezioni, il comportamento di privati in quanto tali non può essere considerato come un atto dello Stato, che può tuttavia essere ritenuto responsabile per non aver preso le misure necessarie per prevenire o punire il fatto illecito commesso dai privati.

[62] Cfr. art. 7 del progetto della CDI.

[63] Cfr. commento alla regola 15 del Manuale di Tallinn, par. 8, pag. 89.

[64] Cfr. art. 6 del progetto della CDI.

Una responsabilità diretta sorge in primo luogo allorché lo Stato, approvando a posteriori il comportamento dei privati, lo adotti come proprio[65]. Ad oggi, nessuna operazione cibernetica condotta da un attore non statuale è stata riconosciuta o adottata a posteriori da uno Stato. Stuxnet e le operazioni del 2007 contro l'Estonia offrono tuttavia degli spunti di riflessione a questo riguardo.

Benché l'origine di Stuxnet non sia ancora stata confermata, due circostanze sono state ritenute indicative delle fonti del malware: nel 2011, riferendosi ai problemi che gli iraniani stavano avendo con le centrifughe della centrale, il coordinatore della Casa Bianca per il controllo degli armamenti e le armi di distruzione di massa, Gary Samore, disse che gli Stati Uniti e i loro alleati stavano facendo tutto quanto in loro potere per complicare la loro situazione; nello stesso anno, alla festa di pensionamento del tenente generale israeliano Gabi Ashkenazi, l'ex capo di stato maggiore delle forze di difesa israeliane, fu proiettato un video che mostrava i suoi successi operativi, incluso un riferimento a Stuxnet. Benché queste due circostanze siano generalmente invocate a sostegno della tesi che attribuisce la paternità di Stuxnet agli Stati Uniti e a Israele, esse non costituiscono un riconoscimento o un'adozione delle operazioni cibernetiche ai sensi del diritto internazionale: da una parte, la dichiarazione del funzionario statunitense è troppo vaga; dall'altra, sembra impossibile attribuire il video al governo israeliano[66].

Dopo le operazioni cibernetiche del 2007 contro l'Estonia, il governo estone ha accusato degli attacchi la Federazione Russa, che non ha mai riconosciuto il proprio coinvolgimento o avallato le operazioni. Tuttavia, Konstantin Goloskokov, un membro del gruppo giovanile russo Nashi, ammise di essere coinvolto nel lancio degli attacchi, e Sergei Markov, un membro del parlamento russo, confermò che il suo assistente aveva condotto le operazioni. Tuttavia, dal momento che Goloskokov e Markov non attribuiscono le operazioni direttamente alla Federazione Russa, tanto più che non hanno la capacità di parlare in nome dello Stato, le loro dichiarazioni non costituiscono un avallo da parte del governo russo[67].

L'attribuzione allo Stato del comportamento di persone che non sono formalmente inquadrabili nella sua organizzazione avviene, in secondo luogo, quando il comportamento contrario all'obbligo internazionale è stato adottato sulla base di istruzioni oppure

[65] Cfr. art. 11 del progetto della CDI.

[66] Cfr. F. Delerue, op. cit., pagg. 154-155.

[67] Cfr. F. Delerue, op. cit., pagg. 155-156.

sotto la direzione o il controllo dello Stato[68]. La Corte internazionale di giustizia (CIG), nella sentenza del 27 giugno 1986 nel caso delle *Attività militari e paramilitari degli Stati Uniti in Nicaragua e contro il Nicaragua* (*Nicaragua* c. *Stati Uniti*), ha ritenuto che occorresse la prova di un "controllo effettivo", da intendersi come controllo sui singoli atti compiuti dai contras. Diversamente, la Camera d'appello del Tribunale per i crimini commessi nella ex Jugoslavia (TPIJ), nella sentenza del 15 luglio 1999 nel caso *Tadić*, ha applicato il criterio del "controllo generale", che rileverebbe nei casi in cui l'illecito sia compiuto da un gruppo organizzato o strutturato gerarchicamente; viceversa, nei casi in cui l'illecito sia compiuto da individui o da gruppi non organizzati, si applicherebbe il criterio del controllo effettivo sui singoli atti. La CIG, nella sentenza del 26 febbraio 2007 nel caso sull'*Applicazione della Convenzione per la prevenzione e la repressione del crimine di genocidio* (*Bosnia-Erzegovina* c. *Serbia e Montenegro*), ha riaffermato il criterio del controllo effettivo, osservando che le conclusioni a cui era pervenuta la TPIJ dipendevano dalla diversità della questione giuridica sottoposta al suo esame: rilevare il carattere internazionale o meno del conflitto bosniaco al fine di stabilire l'applicabilità delle norme previste dalle Convenzioni di Ginevra del 1949 per i conflitti internazionali, senza considerare la questione della responsabilità statale.

La regola 17 del Manuale di Tallinn, nel riprendere il testo dell'art 8 del progetto adottato dalla CDI, lascerebbe impregiudicata la nozione di "controllo" a cui fare riferimento per l'attribuzione di un'operazione cibernetica.

Il criterio del controllo effettivo richiesto dalla CIG potrebbe costituire una soglia troppo elevata per essere applicabile all'utilizzo delle nuove tecnologie. Internet offre infatti a uno Stato la possibilità di coordinare facilmente le azioni di un gruppo di attori non statuali senza necessariamente avere un elevato grado di controllo su di loro.

Gli autori delle operazioni cibernetiche del 2007 contro l'Estonia, perlomeno quelle che si sono svolte dal 27 al 29 aprile e che sono consistite principalmente in attacchi DoS (Denial of Service) contro siti web del governo e di media, coordinati attraverso forum e chat online, non sembrano costituire un singolo gruppo organizzato, bensì sembrano essere per la stragrande maggioranza singoli individui o gruppi non organizzati che hanno deciso di condurre delle operazioni a sostegno della minoranza russa in Estonia. Se così fosse, sarebbe difficile affermare che qualcuno, e a fortiori uno Stato, potesse esercitare un controllo effettivo su tutte le operazioni. Né potrebbe essere soddisfatto il

[68] Cfr. art. 8 del progetto della CDI.

criterio del controllo generale applicato dal TPIJ, sulla base dell'assunto che gli autori delle operazioni non costituivano un gruppo organizzato. Anche nel caso in cui alcuni degli autori appartenessero a gruppi organizzati, il grado di controllo o direzione che potrebbe aver esercitato uno Stato, se effettivamente fosse responsabile di alcuni forum e chat utilizzati per incitare le persone a condurre queste operazioni e avesse dato delle indicazioni su come eseguirle, non raggiungerebbe la soglia prescritta dal criterio del controllo generale[69].

Analogamente, il criterio del controllo effettivo appare troppo restrittivo nel caso di società militari e di sicurezza private che uno Stato abbia reclutato per condurre delle operazioni cibernetiche e che non rientrino nelle fattispecie di organi di fatto o di enti abilitati a esercitare prerogative dell'autorità di governo. Qualora uno Stato si limiti a indicare ad attori privati i risultati da conseguire e lasci alla loro discrezione la decisione sul tipo di operazione da condurre, il loro comportamento potrà essere considerato come un atto dello Stato solo in applicazione del criterio del controllo generale.

Allo Stato possono essere inoltre attribuiti il comportamento di privati che agiscano in sua sostituzione, quando le autorità ufficiali sono venute meno e in circostanze tali da richiedere l'esercizio delle loro prerogative[70], e il comportamento di un movimento insurrezionale, se e quando questo assume le funzioni di nuovo governo dello Stato[71]. La circostanza che i comportamenti di cui trattasi si presentino come operazioni cibernetiche non modificherebbe l'esito dell'attribuzione.

Ove i comportamenti degli autori di un'operazione cibernetica non possano essere considerati come imputabili a uno Stato, su di esso gravano nondimeno gli obblighi di prevenzione atti a impedire che il proprio territorio e le proprie infrastrutture siano utilizzati in maniera ostile nei confronti di altri Stati[72]. L'operatività dell'obbligo di diligenza nel dominio cibernetico sarebbe tuttavia limitata, innanzitutto, dalla difficoltà con la quale uno Stato viene effettivamente a conoscenza delle condotte che si stanno verificando all'interno del proprio territorio[73]. L'obbligo di diligenza non impone infatti a uno Stato

[69] Cfr. F. Delerue, op. cit., pagg. 146-149.

[70] Cfr. art. 9 del progetto della CDI.

[71] Cfr. art. 10 del progetto della CDI.

[72] Al c.d. principio della dovuta diligenza ha fatto riferimento la Corte internazionale di giustizia nella sentenza del 9 aprile 1949 nel caso dello *Stretto di Corfù* (*Albania* c. *Regno Unito*). Sull'adattamento del principio della dovuta diligenza al dominio cibernetico, v. regole 6-7 del Manuale di Tallinn, pag. 31 ss.

[73] Cfr. D. Mandrioli, *Alcune riflessioni sul cyber attack subito dall'Australia: oltre i problemi di attribuzione dell'illecito,* in *Rivista di diritto internazionale,* 2021, pagg. 191-192.

l'adozione di misure che siano al di sopra dei propri mezzi o altrimenti irragionevoli[74]. La condotta preventiva richiesta allo Stato non può inoltre tradursi in condotte di sorveglianza di massa suscettibili di violare i diritti umani posti a tutela della privacy degli individui[75]. Nonostante questi limiti, l'obbligo di diligenza offre un idoneo standard di attribuzione che può colmare le carenze, nell'attuale disciplina generale della responsabilità internazionale, derivanti dall'anonimità e dall'accessibilità che caratterizzano il dominico cibernetico[76].

3.4. La responsabilità per le operazioni condotte da altri Stati

Se uno Stato è generalmente responsabile solo per le azioni a esso attribuibili, possono darsi casi in cui insorge una responsabilità dello Stato in relazione alle azioni di un altro.

Una responsabilità può sorgere innanzitutto per lo Stato che aiuti o assista un altro Stato nella commissione di un illecito[77] o ne diriga e controlli il comportamento nella commissione di quell'atto[78], se agisce con la consapevolezza delle circostanze dell'illecito, quando quell'atto sarebbe illecito se da lui direttamente commesso. Pertanto, se uno

[74] Cfr. M.N. Schmitt, *In Defense of Due Diligence in Cyberspace*, in *The Yale Law Journal Forum*, 2015, pag. 68 ss.

[75] La giurisprudenza della Corte europea dei diritti dell'uomo offre interessanti spunti sulla violazione del diritto alla vita privata, la cui tutela è apparsa sempre più a rischio con la rivoluzione digitale e l'emergere di scandali come quello relativo a Cambridge Analytica, azienda di consulenza che avrebbe usato impropriamente un'enorme quantità di dati prelevati da Facebook. Una delle più recenti pronunce della Corte in merito è quella sul caso *Big Brother Watch e altri* c. *Regno Unito*. I ricorrenti ritenevano che le loro comunicazioni elettroniche potessero essere state intercettate dai servizi di intelligence del Regno Unito, nell'ambito dei programmi di sorveglianza di massa di cui Edward Snowden, ex collaboratore della National Security Agency statunitense, aveva rivelato l'esistenza. Secondo la Corte, alla luce della moltitudine di minacce che oggi gli Stati devono fronteggiare, un regime d'intercettazioni di massa non violerebbe di per sé la CEDU, il cui art. 8 stabilisce che non può esservi ingerenza di un'autorità pubblica nell'esercizio del diritto al rispetto della propria vita privata. Tuttavia, un tale regime deve essere soggetto a salvaguardie *end-to-end*, nel senso che, a livello nazionale, per ogni fase del processo dovrebbe essere fatta una valutazione della necessità e della proporzionalità delle misure adottate; che le intercettazioni di massa dovrebbero essere preliminarmente soggette a un'autorizzazione indipendente, quando l'oggetto e lo scopo dell'operazione sono stati definiti; e che l'operazione dovrebbe essere soggetta a supervisione e a valutazione indipendente *ex post*. Con riferimento al regime d'intercettazioni in vigore nel Regno Unito al tempo dei fatti, la Corte ha riscontrato le seguenti carenze: le intercettazioni erano state autorizzate dal Segretario di Stato, e non da un organismo indipendente dall'esecutivo; nella domanda per un mandato non erano state incluse le categorie di termini di ricerca che definivano i tipi di comunicazioni che sarebbero diventati passibili di indagine; e che i termini di ricerca collegati a un individuo non erano stati preliminarmente soggetti ad autorizzazione interna. Alla luce di ciò, la Corte ha riconosciuto all'unanimità che il regime d'intercettazione violasse l'art. 8 della CEDU.

[76] Cfr. L. Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, in *International and Comparative Law Quarterly*, 2018, pag. 643 ss.

[77] Cfr. art. 16 del progetto della CDI e regola 18, lett. a), del Manuale di Tallinn, pag. 100 ss.

[78] Cfr. art. 17 del progetto della CDI e regola 18, lett. b), del Manuale di Tallinn, pag. 100 ss.

Stato consente a un altro Stato di utilizzare la sua infrastruttura cibernetica, come un Internet provider sotto il suo controllo, senza sapere che sarà utilizzata per condurre un'operazione cibernetica illecita, il primo Stato non sarà chiamato a risponderne. Nel caso in cui uno Stato assista un altro Stato contribuendo al finanziamento dell'operazione cibernetica illecita, il primo Stato sarà responsabile solo nella misura in cui il suo finanziamento ha contributo all'operazione, e non per l'intera operazione, diversamente dal caso della direttiva nella sua commissione.

In secondo luogo, uno Stato è responsabile per l'illecito che ha costretto un altro Stato a compiere[79]. Alla responsabilità dello Stato che esercita la coercizione si accompagna l'esclusione della responsabilità in capo allo Stato sotto la coercizione. Se, per esempio, uno Stato minaccia di adottare delle sanzioni economiche contro un altro Stato, qualora questo non conduca un'operazione cibernetica illecita, come l'alterazione dei dati critici di uno Stato terzo conservati sui server localizzati sul territorio del secondo Stato, solo il primo Stato dovrà affrontare le conseguenze derivanti dall'illecito.

* * *

I casi analizzati nel corso del capitolo hanno evidenziato il primo limite dell'applicazione del diritto internazionale allo spazio cibernetico: i criteri che la CIG e il TPIJ hanno sviluppato per attribuire a uno Stato i comportamenti di attori non statuali non considerano il fatto che le nuove tecnologie e in particolare Internet offrono vari modi per coordinare le operazioni cibernetiche senza un alto livello di organizzazione, creando una situazione in cui la disciplina sulla responsabilità internazionale lascia le vittime impotenti. Un tale scenario invita a riflettere sull'opportunità di abbassare il grado di direzione o controllo richiesto per ricondurre a uno Stato la condotta di soggetti estranei alla sua organizzazione, senza tuttavia allentare i criteri di attribuzione fino al punto di dar luogo a malintesi e, di conseguenza, destabilizzare la pace e la sicurezza cibernetiche internazionali.

[79] Cfr. art. 18 del progetto della CDI e regola 18, lett. c), del Manuale di Tallinn, pag. 100 ss.

CAPITOLO II

La responsabilità dello Stato per operazioni cibernetiche internazionalmente illecite

Verificato che un'operazione cibernetica può essere attribuita a uno Stato ai sensi del diritto internazionale e costituisce una violazione di un suo obbligo internazionale, si pone il problema di stabilire quali conseguenze l'operazione illecita comporti. Prima di concentrarsi sulle conseguenze giuridiche in capo al responsabile dell'illecito e sugli strumenti per costringerlo ad adempiere ai propri obblighi, è necessario analizzare in quali circostanze l'illeceità possa essere preclusa o attenuata.

1. Le cause di esclusione dell'illiceità

Il contrasto con una norma di diritto internazionale integra l'elemento oggettivo dell'illecito a condizione che non sussistano circostanze che escludano la responsabilità internazionale. Gli effetti che discendono dal ricorrere di tali circostanze sono circoscritti: in primo luogo, come stabilito anche dalla CIG nella sentenza del 25 settembre 1997 nel caso del *Progetto Gabčíkovo-Nagymaros* (*Ungheria* c. *Slovacchia*), le circostanze di esclusione dell'illiceità non estinguono l'obbligo internazionale violato[80]; in secondo luogo, il ricorrere delle cause di giustificazione non esclude l'eventuale sussistenza di un obbligo di reintegrazione patrimoniale per il danno comunque causato[81]. L'unico limite all'applicazione delle cause di esclusione dell'illiceità è rappresentato dal rispetto di norme imperative[82], quale, per esempio, il divieto di commettere genocidio. Il progetto di articoli sulla responsabilità degli Stati elenca sei cause di esclusione dell'illiceità: consenso, legittima difesa[83], contromisure[84], forza maggiore, estremo pericolo, necessità.

[80] Cfr. art. 27, lett. a), del progetto della CDI.

[81] Cfr. art. 27, lett. b), del progetto della CDI.

[82] Cfr. art. 26 del progetto della CDI.

[83] V. *infra* cap. III.

[84] V. *infra*.

1.1. Consenso

Il consenso è un atto unilaterale, prestato in forma orale o scritta, con il quale uno Stato autorizza un altro Stato a tenere un comportamento che sarebbe in contrasto con un obbligo internazionale nei suoi confronti. Affinché il consenso esplichi i propri effetti, l'atto altrimenti illecito deve rimanere nei limiti dell'autorizzazione[85], che deve essere espressa precedentemente, o quantomeno contemporaneamente, a tale atto da un ente idoneo a impegnare lo Stato e non essere affetta da vizi della volontà. Qualora legittimamente prestato in un momento successivo al fatto illecito, il consenso costituisce una mera rinuncia dello Stato leso al suo diritto di ottenere una riparazione[86].

Il passaggio nello spazio cibernetico non mette in dubbio la possibilità di ricorrere al consenso quale causa di esclusione dell'illiceità e subordinarne l'effetto scriminante alle stesse condizioni a cui è subordinato nel mondo reale. Ne segue che il consenso dato dalla Georgia alle operazioni che i suoi partner hanno condotto sui server localizzati sul suo territorio, per combattere gli attacchi cibernetici di cui Tbilisi è stata vittima durante il conflitto russo-georgiano nel 2008, ha precluso l'insorgere della responsabilità per atti che altrimenti avrebbero costituito una violazione della sua sovranità[87].

1.2. Forza maggiore e caso fortuito

Ricorre una situazione di forza maggiore, o caso fortuito, allorché si verifica una forza irresistibile o un avvenimento imprevedibile, fuori dal controllo di uno Stato, che rende materialmente impossibile nelle circostanze agire in conformità a quanto richiesto da un obbligo a cui lo Stato è soggetto. Nell'ipotesi del caso fortuito, a differenza dell'ipotesi della forza maggiore, la violazione del diritto internazionale è inconsapevole. La forza maggiore e il caso fortuito si distinguono dai casi dell'estremo pericolo e dello stato di necessità[88], che implicano la presenza di un elemento intenzionale. La forza maggiore e il caso fortuito non operano quando:

> (a) la situazione di forza maggiore [e caso fortuito] è da attribuirsi, sia in via esclusiva che in combinazione con altri fattori, alla condotta dello Stato che la invoca; o

[85] Cfr. art. 20 del progetto della CDI.

[86] V. *infra*.

[87] Cfr. F. Delerue, op. cit., pag. 346.

[88] V. *infra*.

(b) lo Stato ha accettato il rischio che quella situazione poteva verificarsi[89].

Dal momento che la forza maggiore non può essere invocata da uno Stato in una situazione che è conseguenza della sua stessa condotta, tale causa di esclusione non opererebbe quando un virus si diffonde in maniera incontrollata, infettando sistemi che non rientrano tra quelli a cui era diretto in origine.

Più in generale, l'invocazione della forza maggiore quale causa di esclusione dell'illiceità di un'operazione cibernetica appare altamente improbabile, essendo inverosimile che questa sia dovuta a una condotta non implicante nessuna libertà di scelta[90].

1.3. Estremo pericolo

L'illiceità di un comportamento non conforme al diritto internazionale è altresì esclusa allorché costituisca, in una situazione di estremo pericolo, l'unico modo ragionevole di salvare la vita dell'autore o quella delle persone che questo ha il compito di proteggere[91]. A differenza del caso della forza maggiore, la persona che agisce in una situazione di estremo pericolo, pur potendo evitare il comportamento illecito, decide di violare una norma di diritto internazionale, quale male minore rispetto alla perdita di vite umane. La possibilità d'invocare una situazione di estremo pericolo quale causa di esclusione dell'illiceità è tuttavia esclusa nel caso in cui essa sia stata creata dallo Stato autore dell'illecito o se il comportamento tenuto è tale da causare un pericolo comparabile o maggiore rispetto a quello che si cerca di evitare[92].

Benché non si possa escludere l'applicazione di questa causa di esclusione dell'illiceità nello spazio cibernetico, sembra improbabile che un'operazione cibernetica possa costituire il mezzo più ragionevole per salvare la vita dell'autore dell'operazione e delle persone affidate alle sue cure[93].

[89] Art. 23, paragrafo 2, del progetto della CDI.

[90] Cfr. F. Delerue, op. cit., pag. 347.

[91] Cfr. art. 24, paragrafo 1, del progetto della CDI.

[92] Cfr. art. 24, paragrafo 2, del progetto della CDI.

[93] Cfr. F. Delerue, op. cit., pag. 348.

1.4. Stato di necessità

Un'ultima esimente della responsabilità internazionale è rappresentata dallo stato di necessità, che può essere invocato soltanto quando l'adozione del comportamento astrattamente illecito è l'unico modo per salvaguardare un interesse essenziale dello Stato nei confronti di un grave e imminente pericolo, non ritenuto meramente possibile, e non pregiudica seriamente un interesse essenziale dello Stato nei cui confronti è dovuto l'obbligo violato o la comunità internazionale nel suo complesso[94]. In ogni caso, lo stato di necessità non può essere invocato da uno Stato come causa di esclusione dell'illiceità se l'obbligo violato ne esclude la possibilità o se lo Stato ha contribuito al verificarsi di questa situazione[95].

Il Manuale di Tallinn riserva una particolare importanza allo stato di necessità, prevedendo, in aggiunta al riferimento contenuto nella regola 19 sulle circostanze che precludono l'illiceità delle operazioni cibernetiche[96], una specifica regola (26) basata sull'art. 25 del progetto della CDI:

> A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it.

Sarebbero pertanto giustificate dallo stato di necessità le operazioni cibernetiche con cui uno Stato reagisce agli attacchi DDoS condotti sul suo territorio che possano compromettere un interesse essenziale della vittima.

Più controversa è il caso in cui uno Stato vittima di attacchi speculativi aggressivi contro la propria valuta ricorra all'impiego di operazioni cibernetiche per chiudere la borsa valori straniera da cui provengono gli attacchi e limitare i danni. Ad oggi non sembra infatti che il diritto internazionale possa ammettere la necessità economica, e cioè un principio generale che permetterebbe agli Stati di giustificare la violazione di obblighi internazionali nel caso di una grave crisi finanziaria.

Lo stato di necessità potrebbe infine essere invocato per l'illecita raccolta di prove presenti sui server di uno Stato straniero. Nella maggior parte dei casi risulta tuttavia alquanto difficile dimostrare la sua necessità per salvaguardare un interesse essenziale

[94] Cfr. art. 25, paragrafo 1, del progetto della CDI.

[95] Cfr. art. 25, paragrafo 2, del progetto della CDI.

[96] «The wrongfulness of an act involving cyber operations is precluded in the case of: (a) consent; (b) self-defence; (c) countermeasures; (d) necessity; (e) *force majeure*; or (f) distress».

minacciato da un pericolo grave e imminente, se non nell'ipotesi in cui la minaccia riguardi un'infrastruttura critica: nel caso in cui, per esempio, l'impianto nucleare di uno Stato sia a rischio di essere distrutto dalle operazioni cibernetiche di un altro Stato, il primo potrebbe ritenere necessario raccogliere dati nei sistemi informatici del secondo al fine di mitigarne gli attacchi e porre fine al rischio che rappresentano per l'impianto[97].

2. Le conseguenze giuridiche della responsabilità internazionale

Verificato che non ricorrono cause di esclusione dell'illiceità di un'operazione cibernetica che sia contraria al diritto internazionale e attribuibile a uno Stato, si pone il problema di stabilire quali conseguenze giuridiche produca la commissione dell'operazione, che non fa di per sé venire meno il carattere vincolante dell'obbligazione violata[98]. Il progetto di articoli sulla responsabilità degli Stati individua due conseguenze dell'illecito: l'obbligo di cessazione e non ripetizione dell'illecito e l'obbligo di riparazione. Entrambi gli obblighi sono stati ripresi all'interno del Manuale di Tallinn[99].

2.1. Obbligo di cessazione e non ripetizione

Lo Stato responsabile dell'illecito ha innanzitutto l'obbligo di cessare il comportamento che costituisce la violazione dell'obbligo internazionale, ossia di porre termine alle violazioni che si estendono nel tempo[100], a condizione, naturalmente, che la regola violata sia ancora in vigore.

Gli attacchi DDoS, come quelli che hanno colpito l'Estonia nel 2007 o la Georgia nel 2008, mirano generalmente a rendere un servizio online indisponibile, o perturbarne il funzionamento inondandolo di traffico. Gli attacchi DDOS hanno generalmente un carattere di continuità, e i loro effetti perdurano fino a quando l'attacco è perpetrato. Pertanto, non appena gli attacchi DDoS oltrepassano la soglia della legalità, sorge automaticamente e istantaneamente l'obbligo di cessazione da parte dello Stato responsabile, anche qualora lo Stato vittima non abbia identificato gli attacchi o il loro responsabile né abbia intrapreso alcuna azione in risposta a essi.

[97] Cfr. F. Delerue, op. cit., pag. 350.

[98] Cfr. art. 29 del progetto della CDI.

[99] V. regole 27-29, pag. 142 ss.

[100] Cfr. art. 30, lett. a), del progetto della CDI.

L'obbligo di cessare il comportamento illecito si applica inequivocabilmente anche nel caso in cui la sovranità territoriale di uno Stato sia violata dall'intrusione di un malware, anche se dormiente, nel suo sistema informatico. La rimozione del malware dal sistema infettato costituisce al tempo stesso la cessazione dell'illecito e la riparazione del pregiudizio che questo ha causato[101]. L'obbligo di cessazione in capo al responsabile potrebbe tuttavia essere ragionevolmente considerato assolto anche nel caso in cui, benché il malware non sia stato ancora rimosso, siano soddisfatte entrambe le seguenti condizioni: cessazione di ogni utilizzo, controllo e comunicazione con il malware da parte del suo responsabile, e trasmissione alla vittima di tutte le informazioni necessarie alla completa e definitiva rimozione del malware. La trasmissione di queste informazioni, se da una parte consente alla vittima di aggiornare il proprio sistema informatico e impedire possibili future intrusioni attraverso la stessa vulnerabilità, dall'altra non pone fine di per sé all'intrusione, implicando l'adozione di misure concrete da parte dello Stato vittima per rimuovere l'infezione. È infatti preferibile che la rimozione del malware sia eseguita dal legittimo proprietario del sistema: richiedere la rimozione al suo responsabile gli consentirebbe di accedere ancora al sistema infettato e acquisire ulteriori informazioni su di esso; inoltre, l'atto di rimozione da parte del suo responsabile potrebbe produrre maggiori danni al sistema[102].

Se le circostanze lo richiedono, lo Stato ha l'obbligo di offrire assicurazioni e garanzie di non ripetizione del comportamento illecito[103].

Dal momento che uno Stato può essere indotto a ripetere la commissione di operazioni cibernetiche illecite fintantoché la loro legalità resta una questione aperta, le corti e i tribunali internazionali potrebbero essere indotti a richiedere assicurazioni e garanzie di non ripetizione di specifiche operazioni per chiarire il loro carattere illecito. Le garanzie e le assicurazioni possono assumere varie forme, incluse misure immediate e concrete. Nel contesto cibernetico, una misura specifica potrebbe consistere nel modificare la politica cibernetica nazionale al fine di prevedere la proibizione delle operazioni che violano il diritto internazionale[104].

[101] V. *infra*.

[102] Cfr. F. Delerue, op. cit., pagg. 386-388.

[103] Cfr. art. 30, lett. b) del progetto della CDI.

[104] Cfr. F. Delerue, op. cit., pag. 391.

2.2. Obbligo di riparazione

In capo allo Stato responsabile sorge l'obbligo di riparare integralmente il pregiudizio, comprendente ogni danno morale e materiale, causato con l'atto internazionalmente illecito[105]. La riparazione può consistere nella restituzione, nel risarcimento e/o nella soddisfazione[106]. Il calcolo del danno e la conseguente determinazione dell'appropriata riparazione possono essere influenzati dal dovere di ridurre i danni in capo allo Stato leso[107]. Nel contesto cibernetico, questo dovere è da intendersi sia come un generale dovere di ricorrere a validi sistemi di sicurezza cibernetica per proteggere le infrastrutture critiche dello Stato, sia come il dovere di adottare le misure necessarie ad attenuare gli effetti di un'operazione cibernetica in corso su un sistema informatico. Nel caso in cui un malware, come WannaCry[108] e NotPetya, infetti un sistema informatico attraverso una sua vulnerabilità già nota, lo Stato responsabile dell'operazione a cui sia avanzata una richiesta di riparazione potrebbe quindi affermare che la vittima non ha adempiuto al suo dovere di ridurre i danni. Nella maggior parte dei casi, tuttavia, le infrastrutture cibernetiche non sono gestite da uno Stato, bensì da soggetti privati, per le cui vulnerabilità non può essere ritenuto responsabile lo Stato in cui le infrastrutture sono localizzate.

2.2.1. Restituzione

In via generale, lo Stato responsabile di un illecito internazionale è obbligato alla riparazione "in forma specifica", ossia alla restituzione. Il progetto di articoli sulla responsabilità degli Stati, tuttavia, la esclude quando essa sia materialmente impossibile o comporti un onere sproporzionato in capo al soggetto responsabile rispetto al beneficio che da essa derivi per lo Stato leso a paragone di quello che deriverebbe dal risarcimento[109].

Un'operazione cibernetica può corrompere o cancellare i dati del sistema infettato. In situazioni del genere, il pregiudizio non può essere riparato con la restituzione, a meno che il malware, prima di aver cancellato i dati nel sistema infettato, ne abbia conservato

[105] Cfr. art. 31 del progetto della CDI.

[106] Cfr. art. 34 del progetto della CDI.

[107] La CIG, nella sentenza del 25 settembre 1997 nel caso del *Progetto Gabčíkovo-Nagymaros* (*Ungheria* c. *Slovacchia*), ha rilevato che uno Stato leso che non abbia adottato le misure necessarie a limitare il danno sostenuto non avrà il diritto di pretendere il risarcimento per il danno che avrebbe potuto impedire.

[108] WannaCry è un ransomware che nel maggio 2017 ha infettato i sistemi informatici di enti pubblici e grandi aziende in più di 150 paesi, criptando i file salvati sull'hard disk e chiedendo agli utenti il pagamento di un riscatto in bitcoin per poter riavere i dati e le piene funzionalità dei sistemi.

[109] Cfr. art. 35.

una copia: in questa specifica situazione, la riparazione consisterebbe nella restituzione dei dati copiati al loro proprietario originario[110].

2.2.2. Compensazione

Se la restituzione in forma specifica non è possibile (in tutto o in parte), lo Stato responsabile dell'illecito è tenuto a un risarcimento "per equivalente", che si traduce nel pagamento allo Stato leso di un ammontare monetario che corrisponde al valore stimato della restituzione in forma specifica[111].

Il pregiudizio non può essere riparato con la restituzione, per esempio, quando un'operazione cibernetica produce danni materiali, come nel caso di Stuxnet, che ha infettato il sistema informatico dell'impianto nucleare di Natanz in Iran e danneggiato svariate centrifughe aumentando la velocità delle turbine fino al punto di rottura. O come nel caso dell'operazione cibernetica che, secondo un rapporto pubblicato nel 2014 dall'ufficio federale per la sicurezza delle informazioni della Germania, ha causato l'avaria del sistema di controllo di un impianto siderurgico in territorio tedesco, impedendo l'arresto di una fornace e producendo ingenti danni ai macchinari[112].

La maggior parte delle operazioni cibernetiche producono tuttavia danni non materiali, quali l'alterazione o la distruzione di dati. Il problema è quindi determinare se tali danni siano valutabili dal punto di vista finanziario. Se i dati e i software sono regolarmente scambiati, allora il loro valore è facilmente calcolabile, e sarebbe pertanto possibile valutare il danno virtuale risultante da un'operazione cibernetica[113].

Analogamente ai casi di risanamento dell'inquinamento, la compensazione per il danno derivante da un'operazione cibernetica dovrebbe includere anche i costi per la rimozione del malware dal sistema informatico e, in alcuni casi, per il ripristino del sistema[114].

[110] Cfr. F. Delerue, op. cit., pag. 404.

[111] Cfr. art. 36 del progetto della CDI.

[112] Cfr. F. Delerue, op. cit., pagg. 407-408.

[113] Cfr. F. Delerue, op. cit., pag. 409.

[114] Cfr. F. Delerue, op. cit., pag. 410.

2.2.3. Soddisfazione

La soddisfazione è diretta a riparare il danno morale subito dallo Stato che è vittima dell'illecito, ovvero del danno giuridico, «consistente nella rottura della legalità internazionale implicata dalla violazione di un obbligo internazionale»[115]. La soddisfazione può consistere sia nel riconoscimento o nell'accertamento, da parte di una corte o di un tribunale internazionale, della violazione e del carattere obbligatorio della norma violata, sia nella presentazione solenne di scuse o in qualche altra modalità appropriata, quali il pagamento di una somma simbolica di denaro o la punizione degli individui responsabili materiali dell'azione illecita.

La soddisfazione sarebbe la forma di riparazione più appropriata per la violazione della sovranità o per l'offesa all'onore, alla dignità e al prestigio che risulti dalla deturpazione di un sito web istituzionale, come quello del presidente della Georgia durante la guerra russo-georgiana del 2008. Sembra invece più verosimile, quando si tratta di riparare la perdita di reputazione causata dalla messa fuori uso di siti web privati o commerciali, come quelli che sono stati colpiti dagli attacchi contro l'Estonia nel 2007 e contro la Georgia nel 2008, che una corte o un tribunale conceda un risarcimento monetario[116].

Più generalmente, la soddisfazione, quando consiste nel riconoscimento dell'illiceità della condotta cibernetica, potrebbe costituire un utile strumento ai fini della definizione del regime legale delle operazioni cibernetiche, e quindi della certezza del diritto internazionale.

3. Le reazioni all'illecito

Lo Stato leso ha il diritto d'invocare la responsabilità dello Stato autore dell'illecito. Se questo non adempie ai suoi obblighi, lo Stato può ricorrere a procedure giudiziali ed extragiudiziali per costringere lo Stato responsabile dell'illecito ad adempiere ai suoi obblighi.

[115] L. Fumagalli, *Illecito e responsabilità*, in S.M. Carbone, R. Luzzatto e A. Santa Maria (a cura di), op.cit.

[116] Cfr. F. Delerue, op. cit., pagg. 411-412.

3.1. Procedure giudiziali

Ad oggi, nessuna controversia internazionale avente per oggetto un'operazione cibernetica è stata sottoposta a una corte o a un tribunale internazionale. Lo sviluppo delle attività degli Stati nello spazio cibernetico prospetta tuttavia la possibilità che, in futuro, uno Stato possa presentare un'accusa per operazioni cibernetiche illecite davanti alla CIG o a un altro organo giurisdizionale internazionale. Una controversia relativa a un'operazione cibernetica potrebbe comportare un volume significativo di prove di natura estremamente tecnica. Gli Stati potrebbero tuttavia essere riluttanti a divulgare tali prove durante un procedimento giudiziario: in primo luogo, rivelare le evidenze raccolte significherebbe, per uno Stato, fornire indicazioni sulle proprie capacità cibernetiche; in secondo luogo, rendere pubbliche le informazioni relative a un attacco cibernetico potrebbe comportare il rischio che altri attori possano trarre vantaggio dalle vulnerabilità sfruttate dall'attacco. È in ogni caso essenziale che nei procedimenti giudiziari siano coinvolti, insieme agli esperti tecnici, anche esperti di altre discipline con una buona conoscenza del funzionamento dello spazio cibernetico, al fine di colmare la distanza tra la dimensione tecnica e la dimensione legale della controversia[117].

3.2. Procedure stragiudiziali: le contromisure

La commissione di un illecito internazionale comporta la possibilità, per lo Stato leso, di ricorrere a contromisure[118], violando a sua volta, senza incorrere in responsabilità, un diritto soggettivo dello Stato autore dell'illecito. Le contromisure devono essere tenute distinte dalle ritorsioni: anch'esse sono reazioni dello Stato leso nei confronti dello Stato responsabile di un illecito o di un atto ostile, ma non comportano alcuna violazione del diritto internazionale[119].

Soltanto gli Stati possano ricorrere a contromisure. Pertanto, nel caso in cui uno Stato sia stato leso da un atto adottato da un altro Stato, e decida di ricorrere a contromisure sotto forma di attacchi DDoS contro lo Stato responsabile, soltanto gli attacchi DDoS compiuti dagli organi del primo Stato, o da attori non statuali che agiscono sotto la sua

[117] Cfr. F. Delerue, op. cit., pagg. 108-110.

[118] Cfr. art 49, paragrafo 1, del progetto della CDI e regola 20 del Manuale di Tallinn, pag. 112 ss.

[119] In seno all'Unione europea è stata elaborata una raccolta di strumenti (EU Cyber Diplomacy Toolbox) per coordinare le possibili misure diplomatiche a disposizione degli Stati membri al fine di reagire alle azioni malevole nello spazio cibernetico, inclusa l'adozione di misure restrittive contro gli individui e gli enti ritenuti responsabili.

direzione o il suo controllo, e quelli riconosciuti e adottati a posteriori dallo Stato come propri sono attribuibili a esso; diversamente, gli attacchi lanciati da individui o gruppi per sostenere la reazione del primo Stato non possono valere come contromisure.

Dal momento che le contromisure sono adottate al solo fine di indurre lo Stato responsabile dell'illecito a conformarsi ai propri obblighi[120], lo Stato leso da un'operazione cibernetica che, per esempio, violi la sua sovranità e provochi gravi danni a una struttura industriale sul suo territorio può adottare contromisure anche dopo la cessazione dell'operazione, al fine di ottenere una piena riparazione del pregiudizio subito. Non possono tuttavia essere prese contromisure, e se già prese devono essere sospese senza indugio, se l'illecito è cessato e la controversia pende innanzi a una corte o a un tribunale che abbia il potete di adottare decisioni vincolanti per le parti[121].

3.2.1. I limiti delle contromisure

Le contromisure sono innanzitutto legittimate solo se consistenti nel non-adempimento di obbligazioni a cui lo Stato leso è tenuto nei confronti dello Stato responsabile dell'illecito[122]. La contromisura non deve consistere necessariamente nella violazione della stessa regola non osservata dallo Stato responsabile dell'illecito. Ne segue che una contromisura adottata in risposta a un'operazione cibernetica internazionalmente illecita può avvenire al di fuori dell'ambito cibernetico; allo stesso modo, uno Stato leso può adottare contromisure cibernetiche in risposta ad atti illeciti non cibernetici. Benché le contromisure possano essere rivolte soltanto contro lo Stato responsabile dell'illecito[123], attori non statuali potrebbero tuttavia esserne le principali vittime: specialmente le contromisure che assumono la forma di operazioni cibernetiche, per via dell'interconnessione di Internet, possono avere un impatto sui fornitori e sugli utenti di servizi online.

Secondariamente, le contromisure devono essere reversibili[124]. Potrebbero pertanto essere ritenute invalide le contromisure cibernetiche che, bloccando temporaneamente un server o un computer specifici, comportino delle perdite economiche[125].

---

[120] Cfr. art 49, paragrafo 1, del progetto della CDI e regola 21 del Manuale di Tallinn, pag. 117 ss.

[121] Cfr. art. 52, paragrafi 3 e 4, del progetto della CDI.

[122] Cfr. art. 49, paragrafo 2, del progetto della CDI.

[123] La regola 25 del Manuale di Tallinn (pag. 134 ss.) ribadisce il divieto di adottare contromisure, che siano o non siano di natura cibernetica, nei confronti di Stati diversi dallo Stato responsabile dell'illecito.

[124] Cfr. art. 49, paragrafo 3, del progetto della CDI.

[125] Cfr. F. Delerue, op. cit., pag. 441.

In terzo luogo, le contromisure, che siano o non siano cibernetiche, non possono pregiudicare i diritti umani fondamentali, gli obblighi di carattere umanitario che vietano rappresaglie, gli altri obblighi derivanti da norme imperative e gli obblighi relativi all'inviolabilità diplomatica e consolare. Una questione più controversa è la possibilità che una contromisura possa consistere in un uso della forza, quanto meno in risposta a un uso della forza che non costituisca un attacco armato: gli autori del Manuale di Tallinn erano divisi sul tema[126]; in considerazione di questo disaccordo, la regola 22 del Manuale, a differenza dell'art. 50 del progetto della CDI, di cui riproduce quasi interamente il testo, non prevede il divieto di adottare contromisure che pregiudichino l'obbligo di astenersi dalla minaccia o dall'uso della forza come espresso dalla Carta delle Nazioni Unite.

Infine, le contromisure sono legittime solo se proporzionate al pregiudizio sofferto dallo Stato leso[127].

3.2.2. Le contromisure urgenti

L'adozione di contromisure è subordinata alla messa in opera di alcuni adempimenti preventivi: lo Stato leso deve aver invitato lo Stato responsabile ad adempiere ai propri obblighi e comunicato l'intenzione di adottare contromisure, offrendo la disponibilità a negoziare[128]. Queste condizioni non trovano applicazione nel caso in cui lo Stato leso debba adottare contromisure urgenti per salvaguardare i propri diritti[129].

Le contromisure urgenti costituiscono una parte rilevante delle contromisure adottate in risposta a operazioni cibernetiche illecite. Lo Stato leso da attacchi DDoS o da un malware che abbia infettato il suo sistema informatico, causandone il malfunzionamento, può essere costretto a condurre operazioni cibernetiche illecite al fine di attenuare gli effetti degli attacchi, o acquisire le informazioni per farlo. Il successo di tali operazioni può dipendere in qualche misura dalla loro segretezza, a fronte dell'esigenza di non esporre le capacità difensive degli Stati in un settore estremamente sensibile come quello cibernetico. La loro previa notifica darebbe infatti l'opportunità allo Stato responsabile di evitare, o almeno attenuare, gli effetti delle contromisure. Per esempio, nel caso in cui lo Stato leso comunichi la sua decisione di penetrare e manomettere i server dello Stato

[126] Cfr. commento alla regola 22 del Manuale di Tallinn, parr. 9-13, pagg. 125-126.

[127] Cfr. art. 51 del progetto della CDI e regola 23 del Manuale di Tallinn, pag. 126 ss.

[128] Cfr. art. 52, paragrafo 1, del progetto della CDI.

[129] Cfr. art. 52, paragrafo 2, del progetto della CDI.

responsabile degli attacchi DDoS, questo potrebbe far transitare gli attacchi su server localizzati in Stati terzi, impedendo allo Stato leso di ricorrere a contromisure, che possono essere adottate soltanto nei confronti dello Stato responsabile; operazioni dello Stato leso contro i server localizzati in Stati terzi potrebbero tuttavia essere giustificate da altre cause di esclusione dell'illiceità, quale lo stato di necessità. Analogamente, qualora lo Stato vittima di un malware che ha colpito un'infrastruttura industriale sul suo territorio notifichi allo Stato responsabile l'intenzione di penetrarne i computer per acquisire le informazioni necessarie a rimuovere il malware dal sistema infettato, il secondo Stato potrebbe cancellare o trasferire i dati che il primo sta per cercare[130].

3.2.3. Le contromisure collettive

Lo Stato vittima di un'operazione cibernetica che non costituisce un attacco armato[131] non può beneficiare di misure illecite adottate da altri Stati per suo conto. In altre parole, gli Stati diversi dallo Stato leso non possono adottare contromisure nei confronti dello Stato responsabile dell'illecito[132]. Alcuni autori criticano l'impatto di tale limitazione sugli Stati più vulnerabili nel settore cibernetico[133]. Prendendo l'esempio delle operazioni cibernetiche del 2007 contro l'Estonia, qualora questa fosse autorizzata a lanciare delle contromisure di difesa attiva contro i sistemi informatici di uno Stato come la Russia, l'ampia differenza in termini di capacità cibernetiche tra i due paesi renderebbe improduttivi gli sforzi di Tallinn. Nel caso in cui le operazioni che hanno colpito l'Estonia avessero invece costituito un attacco armato, il diritto alla legittima difesa collettiva avrebbe permesso a Tallinn di beneficiare dell'aiuto dei suoi alleati. Per quanto allettante con riferimento al settore cibernetico, la possibilità di ricorrere a contromisure collettive potrebbe essere abusata dagli Stati più potenti ai fini di coercizione. Lo Stato leso da un'operazione cibernetica che non costituisce un attacco armato può tuttavia richiedere agli Stati terzi altre forme di sostegno, diverse dalle contromisure: nel 2008 la Georgia,

[130] Cfr. F. Delerue, op. cit., pagg. 445-448.

[131] V. *infra* cap. III.

[132] Cfr. regola 24 del Manuale di Tallinn, pag. 131 ss.

[133] Cfr. S. Li, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, in *Yale Journal of International Law*, 2013, pp. 211-215.

colpita da diverse operazioni cibernetiche durante il conflitto armato con la Russia, ha potuto attenuare gli effetti di tali operazioni con il sostegno di altri Stati[134].

La possibilità di ricorrere a contromisure collettiva non sarebbe prevista nemmeno in risposta a un'operazione cibernetica che violi un obbligo erga omnes. Il progetto di articoli del 2001 sulla responsabilità degli Stati, pur omettendo qualsiasi riferimento ai crimini internazionali[135], prevede che, in talune circostanze[136], uno Stato diverso da quello leso possa invocare la responsabilità dello Stato offensore, e reclamare l'adempimento dei suoi obblighi[137]. L'art. 54 del progetto specifica, in ogni caso, che gli Stati diversi da quello leso possono prendere soltanto misure lecite. L'art. 41 non esclude, tuttavia, che la violazione grave di un obbligo erga omnes, qualora imposto da una norma imperativa del diritto internazionale generale (*jus cogens*), possa comportare conseguenze ulteriori ai sensi del diritto internazionale.

È peraltro improbabile che, allo stato attuale del diritto internazionale e della tecnologia, un'operazione cibernetica possa costituire una grave violazione di un obbligo erga omnes, e a fortiori di una norma di *jus cogens*: appare infatti difficile immaginare di commettere un genocidio e violare norme appartenenti al diritto internazionale umanitario soltanto con mezzi cibernetici. Questa considerazione non vale a escludere l'assoggettamento delle operazioni cibernetiche, eseguite in un conflitto armato, delle norme a protezione delle vittime e della protezione civile. Ne deriva, per esempio, il principio secondo cui la popolazione civile non può essere oggetto di un attacco cibernetico[138], il divieto d'impiegare metodi e mezzi di guerra cibernetica che causino mali superflui e sofferenze non necessarie[139], e l'obbligo di proteggere i prigionieri di guerra dai danni derivanti dalle operazioni cibernetiche[140].

---

[134] Siti web georgiani sono stati trasferiti su server localizzati negli Stati Uniti e in Estonia, Inoltre, i CERT (Computer Emergency Response Team) francese e polacco hanno aiutato la Georgia ad analizzare le operazioni cibernetiche che l'hanno colpita, e il CERT estone ha inviato due specialisti in Georgia.

[135] L'art. 19 del progetto di articoli del 1996 sulla responsabilità degli Stati qualificava le violazioni di obblighi internazionali essenziali per la protezione di interessi fondamentali della comunità internazionale come crimini internazionali. Dalla violazione di un obbligo erga omnes discendeva la facoltà, per qualsiasi Stato, di adottare contro l'offensore tutte le possibili misure, incluse pertanto le contromisure, per eliminare le conseguenze negative della commissione del crimine internazionale.

[136] Cfr. art. 48, paragrafo 1, del progetto della CDI.

[137] Cfr. art. 48, paragrafo 2, del progetto della CDI e la regola 30 del Manuale di Tallinn, pag. 152 ss.

[138] Cfr. regola 94 del Manuale di Tallinn, pag. 422 ss.

[139] Cfr. regola 104 del Manuale di Tallinn, pag. 453 ss.

[140] Cfr. regola 135 del Manuale di Tallinn, pag. 520 ss.

3.3. La prassi

Tra i pochi esempi conosciuti di risposte a un attacco cibernetico figurano le misure adottate dagli Stati Uniti a seguito delle intrusioni nelle elezioni presidenziali del novembre 2016. [141] Riconducibili alla tipologia di attacchi cibernetici che causano la raccolta e la diffusione pubblica di informazioni o dati sensibili con intento malevolo (*cyber exploitation* o *doxing*), le intrusioni nei processi elettorali sono un fenomeno piuttosto diffuso negli ultimi anni. Secondo l'Office of the Director of National Intelligence e il Department of Homeland Security, le intrusioni sarebbero state dirette dai servizi segreti russi e finalizzate a ridurre il consenso alla candidata Hillary Clinton rispetto a Donald Trump. Per reagire alle presunte ingerenze di Mosca, nel dicembre 2016 gli Stati Uniti hanno adottato sanzioni di tipo finanziario nei confronti di funzionari dei servizi segreti russi[142], cui hanno fatto seguito nel marzo 2018 provvedimenti di congelamento dei beni di altri tredici individui e delle società russe Internet Research Agency, Concord Catering e Concord Management and Consulting LLC[143].

Alla luce della limitata casistica di reazioni a un attacco cibernetico, risultano particolarmente utili, ai fini della ricostruzione della prassi, le posizioni assunte dagli Stati in materia: se alcuni stati, a partire dai membri del G7 (Canada[144], Francia, Germania[145],

[141] Cfr. A. Bonfanti, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Rivista di diritto internazionale*, 2019, pag. 694 ss.

[142] Stati Uniti, Executive Office of the President, *Executive Order 13757. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*, 28 dicembre 2016, www.govinfo.gov/content/pkg/FR-2017-01-03/pdf/2016-31922.pdf.

[143] Stati Uniti, Department of the Treasury, *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*, 15 marzo 2018, home.treasury.gov/news/press-releases/sm0312.

[144] Governo dell'Australia, *International Law applicable in cyberspace*, aprile 2022, www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.

[145] Governo Federale della Germania, *On the Application of International Law in Cyberspace*, marzo 2021, www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

Giappone[146], Italia[147], Regno Unito[148] e Stati Uniti[149]), hanno confermato l'adeguatezza delle contromisure in risposta a operazioni cibernetiche che costituiscono un illecito internazionale (sotto la soglia di un attacco armato), altri stati, come il Brasile[150], raccomandano un approccio più cauto, sulla base di alcuni fattori quali la difficoltà di attribuire un'operazione cibernetica, la possibilità di mascherarne l'autore, e l'alto rischio di escalation.

* * *

Malgrado la supposta legittimità di adottare contromisure in risposta a operazioni cibernetiche illecite, nella prassi si riscontra una reticenza a giustificare come tali le misure che alcuni Stati lesi avrebbero preso nei confronti dei presunti responsabili dell'illecito. La Corea del Nord, dopo essere stata pubblicamente accusata dagli Stati Uniti di essere la responsabile dell'hackeraggio della Sony Pictures Entertainment nel 2014[151], è stata colpita da un attacco DDoS che l'ha disconnessa da Internet per un paio di giorni, e che si presume rappresenti la risposta statunitense all'hackeraggio della Sony[152]. La ragione per cui il governo statunitense, che ha negato qualsiasi coinvolgimento, potrebbe aver deciso di ricorrere a una *covert operation*, anziché giustificare la sua presunta azione

[146] Giappone, Ministry of Foreign Affairs, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, 16 giugno 2021, www.mofa.go.jp/files/100200935.pdf.

[147] Italia, Ministero degli Affari Esteri e della Cooperazione Internazionale, *Italian position paper on 'international law and cyberspace'*, novembre 2021, www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

[148] Regno Unito, Foreign, Commonwealth & Development Office, *Application of international law to states' conduct in cyberspace: UK statement*, 3 giugno 2021, www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

[149] Nazioni Unite, Assemblea generale, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States*, A/76/136 (13 luglio 2021), pag. 136 ss.

[150] Ivi, pag. 17 ss.

[151] Cfr. D.E. Sanger e N. Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, 17 dicembre 2014, www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

[152] Cfr. M. Fackler, *North Korea Accuses U.S. of Staging Internet Failure*, 27 dicembre 2014, www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html.

come contromisura, potrebbe risiedere nell'incertezza a cui è ancora soggetta l'applicazione del diritto internazionale allo spazio cibernetico e nella convenienza a non inquadrare la reazione all'interno di un quadro giuridico suscettibile di essere contestato[153].

[153] Cfr. F. Delerue, op. cit., pagg. 488-490.

CAPITOLO III

L'uso della forza e il sistema di sicurezza collettiva nello spazio cibernetico

La Carta delle Nazioni Unite è stata adottata circa cinquant'anni prima delle prime operazioni cibernetiche e non include pertanto nessuna disposizione specifica su di esse. L'assenza di specifici riferimenti alle operazioni cibernetiche non rende tuttavia la Carta inapplicabile a esse: i suoi articoli sono stati scritti con sufficiente flessibilità da adattarsi ai nuovi sviluppi in materia di sicurezza internazionale[154].

1. Il divieto dell'uso della forza

Attualmente non esiste nessun trattato internazionale che proibisca il ricorso di uno Stato alla forza cibernetica, che è pertanto limitato dal divieto generale della minaccia e dell'uso prevista nella Carta e nel diritto internazionale generale.

Benché non producano effetti esplosivi, analogamente alle armi chimiche, batteriologiche e biologiche, e mettano quindi in discussione le caratteristiche che tipicamente identificano un'arma, le operazioni cibernetiche possono costituire in determinate circostanze un uso della forza proibito dall'art. 2, comma 4 della Carta[155]. A esse può infatti essere applicata la definizione sviluppata da Ian Brownlie, secondo cui il ricorso alle armi non tradizionali può essere assimilato all'uso della forza sulla base di due considerazioni: il loro uso è comunemente indicato come una forma di guerra, ed esse possono essere impiegate per distruggere vite umane e proprietà[156].

1.1. La nozione di forza cibernetica

La dottrina identifica tradizionalmente tre principali approcci ai fini della qualificazione di un'operazione come uso della forza, basati rispettivamente sull'obiettivo dell'operazione, sullo strumento utilizzato e sulle conseguenze che l'operazione produce.

---

[154] Cfr. F. Delerue, op. cit., pagg. 277-284.

[155] Cfr. regola 68 del Manuale di Tallinn, pag. 329 ss.

[156] Cfr. I. Brownlie, *International Law and the Use of Force by States*, 1963, pag. 362.

Secondo l'approccio basato sull'obiettivo, si configura come uso della forza ogni operazione cibernetica che penetri il sistema di infrastrutture critiche nazionali. Questo approccio, sviluppato sulla base dell'idea che l'attuale quadro giuridico non offra sufficiente protezione agli Stati colpiti, risulterebbe troppo inclusivo in quanto non tiene in considerazione l'intensità delle operazioni[157].

L'approccio basato sul vettore dell'attacco è ancora più problematico perché la maggior parte delle operazioni cibernetiche sono difficilmente configurabili come armi tradizionali. Questo approccio, più ragionevole in passato, ha perso molta della sua rilevanza con lo sviluppo delle nuove tecnologie, in particolare quelle a duplice o molteplice uso[158].

Secondo l'approccio basato sugli effetti, le operazioni cibernetiche che causano distruzione fisica o perdita di vite umane si configurerebbero sempre come uso della forza, mentre la qualificazione delle operazioni che abbiano soltanto conseguenze virtuali sarebbe controversa[159].

Questi approcci si basano sull'attuale quadro giuridico che disciplina la proibizione dell'uso della forza. Benché possa apparire attraente l'idea di concepire un nuovo quadro giuridico su misura per le operazioni cibernetiche, la flessibilità della Carta e la difficoltà di raggiungere un consenso su questi temi suggeriscono di continuare a impiegare il regime esistente. Nel quadro della Carta, l'approccio più idoneo per accertare l'uso della forza cibernetica sembra essere quello basato sugli effetti, integrato con elementi tratti dagli altri due approcci, tanto da essere fatto poprio anche dal Manuale di Tallin: secondo la regola 69, «un'operazione cibernetica costituisce un uso della forza quando la sua portata e i suoi effetti sono paragonabili alle operazioni non-cibernetiche che raggiungono il livello di un uso della forza». La gravità è pertanto il fattore più significativo da tenere in considerazione al momento di decidere se un'operazione cibernetica si configuri come uso della forza: le operazioni che provocano danni fisici a individui e proprietà costituiscono un uso della forza, mentre le operazioni che ingenerano meri disagi o irritazione non saranno mai considerate tali[160].

---

[157] Cfr. M. Roscini, *Cyber Operations and the Use of Force in International Law*, 2014, p. 54.

[158] Cfr. M. Roscini, *World Wide Warfare* - Jus ad bellum *and the Use of Force*, in *Max Planck Yearbook of United Nations Law*, 2010, p. 106.

[159] V. nota 118.

[160] Cfr. F. Delerue, op. cit., pag. 290.

Dal momento che le situazioni tra questi due estremi sono meno intuitivamente definibili, il gruppo di esperti che ha partecipato alla redazione del Manuale di Tallinn ha individuato altri sette fattori, oltre a quello della gravità, che gli Stati tendono a considerare quando si tratta di determinare se ricorre un uso proibito della forza cibernetica[161]:

a. *Immediatezza.* Gli Stati nutrono maggiore preoccupazione per le conseguenze immediate rispetto a quelle che hanno l'opportunità di prevenire. Gli Stati sono pertanto più propensi a qualificare come un uso della forza un'operazione cibernetica che produca effetti immediati rispetto a un'operazione che impieghi settimane o messi a raggiungere gli effetti voluti.

b. *Causalità.* Quanto più stretto è il nesso di causa ed effetto tra un'operazione cibernetica e i suoi effetti, tanto maggiore è la probabilità che l'operazione sia qualificata come un uso della forza.

c. *Invasività.* Di regola, quanto più è sicuro un sistema informatico, tanto maggiore è la preoccupazione che suscita una sua penetrazione. Inoltre, quanto più gli effetti di un'operazione cibernetica sono limitati a uno Sato specifico, tanto maggiore è il grado d'invasività percepito.

d. *Misurabilità degli effetti.* Quanto più un'operazione cibernetica è valutabile in termini specifici (come la quantità dei dati corrotti, la percentuale di server disabilitati o il numero di file confidenziali esfiltrati), tanto più facile sarà per gli Stati determinare se l'operazione costituisca un uso della forza.

e. *Natura militare.* Il fatto che la Carta presti particolare attenzione alla forza armata suggerisce che un nesso tra un'operazione cibernetica e un'operazione militare accresca la probabilità che l'operazione sia qualificata come un uso della forza.

f. *Coinvolgimento dello Stato.* Quanto maggiore è il coinvolgimento di uno Stato nella conduzione di un'operazione cibernetica, tanto maggiore è la probabilità gli altri Stati qualifichino l'operazione come un uso della forza.

g. *Presunta legittimità.* Nel diritto internazionale, gli atti che non sono espressamente vietati sono presuntivamente leciti. Pertanto, è meno probabile che le operazioni cibernetiche che ricadono in alcune categorie di atti che il diritto internazionale non

[161] Cfr. commento alla regola 69 del Manuale di Tallinn, par. 9, pagg. 333-336.

proibisce (come la propaganda, le operazioni psicologiche, lo spionaggio o la mera pressione economica) siano considerate un uso della forza.

Quando si voglia trovare conferma ulteriore del risultato al quale si è giunti sulla base dell'approccio elaborato dal gruppo di esperti, o quando la sua utilizzazione non abbia eliminato i dubbi sulla qualificazione dell'operazione cibernetica, possono essere presi in considerazione l'intento dello Stato offensore, la pubblicità dell'operazione e le circostanze in cui questa è stata lanciata[162].

1.2. Il divieto della minaccia della forza

Una minaccia di ricorrere alla forza cibernetica violerà la proibizione di cui all'art. 2, quarto comma, della Carta soltanto se la forza cibernetica minacciata equivale a un uso della forza proibito nelle stesse circostanze[163].

La minaccia di ricorrere alla forza è credibile se è sufficientemente grave da essere considerata tale dallo Stato minacciato. Per esempio, è probabile che la minaccia da parte della Federazione Russa di ricorrere alla forza cibernetica contro un altro Stato postsovietico sia qualificata come una minaccia proibita per il precedente, presunto, ricorso di Mosca a operazioni cibernetiche contro la Georgia e l'Estonia. Diversamente, la minaccia di ricorrere alla forza cibernetica contro uno Stato con un'infrastruttura Internet scarsamente sviluppata potrebbe non essere considerata sul serio, dal momento che l'uso della forza promesso non si ripercuoterebbe pesantemente sullo Stato minacciato.

Non si esclude che la minaccia possa essere avanzata implicitamente e quindi formulata attraverso comportamenti concludenti. Per esempio, attacchi DDoS su larga scala contro uno Stato dipendente da Internet o malware che infettino un impianto nucleare modificando i dati presenti nel suo sistema informatico, senza arrecare nessun danno fisico, potrebbero avere lo scopo di dimostrare le capacità dell'offensore e la sua determinazione a condurre ulteriori attacchi.

La CIG, nella sentenza del 27 giugno 1986 nel caso delle *Attività militari e paramilitari degli Stati Uniti in Nicaragua e contro il Nicaragua* (*Nicaragua* c. *Stati Uniti*), ha ritenuto che il rafforzamento del potenziale bellico non costituisse una minaccia di ricorrere alla forza e fosse pertanto conforme al diritto internazionale. La stessa conclusione varrebbe per il rafforzamento delle capacità cibernetiche.

[162] Cfr. F. Delerue, op. cit., pagg. 305-310.

[163] Cfr. regola 70 del Manuale di Tallinn, pag. 337 ss.

Fino ad oggi non si registrano casi di minaccia dell'uso della forza cibernetica vietata dall'art. 2, quarto comma, della Carta. Per la specificità delle operazioni cibernetiche, la cui efficacia è dovuta allo sfruttamento delle vulnerabilità e all'elemento di sorpresa, è infatti improbabile che sorgano delle minacce di ricorre alla forza cibernetica. La minaccia di ricorrere a operazioni cibernetiche contro uno Stato consentirebbe infatti a quest'ultimo di proteggere le proprie infrastrutture e preparare delle possibili contromisure al fine di prevenire gli effetti dell'uso della forza cibernetica che è stato minacciato.

2. La legittima difesa

Per analogia con l'art. 51 della Carta, soltanto le operazioni cibernetiche che raggiungono il livello di un "attacco armato" conferiscono allo Stato che ne è vittima il diritto all'autotutela, individuale[164] e collettiva[165]; le misure prese nell'esercizio di questo diritto devono essere immediatamente portate a conoscenza del Consiglio di sicurezza delle Nazioni Unite[166]. In risposta alle operazioni che costituiscono un uso della forza ma non raggiungono il livello di un attacco armato, gli Stati, oltre a tentare di risolvere la controversia con mezzi pacifici[167] o sottoporre la situazione al Consiglio di sicurezza delle Nazioni Unite, possono ricorrere soltanto a misure non implicanti l'uso della forza. Ad oggi nessuna operazione cibernetica è stata inequivocabilmente ritenuta idonea a integrare la fattispecie di attacco armato, che richiede un certo grado d'intensità.

Le operazioni cibernetiche che provocano danni, distruzioni, lesioni o decessi possono configurarsi come attacchi armati se le loro conseguenze raggiungono una determinata soglia[168]. Per esempio, la distruzione di uno smartphone dovuta al surriscaldamento causato da un'operazione cibernetica non costituirebbe un attacco armato cibernetico; in questo caso, lo Stato vittima potrebbe quindi ricorrere a contromisure contro lo Stato responsabile dell'operazione cibernetica illecita, ma non potrebbe esercitare il suo diritto di autotutela. Ad oggi Stuxnet è l'unica operazione cibernetica nota che ha causato danni

[164] Cfr. regola 71 del Manuale di Tallinn, pag. 340 ss.

[165] Cfr. regola 74 del Manuale di Tallinn, pag. 355 ss.

[166] Cfr. regola 75 del Manuale di Tallinn, pag. 356 ss.

[167] Cfr. regola 65 del Manuale di Tallinn, pag. 304 ss.

[168] Gli autori del Manuale di Tallinn convengono che rilevino «tutte le conseguenze ragionevolmente prevedibili» (commento alla regola 71, par. 13, pag. 343). Se, per esempio, un'operazione cibernetica colpisse un impianto di purificazione dell'acqua, il rischio di contagio e morte provocato dall'assunzione di acqua contaminata andrebbe preso in considerazione.

gravi; alcuni autori del Manuale di Tallinn ritengono che essa abbia raggiunto il livello di un attacco armato, e ciò anche alla luce del fatto che essa ha colpito un impianto nucleare[169].

Le operazioni cibernetiche che producono conseguenze immateriali non sono generalmente considerate un uso della forza, e a fortiori non potrebbero equivalere a un attacco armato, se non in circostanze estremamente limitate. Una minoranza di commentatori, tuttavia, sostiene che il furto di informazioni militari sensibili pregiudica la sicurezza nazionale e può quindi qualificarsi come attacco armato[170].

Se l'incursione militare di uno Stato nel territorio di un altro è l'ipotesi più comune di attacco armato, può configurarsi come tale anche un attacco rivolto contro la manifestazione esterna di uno Stato localizzata all'estero. È pacifico che le unità e le installazioni militari all'estero siano considerate una manifestazione esterna dello Stato ai fini dell'esercizio del diritto di autotutela. Un attacco cibernetico che colpisce il sistema di bordo di un velivolo militare – ciò vale, in determinate circostanze, anche nel caso di un aeromobile civile – in volo al di fuori dello spazio aereo nazionale, causandone la caduta, costituirebbe pertanto un attacco armato e consentirebbe allo Stato di bandiera di esercitare il diritto di autotutela. Lo stesso dicasi per un'operazione cibernetica contro i computer e i sistemi informatici di un'ambasciata che raggiunga il grado d'intensità richiesto per poter essere qualificata come un attacco armato.

In alcune circostanze, uno Stato potrebbe condurre simultaneamente molteplici operazioni cibernetiche, di scarsa portata ma di intensa frequenza, che singolarmente non costituiscono un attacco armato; in situazioni come queste, secondo la dottrina dell'accumulazione degli eventi[171], le operazioni andrebbero considerate nel loro insieme per verificare se la soglia minima di portata ed effetti dell'attacco armato è stata oltrepassata. Le situazioni in cui è possibile avvalersi dell'accumulazione degli eventi nell'ambito cibernetico per determinare la risposta più appropriata all'attacco sono tuttavia limitate dalla difficoltà di accertare che le singole operazioni equivalgano a un uso della forza.

---

[169] Cfr. commento alla regola 71 del Manuale di Tallinn, par. 10, pag. 342.

[170] Cfr. C.C. Joyner e C. Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, in *European Journal of International Law*, 2001, pag. 855.

[171] Cfr. CIG 27 giugno 1986, *Attività militari e paramilitari in Nicaragua e contro il Nicaragua* (*Nicaragua* c. *Stati Uniti*), par. 231; CIG 6 novembre 2003, *Piattaforme petrolifere* (*Iran* c. *Stati Uniti*), par. 64; CIG 19 dicembre 2005, *Attività armate sul territorio del Congo* (*Repubblica Democratica del Congo* c. *Uganda*), par. 146.

2.1. I requisiti della legittima difesa

Il diritto consuetudinario prevede che la legittima difesa sia esercitata nei limiti della necessità e della proporzionalità[172].

Il requisito della necessità richiede che l'autotutela sia usata soltanto in ultima istanza: prima di ricorrere all'uso della forza, lo Stato vittima dell'attacco cibernetico potrebbe, in primo luogo, modificare le caratteristiche di sicurezza del proprio sistema o correggere le vulnerabilità sfruttate dall'attacco e, in secondo luogo, adottare delle contromisure contro lo Stato responsabile, come arrestare il computer usato per condurre l'operazione o colpire il sistema elettrico che alimenta l'infrastruttura Internet utilizzata per il transito dell'operazione[173].

La proporzionalità non pretende perfetta simmetria tra "violazione subita" e "reazione" dello Stato: è sufficiente che la reazione abbia la finalità di respingere l'attacco e porre fine a esso. Le operazioni cibernetiche possono pertanto essere impiegate per legittima difesa contro attacchi armati cinetici, e viceversa. I requisiti di necessità e proporzionalità possono tuttavia influenzare la scelta delle armi e dei metodi da utilizzare. Spesso, in risposta a un attacco cibernetico, soltanto le operazioni cibernetiche soddisfano i già menzionati requisiti. Per esempio, lo Stato vittima di un attacco cibernetico, al fine di spegnere i server usati dal suo responsabile, può bombardarli fisicamente o lanciare un'operazione cibernetica che li danneggi arrestando il loro sistema di raffreddamento. In un tale scenario, la prima opzione risulterebbe sproporzionata e non necessaria, se quella meno distruttiva fosse disponibile, se cioè lo Stato vittima avesse sufficienti capacità cibernetiche. Il minore rischio di escalation che le operazioni cibernetiche comportano incoraggia il ricorso a esse anche per legittima difesa contro attacchi armati non cibernetici[174].

I requisiti di necessità e proporzionalità possono rendere più problematico lo sviluppo e l'impiego dei sistemi di difesa cibernetica autonomi, che dovranno essere programmati in modo che possano non solo determinare con certezza se le operazioni cibernetiche a cui reagiscono costituiscono un attacco armato, ma anche calibrare la reazione nel rispetto dei requisiti della legittima difesa.

---

[172] Cfr. CIG 27 giugno 1986, cit. alla nota 133.

[173] Cfr. F. Delerue, op. cit., pagg. 479-480.

[174] Cfr. F. Delerue, op. cit., pagg. 481-482.

2.2. La legittima difesa preventiva

Ulteriore requisito a cui è subordinata la legittima difesa è quello temporale: l'art. 51 della Carta consente il ricorso alla legittima difesa nel caso in cui l'attacco armato «abbia luogo», o quanto meno sia già iniziato ancorché non abbia ancora raggiunto l'obiettivo (c.d. legittima difesa intercettiva).

Le operazioni cibernetiche possono impiegare meno di un secondo a transitare tra il sistema da cui sono lanciate e il sistema a cui sono dirette. La legittima difesa intercettiva avrebbe pertanto poca rilevanza in questi casi. In alcune circostanze, l'operazione cibernetica che produce il danno può essere preceduta da un'altra operazione tesa a raccogliere informazioni sul sistema da colpire. In questa ipotesi, l'attacco armato comincia soltanto quando avviene il danno, e non con la fase di ricognizione, altrimenti si ammetterebbe l'esercizio del diritto di autotutela ogniqualvolta uno Stato scopre di essere vittima di spionaggio cibernetico. In altri casi, l'operazione cibernetica dannosa può impiegare più tempo a produrre i propri effetti. Per esempio, ipotizzando che Stuxnet costituisse un attacco armato e che fosse riconducibile a uno Stato, qualora l'Iran avesse identificato il virus nel sistema prima che danneggiasse le centrifughe sarebbe stato autorizzato a prendere delle misure di legittima difesa intercettiva per impedire la prosecuzione dell'attacco. In questo scenario, la difficoltà consiste nel determinare il momento in cui l'operazione cominci la sua azione distruttiva, che coincide con l'accelerazione delle turbine delle centrifughe. Diversamente, impiantare una "bomba logica" in un sistema informatico non sarebbe sufficiente a giustificare l'adozione di misure di legittima difesa intercettiva: fintanto che la bomba rimane dormiente, sussiste soltanto una violazione della sovranità dello Stato, che può ricorrere a misure non implicanti l'uso della forza per rimuovere il malware[175].

Secondo parte della dottrina, la legittima difesa preventiva sarebbe eccezionalmente ammessa anche quando vi siano prove certe che l'attacco sia oggettivamente imminente. Sono stati proposti tre condizioni per determinare se un'operazione cibernetica possa fondare il diritto di autotutela preventiva: in primo luogo, l'operazione cibernetica dovrebbe essere parte di una più grande operazione che possa costituire un attacco armato; in secondo luogo, l'operazione cibernetica deve essere irrevocabile; in terzo luogo, lo

[175] Cfr. F. Delerue, op. cit., pagg. 468-472.

Stato colpito può agire solo nell'ultima finestra di opportunità[176]. Nella pratica, è chiaro che nella maggior parte dei casi sarebbe quasi impossibile identificare il risultato complessivo di un'operazione imminente, o dimostrare la sua attribuzione a uno Stato ai fini dell'esercizio del diritto di autotutela; il test appare pertanto difficile da applicare.

2.3. La legittima difesa contro gli attori non statuali

L'assenza di una definizione di "attacco armato", e in particolare l'assenza di qualsiasi riferimento al suo potenziale autore, può essere spiegata dal fatto che nel 1945 era evidente che solo uno Stato potesse ricorrere a un tale livello di forza contro un altro Stato. Le modalità e la gravità di attentati, come quello dell'11 settembre 2001, realizzati da movimenti non direttamente riconducibili a uno Stato hanno tuttavia messo in dubbio l'attualità delle categorie tradizionali alla base del concetto di legittima difesa.

Nell'ambito cibernetico può risultare particolarmente difficile definire la relazione tra l'autore non statuale responsabile di un attacco e il presunto Stato patrocinante. La prospettiva di estendere l'esercizio del diritto di autotutela alle minacce poste da attori non statuali può pertanto apparire seducente. Gli autori del Manuale di Tallinn sono divisi sul tema, ma la maggioranza di loro ritiene che il diritto di autotutela si applichi anche nei confronti degli attori non statuali[177]. La CIG, se nel parere del 9 luglio 2004 ha escluso che Israele potesse invocare la legittima difesa a giustificazione della costruzione del muro nei Territori palestinesi occupati, affermando che l'art. 51 della Carta si riferisse soltanto all'attacco armato di uno Stato contro altri Stati e non agli attacchi perpetrati da gruppi di privati, nella successiva sentenza del 19 dicembre 2005 sulla attività militari nel territorio del Congo si è astenuta dal pronunciarsi sulla questione.

3. Il sistema di sicurezza collettiva delle Nazioni Unite

Il Consiglio di sicurezza delle Nazioni Unite, qualora determini, ai sensi dell'art. 39 della Carta, che un'operazione cibernetica costituisce una minaccia alla pace, una violazione della pace o un atto di aggressione, può prendere in considerazione l'adozione di misure

[176] Cfr. M.N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, pagg. 932-933.

[177] Cfr. commento alla regola 71 del Manuale di Tallinn, parr. 18-20, pagg. 345-346.

non implicanti l'uso della forza (art. 41 della Carta) o implicanti l'uso della forza (art. 42 della Carta), incluse misure cibernetiche[178].

L'elenco, meramente esemplificativo, dei possibili contenuti delle misure non implicanti l'uso della forza che compare nello stesso art. 41 della Carta include anche «un'interruzione totale o parziale […] delle comunicazioni […] postali, telegrafiche, radio ed altre». Questa previsione conferma che il Consiglio di sicurezza potrebbe decidere un'interruzione delle comunicazioni cibernetiche. In tal caso, è indispensabile che gli Stati adottino una legislazione nazionale per obbligare i service provider sottoposti alla loro giurisdizione a prendere tutte le misure necessarie a rispettare la risoluzione del Consiglio di sicurezza, come l'istituzione di una "lista nera" di nomi di dominio o l'impiego di strumenti che filtrino l'instradamento dei pacchetti IP.

Qualora le misure non implicanti l'uso della forza siano valutate o si siano rivelate inidonee al mantenimento o al ristabilimento della pace, il Consiglio di sicurezza può decidere l'adozione di misure implicanti l'uso della forza. La prassi sull'adozione di azioni implicanti l'uso della forza evidenzia il frequente ricorso ad autorizzazioni con le quali il Consiglio di sicurezza invita gli Stati, o le organizzazioni regionali (ai sensi dell'art. 53 della Carta)[179], ad adottare "tutte le misure necessarie" ad attuare la sua risoluzione: questa espressione implicherebbe pertanto la possibilità di usare anche la forza cibernetica, seppur non strettamente in linea con il riferimento alle sole «forze aeree, navali o terrestri» contenuto nell'art. 42.

Tra i modelli alternativi di intervento a cui ricorre il Consiglio di sicurezza spiccano le operazioni di *peace-keeping*, che si caratterizzano per il divieto dell'uso delle armi salvo il ricorrere di situazioni di legittima difesa, per la subordinazione della forza di pace al consenso dello Stato territoriale e per la sua rigorosa neutralità rispetto alle parti in conflitto. In taluni casi le operazioni cibernetiche possono essere i mezzi più efficaci per svolgere i compiti delineati nel mandato dell'operazione, che verosimilmente non menzionerà espressamente il loro uso: la valutazione della loro liceità richiederà pertanto l'interpretazione dei termini del mandato[180]. Così, se la funzione delle forze armate impiegate in un'operazione di *peace-keeping* è la garanzia dell'attuazione del cessate-il-fuoco, il

[178] Cfr. regola 76 del Manuale di Tallinn, pag. 357 ss.

[179] Cfr. regola 77 del Manuale di Tallinn, pag. 360 ss.

[180] Cfr. regola 78 del Manuale di Tallinn, pag. 361 ss.

mandato dell'operazione potrebbe essere interpretato nel senso di permettere il monitoraggio delle comunicazioni cibernetiche delle parti al fine di assicurare che non intraprendano attività contrarie all'accordo.

A partire dagli anni '90, al modello tradizionale del *peace-keeping* si è affiancata una nuova generazione di operazioni il cui mandato è quello di garantire la pacificazione di un'area ovvero un obiettivo di soccorso umanitario, da conseguire anche attraverso l'impiego della forza armata. Nelle c.d. operazioni di *peace-enforcement*, la liceità dall'uso della forza cibernetica dipenderebbe dalla precisa autorizzazione conferita dal Consiglio di sicurezza, e dal rispetto del diritto internazionale applicabile. L'uso della forza sarebbe inoltre permesso per contrastare i tentativi di interferire con l'esecuzione della missione: se un'operazione cibernetica compromette il sistema di comando e controllo dell'operazione, la forza di pace è legittimata a usare la forza cibernetica per interrompere l'operazione.

Meno pacifica è la liceità di utilizzare la forza per assistere dei civili quando l'uso della forza non sia espressamente autorizzato. Gli autori del Manuale di Tallinn ritengono che sia appropriato colpire con mezzi cibernetici un social media utilizzato per incitare alla violenza contro un gruppo etnico locale[181].

I componenti di una forza di pace godono della protezione conferita ai civili dal diritto dei conflitti armati e non potranno essere oggetto di alcun attentato, inclusi quelli di natura cibernetica[182]. Il personale delle Nazioni Unite e il personale associato perderanno tuttavia la loro protezione se partecipano in maniera diretta alle ostilità. Nel momento in cui una forza di pace diventa una delle parti in conflitto, le sue operazioni cibernetiche saranno sottomesse alle regole del diritto dei conflitti armati.

* * *

[181] Cfr. commento alla regola 78, par. 19, pag. 365.

[182] Cfr. regola 79 del Manuale di Tallinn, pag. 368 ss.

Il presente capitolo ha dimostrato che le operazioni cibernetiche, benché ad oggi nessuno Stato o nessuna organizzazione internazionale abbia pubblicamente qualificato una di esse come un uso della forza, in talune circostanze potrebbero costituire un attacco armato. Anche nei casi in cui sia possibile ricorrere alla legittima difesa, tuttavia, le contromisure potrebbero rappresentare la risposta più appropriata per reagire a un attacco cibernetico.

CONCLUSIONI

Disconnessione

La ricerca sull'applicazione del diritto internazionale alle operazioni cibernetiche ha evidenziato che, sebbene l'adattamento allo spazio cibernetico della maggior parte delle norme che disciplinano la responsabilità degli Stati e l'uso della forza non si riveli eccessivamente complesso, permangono, da una parte, alcune difficoltà interpretative e, dall'altra, alcune questioni irrisolte. Basti citare la definizione del grado di controllo che consente di attribuire a uno Stato l'operazione cibernetica condotta da attori non statuali, l'individuazione delle circostanze che configurano un'operazione cibernetica come un uso della forza o un attacco armato, la liceità di un'operazione cibernetica equivalente a un uso della forza come contromisura, e la legittimità di adottare contromisure collettive in risposta a un'operazione cibernetica illecita. Non si tratta che della trasposizione, nell'ambito cibernetico, di quesiti già emersi in occasione dell'interpretazione e dell'applicazione di specifiche norme di diritto internazionale fuori dal "metaverso". La loro soluzione dipenderà pertanto dalla risposta che tali quesiti riceveranno nella dimensione tradizione del diritto internazionale. Va tuttavia sottolineato che le caratteristiche del funzionamento dello spazio cibernetico possono esasperare la difficoltà di classificare alcune fattispecie all'interno delle categorie previste dal quadro giuridico esistente: oggi è infatti relativamente facile ed economico, per un attore non statuale, preparare e condurre un'operazione cibernetica equivalente a un uso della forza o a un attacco armato. Questa circostanza impone l'esigenza d'interrogarsi sulla persistente validità dell'assunto secondo cui il diritto internazionale non dovrebbe regolare i comportamenti, e le operazioni cibernetiche, degli attori non statuali, se non in limitati casi[183].

L'incertezza sulla corretta applicazione di norme a portata universale rischia di condurre a una pericolosa frammentazione del diritto internazionale e a una maggiore instabilità dell'ordine globale, se si considera che è più probabile che operazioni cibernetiche illecite sorgano tra Stati che non condividono gli stessi orientamenti. In tale contesto, acquista particolare significato l'adozione, nel giugno 2021, del rapporto finale del

[183] Cfr. regola 33 del Manuale di Tallinn, pag. 175 ss.

sesto GGE[184], dopo il mancato raggiungimento di un consenso nel 2017[185]. Nonostante l'unico passo avanti nel rapporto del 2021, rispetto a quelli adottati nel 2013 e nel 2015, sia stato il riconoscimento dell'applicabilità del diritto internazionale umanitario alle operazioni cibernetiche – non si sono registrati progressi su temi come la sovranità e l'obbligo di diligenza, né sono state trattate le contromisure – il solo fatto che attori chiave nella disciplina dello spazio cibernetico abbiano ripreso a lavorare insieme all'indomani del fallimento del 2017 è incoraggiante. Analogamente, il riconoscimento, da parte del GGE, che al momento attuale non sono ravvisabili significativi avanzamenti nell'identificazione delle norme internazionali applicabili allo spazio cibernetico, e la conseguente attenzione riservata all'elaborazione di norme non vincolanti non devono essere considerati in maniera negativa: nel corso del tempo, infatti, alcune di queste norme possono essere riconosciute come vincolanti dalla comunità internazionale e cristallizzarsi in norme di diritto internazionale generale[186].

Fintantoché alcuni aspetti della disciplina delle operazioni cibernetiche restano controversi, il mezzo migliore che gli Stati hanno per proteggersi da esse è sviluppare le proprie capacità di difesa cibernetica, insieme a un'azione di sensibilizzazione nei confronti dei propri cittadini sulle minacce cibernetiche, se si considera che, nella maggior parte dei casi, la disattenzione o la scarsa informazione degli utenti vittima di phishing sono all'origine dell'infezione dei loro sistemi informatici.

Prima di terminare, è importante sottolineare che gli effetti della diffusione massiccia di Internet non si registrano solo nel contenuto materiale delle norme di diritto internazionale, ma anche nelle stesse modalità di formazione ed applicazione del diritto internazionale. Secondo una parte della dottrina, l'impatto della tecnologia sull'ordinamento internazionale sarebbe triplice: essa modifica i problemi che il diritto internazionale deve risolvere (alterazione degli scopi); modifica la gamma di risposte disponibili per i problemi che si confrontano con il diritto internazionale (alterazione dei mezzi); modifica le strutture intellettuali che formano il pensiero giuridico in generale e il diritto internazionale in particolare, e trasforma la natura e le funzioni del diritto internazionale

[184] Nazioni Unite, Assemblea generale, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135 (14 luglio 2021).

[185] V. nota 8.

[186] Cfr. M.N. Schmitt, *The Sixth United Nations GGE and International Law in Cyberspace*, 10 giugno 2021, www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

anche quando non sono toccate da cambiamenti tecnologici (alterazione strutturale)[187]. L'influenza derivante dall'uso dalla Rete si è prodotta soprattutto con riferimento alle fasi di produzione, applicazione ed enforcement delle norme di diritto internazionale, nonché al novero dei soggetti rilevanti nell'ordinamento internazionale. Innanzitutto, la diffusione delle ICT ha semplificato la circolazione di una pluralità di modelli culturali e favorito la creazione dei c.d. network transnazionali (o transgovernativi), reti di coordinamento che hanno accresciuto l'apertura degli ordinamenti interni al diritto internazionale. La Rete ha anche accelerato il processo di "democratizzazione" dell'ordinamento internazionale, riducendo i tempi e i costi dei negoziati relativi ai trattati internazionali, e rendendo possibile la partecipazione di attori diversi da quelli tradizionali nella fase di creazione del diritto. La società civile, oltre ad acquistare un ruolo sempre più rilevante nella fase di produzione delle norme, è diventata il "controllore" della loro osservanza da parte degli Stati e delle organizzazioni internazionali. Internet, poi, ha aumentato sia la circolazione della dottrina e della giurisprudenza, sia la diffusione delle notizie relative alle violazioni di obblighi internazionali commesse dagli Stati. Si può pertanto affermare che rispetto alla metà degli anni '90 del secolo scorso, con l'avvento di Internet, «sebbene non sia mutato né il numero dei soggetti di diritto internazionale né il sistema delle fonti dell'ordinamento medesimo, i primi si trovano oggi però a "utilizzare" le seconde in un contesto molto più permeabile ad influenze esterne promananti soprattutto da soggetti privati i quali, anche se privi di veri e propri poteri di enforcement del diritto internazionale, esercitano in via di fatto […] un sempre più efficace controllo diffuso del rispetto degli obblighi internazionali da parte di coloro che ne sono vincolanti»[188].

[187] Cfr. J.W. Dellapenna, *Law in a Shrinking World: The Interaction of Science and Technology in International Law*, in *Kentucky Law Journal*, 2000, pag. 828.

[188] G.M. Ruotolo, op. cit., pag. 133.

APPENDICE I

La governance di Internet

Con l'espressione "governance di Internet" si fa riferimento allo sviluppo e all'applicazione da parte dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, di principi, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet[189]. Questa definizione operativa riconosce alla governance di Internet una natura "multilivello", alla quale sono invitati a partecipare non solo gli Stati e le organizzazioni internazionali, ma anche le ONG e gli operatori economici.

Negli anni '90, momento della definitiva affermazione su base globale di questo fenomeno, si è aperto il dibattito circa l'approccio più idoneo a governare la Rete. Il dibattito è ancora aperto, tanto che «Internet non è attualmente sottoposta ad alcuna forma di governance generale verticalizzata»[190], ovvero non esistono meccanismi istituzionali unici di gestione della Rete, sia per quanto riguarda i suoi aspetti tecnici sia in merito alle politiche di accesso e uso. Ciò è in parte dovuto all'architettura propria di Internet: essa è priva di una struttura gerarchica, dal momento che le singole sottoreti che la compongono sono connesse tra loro in numerosi punti e non esiste un nodo centrale da cui si diramano tutti i percorsi.

1.1. Il ruolo degli Stati

I soggetti classici del diritto internazionale appaiono sempre meno in grado di garantire appieno l'esercizio della propria sovranità rispetto alle attività praticate su Internet. Infatti, «l'assenza di frontiere fisiche nel cyberspazio impedirebbe l'individuazione del diritto (statale) applicabile ad una determinata fattispecie e, per il medesimo motivo, il giudice competente a dirimere le controversie»[191]. Si parla, a questo proposito, di "carattere aterritoriale" della Rete per indicare la difficoltà di stabilire la corretta disciplina applicabile a determinati rapporti:

---

189 Cfr. il *Report of the Working Group on Internet Governance* (giugno 2005), disponibile all'indirizzo www.wgig.org/docs/WGIGREPORT.pdf.

190 G.M. Ruotolo, op. cit., pag. 48.

191 Ivi, pag. 28.

> L'avvento della Rete mette in crisi l'idea di diritto come insieme di regole ancorato ad un ambito territoriale determinato che ne segna il raggio d'azione in relazione ad individui soggetti alle regole in quanto fisicamente insediati su quel territorio[192].

In aggiunta, da più parti viene mossa agli Stati la critica secondo cui sottoporre Internet alla legge nazionale comporterebbe il rischio che si formino tante differenti regolamentazioni del medesimo fenomeno, tra loro confliggenti, quanti sono i legislatori statali (c.d. *spillover effect*).

1.2. (segue): la gestione unilaterale del sistema DNS da parte degli USA

Nonostante la perdita di centralità da parte degli Stati, una procedura indispensabile per l'esistenza stessa dalle Rete vede proprio uno di loro, gli Stati Uniti, in una posizione privilegiata. Si tratta dell'assegnazione dell'indirizzo IP e del nome di dominio a esso associato. Il nome di dominio è costituito da una serie di stringhe alfanumeriche separate da punti, ognuna delle quali, lette da destra verso sinistra, rappresenta un livello gerarchico via via più specifico. I domini si dividono fra quelli generici, che possono essere utilizzati da particolari categorie di organizzazioni indipendentemente dalla loro localizzazione geografica, e quelli nazionali, che fanno riferimento a indirizzi di operatori localizzati in un determinato Stato. Il sistema dei nomi di dominio (Domain Name System o DNS) funziona grazie a 13 *root* server, i quali, operando attraverso un database che fa conoscere alle macchine che lo consultano (client) come individuare il nodo desiderato, hanno il compito di tradurre i nomi degli host in indirizzi IP (query).

La procedura di assegnazione dei nomi di dominio è coordinata dalla Internet Corporation for Assigned Names and Numbers (ICANN), un'organizzazione statunitense di diritto privato senza scopo di lucro istituita nel 1988. Essa gestisce direttamente i domini generici di primo livello e indirettamente tutti gli altri livelli di dominio. Sotto la sua diretta amministrazione, la Internet Numbers Assigned Authority (IANA)[193] è incaricata di assegnare gli indirizzi IP. Per il tramite di ICANN e IANA, il governo statunitense, e specificamente la National Telecommunications and Information Administration (NTIA) del Department of Commerce, è in grado di modificare il contenuto del *root* database.

---

[192] G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2010, p. 278.

[193] La IANA è un organismo che ha la responsabilità nell'assegnazione degli indirizzi IP, la quale viene però delegata a enti regionali denominati Regional Internet Registries: RIPE per l'Europa e il Medio Oriente, APNIC per l'area Asia-Pacifico, ARIN per gli Stati Uniti e il Canada, LACNIC per l'America Latina e l'area caraibica, AfriNIC per l'Africa.

Per la teoria classica del diritto internazionale, la situazione appena descritta potrebbe costituire un'ipotesi di applicazione extraterritoriale della potestà di governo statunitense, dal momento che parte *dei* root server è posizionata al di fuori degli Stati Uniti. Il principio consuetudinario di non ingerenza impone agli Stati l'obbligo «di astenersi dal compimento di qualsiasi attività comportante svolgimento di pubbliche funzioni in territorio altrui, senza il consenso dello Stato territoriale […] il compimento di attività di questo tipo nel territorio è riservato allo Stato territoriale, e il suo svolgimento che abbia materialmente luogo da parte di un altro stato in quel territorio viola il diritto di sovranità rispetto allo Stato territoriale»[194].

Per giustificare il potere autorizzatorio esercitato dalla NTIA su macchine localizzate al di fuori del suo territorio, gli Stati Uniti hanno dichiarato di voler preservare la sicurezza e la stabilità del sistema dei nomi di dominio e si sono impegnati a non realizzare alcun comportamento idoneo a metterne in pericolo l'efficienza[195]. Gli Stati Uniti fanno inoltre riferimento ad una sorta di tradizione del loro ruolo storico nella gestione del DNS, benché in merito all'esistenza di una qualche consuetudine si registra l'opposizione del Brasile, il cui delegato, nel corso della riunione del terzo Preparatory Committee della seconda fase del World Summit on Information Society (WSIS), contestò l'esercizio del potere statunitense di gestione dei server. Secondo il rappresentante brasiliano, l'attuale struttura per la governance globale di Internet, pur riuscendo ad assicurare alta disponibilità e grande stabilità all'operatività del network, presenta significative limitazioni e un'evidente mancanza di legittimazione.

D'altra parte, l'illiceità di un comportamento in contrasto con un obbligo internazionale sarebbe esclusa ove quel comportamento sia tenuto con il consenso del soggetto verso cui sussiste quell'obbligo. La legittimazione delle azioni degli Stati Uniti risiederebbe così nell'acquiescenza da parte degli Stati di allocazione territoriale dei server; riprendendo la definizione datane dalla CIG nella sentenza del 12 ottobre 1994 sulla *Delimitazione della frontiera marittima nella regione del golfo del Maine*, l'acquiescenza consiste in un tacito riconoscimento manifestato da un comportamento unilaterale che l'atra parte può interpretare come un consenso.

[194] R. Luzzatto, I. Queirolo, *Sovranità territoriale, "jurisdiction" e regole di immunità*, in S.M. Carbone, R. Luzzatto, A. Santa Maria (a cura di), op. cit., pag. 238.

[195] V. nota 10.

Secondo un approccio più recente, il comportamento degli Stati Uniti rientrerebbe fra i modi attraverso cui si esprime il diritto amministrativo globale. L'aggettivo "globale" richiama il concetto di globalizzazione, formatosi nel contesto economico:

> Proprio lo sviluppo e l'intensificazione della velocità degli scambi e dei mercati finanziari su scala mondiale, infatti, hanno contribuito in misura determinante a creare sistemi regolatori dove gli Stati non figurano più come soggetti sovrani unitari – secondo le forme classiche del diritto internazionale – e si delineano vere e proprie pubbliche amministrazioni globali[196].

Spesso, infatti, i negoziati tra gli Stati risultano inefficaci ai fini della tutela di interessi che presentino caratteri globali, come l'ambiente, i beni culturali dell'umanità, il mercato del lavoro internazionale, l'integrazione dei mercati, la lotta alla criminalità internazionale:

> La dimensione globale degli interessi pubblici, quindi, può avere la conseguenza di richiedere la presenza di un'amministrazione internazionale che operi in un ordine giuridico extra-statale[197].

La scienza giuridica ha individuato cinque tipi di *global administration*: l'amministrazione condotta da organizzazioni internazionali di stampo classico; l'amministrazione basata sull'azione collettiva di amministrazioni nazionali per mezzo di reti di coordinamento (i c.d. network transnazionali); l'amministrazione "distribuita", delegata a un apparato amministrativo nazionale legittimato da obblighi internazionali a svolgere funzioni di rilevanza globale; l'amministrazione "ibrida", esercitata in forza di accordi tra strutture amministrative pubbliche e soggetti privati; l'amministrazione diretta da istituzioni non governative che assumono funzioni regolatorie. In questo senso, l'esercizio extraterritoriale della potestà regolamentaria del sistema DNS da parte degli Stati Uniti apparterrebbe alla categoria dell'amministrazione "distribuita". Tale potere, che rimane comunque soggetto a una serie di norme stabilite dal diritto internazionale, sarebbe condizionato, nel caso di specie, dalla mancata opposizione degli altri Stati al suo concreto esercizio.

[196] L. Casini, *Diritto amministrativo globale*, in S. Cassese (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, pag. 1944.

[197] Ivi, pag. 1945.

1.3. (segue): la posizione italiana sui principi fondamentali di Internet

Un importante elemento della prassi italiana in materia di Internet governance è rappresentato da un documento elaborato dall'allora Ministero dell'Istruzione, dell'Università e della Ricerca in occasione del lancio della consultazione pubblica sui principi fondamentali di Internet[198].

Il documento[199], che riassume la posizione italiana sull'argomento, si apre con un preambolo che elenca le complessità di Internet:

> Anzitutto è un luogo fondamentale di produzione e scambio di conoscenza e, in quanto tale, è un'inestimabile risorsa per l'educazione, l'informazione, la ricerca, e lo sviluppo dei popoli. Favorendo l'accesso all'informazione, promuove inoltre meccanismi virtuosi di trasparenza e buon governo. In secondo luogo, Internet è il motore dell'economia globale: è driver di innovazione, ma anche l'infrastruttura principale per la partecipazione delle imprese, anche locali, all'economia mondiale. In terzo luogo, Internet è una piattaforma di comunicazione interpersonale che, anche grazie alla diffusione di dispositivi mobili, sta rapidamente diventando il mezzo principe di comunicazione, in grado di abbattere barriere geografiche e di aprire nuovi canali tra istituzioni pubbliche e cittadini, promuovendo creatività, condivisione e partecipazione. Infine, Internet è un veicolo sempre più indispensabile di organizzazione sociale e partecipazione dal basso.

Il preambolo si chiude con l'ammissione che «la governance di Internet non può prescindere dall'apporto e dalla partecipazione attiva dei netizens, ossia coloro che quotidianamente usano e costruiscono la rete e le sue applicazioni».

Seguono i principi fondanti della Rete, divisi nelle seguenti cinque sezioni: principi generali, che definiscono le caratteristiche principali dell'infrastruttura; cittadinanza in rete; utenti in quanto consumatori di servizi in Internet; produzione e circolazione dei contenuti; sicurezza in rete.

Fra i principi generali spiccano "Internet bene comune" e "Internet strumento cruciale per lo sviluppo e l'esercizio dei diritti umani": viene così individuato il diritto di ciascun individuo ad accedere ai contenuti pubblici disponibili in Rete e a beneficiare dei

[198] La consultazione pubblica era attiva dal 18 settembre al 1° novembre 2012 e aperta a tutti i cittadini, organizzazioni private, società civile organizzata o istituzioni pubbliche che volessero inviare un contributo al dibattito. La consultazione serviva a definire e preparare la posizione italiana sui principi fondamentali di Internet in vista del settimo Internet Governance Forum.

[199] Il documento è disponibile è all'indirizzo download.repubblica.it/pdf/2012/tecnologia/internet.pdf.

progressi della tecnologia digitale. Vengono inoltre assicurati i requisiti di apertura, competitività e innovazione del sistema grazie alla neutralità delle Rete, nonché al modello decisionale trasparente con il coinvolgimento di tutti gli stakeholder.

La promozione della cittadinanza digitale prevede, da una parte, che lo Stato aiuti tutti i cittadini, senza alcuna discriminazione, a diventare utenti attivi della Rete e, dall'altra, che le istituzioni pubbliche, oltre a condividere con loro i dati che producono e gestiscono, s'impegnino a offrire un'adeguata distribuzione di punti di accesso a Internet. Affinché la Rete e le sue applicazioni costituiscano importanti mezzi di partecipazione democratica dal basso, viene tutelata la capacità di organizzarsi, promuovere azioni collettive e manifestare il proprio dissenso online.

Le istituzioni pubbliche, e in particolare il sistema educativo in collaborazione con imprese e governi locali, s'incaricano di favorire l'acquisizione e l'aggiornamento continuo delle competenze digitali nei diversi settori della società. L'identità digitale viene protetta attraverso la promozione, nell'utente, della consapevolezza delle tracce informative memorizzate in rete e la protezione, da ingerenze commerciali e/o istituzionali, della riservatezza degli utenti e delle relative comunicazioni attraverso la Rete. Ogni utente è poi titolare del cosiddetto "diritto all'oblio", vale a dire la possibilità di richiedere la cancellazione di informazioni e dati personali presenti negli archivi, anche online.
Riguardo alla produzione e circolazione dei contenuti, se da una parte si garantisce la tutela dei diritti dei loro creatori (diritto d'autore, marchi, brevetti e segreto commerciale), dall'altra s'incoraggiano gli utenti a essere parte attiva ai flussi di conoscenza culturale e scientifica, mediante il diritto alla copia personale, alla citazione e al riuso della conoscenza in Rete.

Infine, i profilli della sicurezza in Rete prevedono che lo Stato preservi Internet, in quanto infrastruttura di interesse nazionale, da attacchi esterni, fatte salve le norme del diritto internazionale, e adotti adeguate misure per assicurare l'integrità della Rete e il suo uso non malevolo o per fini terroristici e criminali, salvaguardando al tempo stesso il suo uso nell'esercizio della libertà di espressione.

2.1. Il ruolo delle Nazioni Unite: la convocazione del WSIS

La redazione di una convenzione sulla governance della Rete era lo scopo primario del WSIS, indetto dall'Assemblea generale delle Nazioni Unite con la risoluzione 56/183 del 21 dicembre 2001. La prima fase del summit si è svolta a Ginevra dal 10 al 12 dicembre

2003 e vi hanno partecipato 175 paesi e numerose organizzazioni internazionali, governative e no. Al termine della conferenza di Ginevra sono stati adottati una Dichiarazione di principi e un Piano d'azione sul prosieguo dei lavori[200].

La Dichiarazione di principi si apre con l'esposizione di una visione comune da parte dei partecipanti alla conferenza, i quali si autodefiniscono "rappresentanti dei popoli del mondo" e dichiarano il proprio desiderio comune di costruire una società dell'informazione centrata sulla persona, inclusiva e orientata allo sviluppo, dove ognuno possa creare, accedere, utilizzare e condividere informazioni e conoscenza, consentendo nel contempo agli individui, alle comunità e ai popoli di promuovere il loro sviluppo sostenibile e migliorare il loro tenore di vita.

Le questioni relative a Internet vengono affrontate ai punti 48-50 della Dichiarazione di principi. Al punto 48 sono elencate le caratteristiche che deve possedere la governance di Internet: la gestione internazionale della Rete dovrebbe essere multilaterale, trasparente e democratica, con il pieno coinvolgimento dei governi, del settore privato, della società civile e delle organizzazioni internazionali, e dovrebbe garantire un'equa distribuzione di risorse, facilitare l'accesso per tutti e assicurare un funzionamento di Internet stabile e sicuro, tenendo conto del multilinguismo.

Al punto seguente, oltre a ribadire la necessità della partecipazione di tutti gli stakeholder alla definizione delle questioni tecniche della Rete, viene confermata la sovranità degli Stati sopra le politiche pubbliche relative a Internet, ma viene altresì riconosciuto il ruolo fondamentale che il settore privato, la società civile, le organizzazioni intergovernative e le altre organizzazioni internazionali hanno avuto, e devono mantenere, nello sviluppo di Internet.

Il Piano d'azione, riprendendo il punto 50 della Dichiarazione di principi, prevede la creazione, da parte del Segretario generale delle Nazioni Unite, di un gruppo di lavoro sulla governance di Internet, all'interno di un processo aperto che assicurasse la partecipazione dei governi, del settore privato e della società civile e che coinvolgesse le organizzazioni internazionali. Il gruppo di lavoro sarebbe stato incaricato di sviluppare una definizione operativa della governance di Internet, identificare le questioni di politica pubblica riguardanti la governance di Internet, sviluppare una comprensione comune dei rispettivi ruoli e responsabilità degli attori coinvolti, preparare un rapporto sui risultati di questa attività da presentare in occasione della seconda fase del WSIS. Questa si è tenuta

[200] I documenti adottati nel corso del Summit sono disponibili all'indirizzo www.itu.int/net/wsis/.

a Tunisi dal 16 al 18 novembre 2005. Le due fasi del WSIS sono state intervallate dalle riunioni del Preparatory Committee, svoltesi a Ginevra.

A differenza della prima conferenza, piuttosto generalista, quella di Tunisi si è concentrata sulla lotta al divario digitale[201] e sulla governance di Internet. Essa ha portato all'adozione di un atto di impegno esclusivamente politico, il Tunis Commitment, e dell'Agenda di Tunisi per la società dell'informazione. I partecipanti non riuscirono a trovare un accordo sulle modifiche da apportare al regime corrente dell'ICANN: le cause sono da ricercarsi sia nel rifiuto degli Stati Uniti a cedere i propri privilegi nella gestione del root database, sia nell'incapacità degli altri attori di suggerire alternative all'ICANN o proposte per l'attuazione di un regime internazionale. Al punto 68, l'Agenda di Tunisi dichiara che tutti i governi dovrebbero avere un ruolo e una responsabilità paritari per la governance internazionale di Internet e per assicurare la stabilità, la sicurezza e la continuità della Rete. Le modalità concepite per l'implementazione di questo principio erano troppo vaghe e l'ICANN ha continuato a operare senza cambiamenti di sorta, pur persistendo i suoi problemi di legittimazione.

Il Summit si è rivelato un fallimento sotto il profilo della redazione di un trattato per disciplinare la Rete. La mancata stesura di una convenzione generale sulla governance del Web ha rappresentato un segnale positivo per quanti credevano che «l'idea stessa di una verticalizzazione del controllo della Rete nelle mani degli Stati o di organizzazioni da questi create […] potrebbe risultare strutturalmente incompatibile con le logiche che fino ad oggi hanno permesso alla Rete di proliferare»[202], rappresentando un limite per i suoi sviluppi futuri.

L'unico sviluppo di rilievo emerso a Tunisi è stata la creazione dell'Internet Governance Forum (IGF), a cui sono stati assegnati i seguenti compiti: allargare la partecipazione alla discussione sulle tematiche della Rete a tutti i possibili gruppi d'interesse, affrontare le questioni relative alle risorse critiche di Internet, cercare delle soluzioni per i problemi legati all'abuso di Internet. Ad oggi, l'IGF si è riunito sedici volte, l'ultima delle quali a Katowice, in Polonia, dal 6 al 10 dicembre 2021.

[201] V. *infra* appendice II.

[202] G.M. Ruotolo, op. cit., pag. 65.

3.1. Il ruolo dell'Unione europea

L'Unione europea promuove lo sviluppo e la diffusione delle nuove ICT sin dal 1998, quando ha liberalizzato il mercato europeo delle telecomunicazioni.

Al proprio interno, l'Unione ha svolto un ruolo di sostegno fondamentale alla rivoluzione digitale, mediante la creazione di un mercato europeo aperto, la garanzia di condizioni di accesso equo a tutte le imprese, la tutela degli interessi dei consumatori e lo sviluppo di standard tecnici. L'Unione trae la legittimità a intervenire nel campo delle ICT dagli artt. 179-190 del Trattato sul funzionamento dell'Unione europea (TFUE), sotto il Titolo XIX della sua Parte Terza (Politiche e azioni interne dell'Unione). In base all'art. 4 TFUE, nei settori di cui al Titolo XIX (Ricerca e sviluppo tecnologico e spazio), l'Unione ha competenza per condurre azioni e una politica comune, senza che l'esercizio di tale competenza possa impedire agli Stati membri di esercitare la loro (competenza concorrente). L'insieme delle azioni svolte dall'Unione, elencate all'art. 180, è contenuto in un programma quadro pluriennale che viene adottato dal Parlamento europeo e dal Consiglio, che deliberano secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale. Ai sensi dell'art. 182, il programma quadro fissa gli obiettivi scientifici e tecnologici da realizzare mediante le azioni previste dall'art. 180 – vi rientrano la promozione della cooperazione in materia di ricerca, sviluppo tecnologico e dimostrazione dell'Unione con i paesi terzi e le organizzazioni internazionali – e le relative priorità, indica le grandi linee di dette azioni, stabilisce l'importo globale massimo e le modalità della partecipazione finanziaria dell'Unione al programma quadro, nonché le quote rispettive di ciascuna azione prevista.

All'esterno, l'Unione esercita un ruolo attivo in occasione delle conferenze multilaterali convocate per decidere il futuro e il controllo della Rete. Al termine del secondo IGF, svoltosi a Rio de Janeiro dal 12 al 15 novembre 2007, il Parlamento europeo ha adottato una risoluzione[203] nella quale afferma che «benché l'IGF non adotti conclusioni formali, sia responsabilità dell'Unione europea sostenere tale processo, poiché offre un quadro positivo e concreto per definire il futuro di Internet sulla base di un approccio multilaterale [e] sottolinea la necessità di garantire in futuro una rete aperta e indipendente, basata sulle iniziative e sulle esigenze dei soggetti interessati e sulla libertà di espressione».

[203] Risoluzione del Parlamento europeo, del 17 gennaio 2008, *Risultati del forum sulla governance di internet, svoltosi a Rio de Janeiro dal 12 al 15 novembre 2007*, in GUUE C 41 E, del 12 febbraio 2009, pagg. 80-81.

La Commissione europea ha trattato la questione della governance di Internet in due comunicazioni[204] emesse il 18 giugno 2009. Nella prima[205] si legge:

> L'uso e la penetrazione di internet sono tanto capillari, soprattutto in paesi sviluppati come quelli dell'UE, che internet è ormai una risorsa critica e gravi perturbazioni del suo funzionamento potrebbero avere effetti catastrofici sulla società e l'economia […] La maggior parte degli internauti della CE hanno pertanto aspettative legittime quanto all'affidabilità del "loro internet". In caso di grave perturbazione del servizio internet a livello nazionale è ovvio aspettarsi che gli utenti si rivolgano ai governi e non già ai vari organismi di governance di internet responsabili del coordinamento delle risorse.

L'Unione si fa quindi promotrice dei seguenti principi fondamentali per il successo di Internet: mantenere la sua struttura aperta; garantire la leadership del settore privato nell'operatività giornaliera di Internet e lasciare i temi di interesse pubblico ai governi; assicurare la partecipazione di una pluralità di soggetti al processo di governance di Internet, per promuovere la cooperazione globale.

La seconda comunicazione[206] dedica l'intero paragrafo 3 alla governance della Rete. Nelle parole della Commissione, «demandare interamente lo sviluppo dell'internet degli oggetti al settore privato, o ad altre regioni del mondo, non è ragionevole dati i profondi mutamenti a livello sociale che l'internet degli oggetti comporterà. Molti di questi cambiamenti dovranno essere affrontati dai responsabili politici europei e dalle autorità pubbliche per garantire che le tecnologie e le applicazioni dell'Internet degli oggetti stimolino la crescita economica, migliorino il benessere dei singoli e consentano di affrontare alcuni dei problemi che interessano la società odierna». Con questo intento, sono state elaborate le seguenti linee di azione: definire una serie di principi per la governance

[204] Le comunicazioni della Commissione sono atti atipici. Gli atti atipici costituiscono una categoria di atti formalmente non vincolanti adottati dalle istituzioni europee. Essi possono riguardare l'organizzazione interna all'Unione europea o avere una portata più generale relativa a settori politici precisi: ne fanno parte i regolamenti interni delle istituzioni, i programmi generali attuati dal Consiglio su una determinata materia, lo statuto della Corte di Giustizia, gli accordi interistituzionali ecc. Si chiamano "atipici" perché non fanno parte dalla nomenclatura degli atti giuridici prevista dai trattati e la loro portata è generalmente politica.

[205] Comunicazione della Commissione al Parlamento europeo e al Consiglio, del 18 giugno 2009, *Governance di Internet: le prossime tappe* [non pubblicata nella Gazzetta ufficiale].

[206] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, del 18 giugno 2009, *L'internet degli oggetti - Un piano d'azione per l'Europa* [non pubblicata nella Gazzetta ufficiale].

dell'Internet degli oggetti; creare un'architettura con una struttura di gestione decentralizzata; identificare i rischi emergenti; sensibilizzare le istituzioni.

3.2. (segue): il principio di neutralità della Rete

Nel 2009 le istituzioni europee hanno fatto proprio il principio della neutralità della Rete[207], con l'adozione, il 25 novembre 2009, delle direttive n. 136[208] e 140[209] e del regolamento n. 1211[210]. In attuazione del c.d. Telecoms Package, l'Olanda è stato il primo Paese membro a riconoscere il principio di neutralità della Rete all'interno della propria legislazione. La norma, in risposta ai comportamenti di molte società di telecomunicazioni che hanno iniziato a discriminare determinati contenuti nei confronti di utenti che non avevano sottoscritto i loro servizi di velocità superiore, vieta ai fornitori di rete d'impedire o rallentare applicazioni e servizi su Internet, a meno che la misura in questiona abbia il fine di ridurre gli effetti di una congestione del traffico, preservare l'integrità della Rete, applicare una norma legislativa o un ordine giudiziario.

La Commissione europea ha successivamente emanato una Dichiarazione sulla neutralità della rete[211] in cui ribadisce «che sia della massima importanza conservare

[207] Con la diffusione della rete Internet, si è avvertito il bisogno di garantire a tutti gli utenti l'opportunità di usufruire indiscriminatamente di qualsiasi servizio offerto online. Secondo il principio di neutralità della Rete, «una rete a banda larga deve essere priva di restrizioni arbitrarie sui dispositivi connessi e sul modo in cui essi operano» (G. Pascuzzi, op. cit., p. 22). Nella pratica, il rispetto di questo principio si traduce nella possibilità di ciascun utente connesso a Internet di accedervi sempre alla stessa velocità di collegamento (banda), preventivamente concordata con il proprio fornitore di rete, senza che la tipologia di dati scambiati con qualsiasi altro nodo della Rete possa determinarne la velocità di trasferimento. L'osservanza del principio di neutralità implica che la Rete faccia tutto il possibile «per trasmettere tutti i dati inviati o richiesti da un determinato utente senza discriminarne alcune, anche se, a volte, una discriminazione, nei fatti, dovesse verificarsi» (G.M. Ruotolo, op. cit., p. 36), come nel caso di un rallentamento nel trasferimento di grandi quantità di dati dovuto a un intasamento della Rete. L'alternativa alla neutralità della Rete è rappresentata dalla c.d. *quality of service*, la quale muove dalla considerazione che determinate trasmissioni via Internet non debbano subire interruzioni, ma anzi godere di una priorità rispetto ad altri dati.

[208] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia d reti e di servizi di comunicazione elettronica, delle direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, in GUUE L 337, del 18 dicembre 2009, pag. 11 ss.

[209] Direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica, in GUUE L 337, del 18 dicembre 2009, pag. 37 ss.

[210] Regolamento (CE) n. 1211/2009 del Parlamento europeo e del Consiglio, del 25 novembre 2009, in GUUE L 337, del 18 dicembre 2009, pag. 1 ss.

[211] In GUUE C 308, del 18 dicembre 2009, pag. 2.

l'apertura e la neutralità di Internet, tenendo pienamente conto della volontà dei colegislatori di dichiarare la neutralità della rete come obiettivo politico e principio della regolamentazione che dovrà essere promosso dalle autorità nazionali di regolamentazione, rafforzare i correlati requisiti di trasparenza e conferire strumenti di salvaguardia alle autorità nazionali di regolamentazione per prevenire il degrado dei servizi e intralci o rallentamenti del traffico sulle reti pubbliche».

4.1. Il ruolo delle ONG e degli enti di standardizzazione

Come si è già accennato, il modello monistico di natura giuspositivistica, secondo cui tutte le norme sono produzione diretta o delegata dello Stato, è entrato in crisi. Si sta verificando un effetto irreversibile per cui la vita della comunità internazionale è sempre più interdipendente e gli Stati-nazione non sono più gli attori privilegiati. Sul piano del diritto, questa tendenza si traduce in una moltitudine di processi decentrati di produzione giuridica. Il fenomeno in esame, a cui alcuni si riferiscono con l'espressione "globalizzazione del diritto" e che trova fra i suoi primi casi la *lex mercatoria*[212], ha come conseguenza non «la creazione di un corpus unico di regole, ma la nascita o lo sviluppo di diversi ordinamenti, indipendenti da quelli statali, variamente intrecciati tra loro, che regolano differenti settori della vita sociale a livello transnazionale»[213]. Ciò è particolarmente vero per le attività di regolamentazione della Rete, che vedono maggiormente coinvolti nel processo di decision-making soggetti diversi dagli attori tradizionali, come le organizzazioni non governative (ONG) e i singoli individui.

Un esempio di produzione giuridica decentrata è la c.d. netiquette, ovvero quell'insieme di «regole che disciplinano il comportamento di un utente di Internet nei suoi rapporti con altri soggetti mediante strumenti come i newsgroup, le mailing list, i forum, i social network o semplicemente le mail»[214]. La maggior parte di queste regole viene formalizzata in testi denominati Requests For Comments (RFC) sulla base delle pratiche rivelatesi più efficaci.

[212] La *lex mercatoria* è un sistema di norme e regole di tipo consuetudinario, nate in forma spontanea tra gli appartenenti a determinati settori commerciali, finalizzato alla regolamentazione di rapporti contrattuali ed extracontrattuali aventi elementi di internazionalità.

[213] G. Pascuzzi, op. cit., pag. 277.

[214] G.M. Ruotolo, op. cit., pag. 29.

La redazione di tali documenti viene promossa dalla Internet Engineering Task Force (IETF) con lo scopo di farne veri e propri standard[215]. L'IETF è un'organizzazione internazionale non governativa che venne creata nel 1986 dal governo statunitense. Inizialmente costituita da tecnici e ricercatori, col tempo la sua composizione si è allargata a chiunque fosse interessato a titolo individuale all'evoluzione tecnologica del Web.

La standardizzazione tecnica della Rete viene sviluppata dall'IETF mediante la cooperazione con altre organizzazioni. Le più importanti sono l'Internet Research Task Force (IRTF)[216], il World Wide Web Consortium (c.d. W3C)[217], l'Internet Society (ISOC)[218] e l'International Organization for Standardization (ISO)[219].

Tra i documenti elaborati dai gruppi di lavoro istituiti in seno all'IETF, si distinguono, in base al loro successo nella comunità della Rete che ne condiziona la portata "normativa", i *proposed* standard, sufficientemente stabili ma non ancora abbastanza maturi per essere definitivamente formalizzati, i *draft* standard – hanno ottenuto almeno due implementazioni che ne hanno dimostrato la operatività – e gli standard veri propri, che richiedono la presenza di un numero significativo di applicazioni. I documenti che non vengono ritenuti idonei a divenire standard, invece, vengono classificati come *experimental*, qualora concernano oggetti in fase di sviluppo, *informational*, qualora contengano mere informazioni su un determinato argomento, *historic*, qualora contengano standard divenuti obsoleti, e *best common practice*, qualora si limitino a suggerire determinate modalità di configurazione.

[215] In tale contesto, l'espressione standard indica una normativa tecnica adottata per fissare i parametri più strettamente operativi e materiali dei comportamenti.

[216] L'IRTF promuove la ricerca dell'evoluzione di Internet creando gruppi di lavoro a lungo termine su argomenti relativi ai protocolli, alle applicazioni, all'architettura e alla tecnologia di Internet.

[217] Il W3C è un'ONG fondata nel 1994 presso il Massachusetts Institute of Technology che ha formalizzato tutti i principali protocolli che garantiscono la c.d. interoperabilità, cioè la comunicazione tra macchine diverse.

[218] L'ISOC è un'organizzazione non-profit fondata nel 1992 che assicura lo sviluppo, l'evoluzione e l'uso in modo aperto di Internet per il bene di tutte le persone nel mondo.

[219] L'ISO definisce ii nomi e i codici postali di Paesi, territori dipendenti e speciali aree di rilevanza geografica. Molti degli standard da essa promossi hanno poi assunto una portata vincolante sul piano del diritto internazionale, per essere stati incorporati in accordi internazionali, o sul piano del diritto interno, mediante il rinvio ad essi effettuato da norme nazionali.

5.1. La revisione delle International Telecommunication Regulations

Alla fine degli anni '80 si fece strada l'idea di redigere un trattato internazionale che potesse adeguatamente consentire agli operatori di telecomunicazioni di connettersi tra loro e sviluppare, di conseguenza, una rete di comunicazione di dimensioni planetarie. Nel 1988, l'Unione internazionale delle telecomunicazioni (ITU)[220] indisse pertanto la World Administrative Telegraph and Telephone Conference, che si concluse con l'adozione delle International Telecommunication Regulations (ITRs), sottoscritte da 178 paesi ed entrate in vigore nel 1990.

Le ITRs si proponevano di facilitare l'interoperatività delle attrezzature per le telecomunicazioni e di promuovere l'efficienza, l'utilità e la disponibilità al pubblico dei servizi di telecomunicazioni internazionali. Esse hanno costituito «il principale strumento internazionale di regolamentazione dell'interconnessione tra le diverse reti nazionali di telecomunicazioni preesistenti all'avvento di Internet, consentendo così la nascita di una rete "globale"»[221]. La nascita e lo sviluppo della Rete si devono anche ai meccanismi normativi previsti dalle ITRs, che fornivano un quadro di riferimento globale idoneo a garantire l'interoperabilità delle telecomunicazioni.

Le ITRs furono concepite in un momento in cui gli Stati erano gli unici fornitori di servizi di telecomunicazioni. Il mutato contesto in cui queste si sono trovate a operare, a seguito dei processi di privatizzazione e liberalizzazione dei mercati nazionali, ha spinto l'ITU a indire una nuova conferenza mondiale per la revisione delle ITRs.

---

[220] L'ITU ha sede a Ginevra. È stata fondata nel 1865 a Parigi come International Telegraph Union ed ha assunto il suo nome attuale nel 1932. A partire dal 1947 è entrata a far parte delle agenzie specializzate delle Nazioni Unite. Una delle sue funzioni principali è quella di favorire la cooperazione internazionale nel settore delle telecomunicazioni. La sua struttura istituzionale comprende la Conferenza dei plenipotenziari, il Consiglio e il Segretariato. La Conferenza dei plenipotenziari è un organo a composizione plenaria a competenza generale che si riunisce ogni cinque anni. Il Consiglio ha la funzione di garantire la continuità dell'amministrazione dell'attività dell'organizzazione ed è composta di rappresentanti degli Stati membri eletti dalla Conferenza e dotati di competenze individuali nel campo delle telecomunicazioni. L'ITU organizza periodicamente le c.d. Conferenze mondiali sulle telecomunicazioni, in cui gli Stati membri aggiornano gli impegni già assunti in questo settore e ne negoziano di nuovi. Le Conferenze di Nizza del 1989 e di Ginevra del 1992 hanno condotto all'adozione di una Costituzione ITU e di una Convenzione integrativa, che costituiscono i due atti fondamentali dell'organizzazione e devono essere ratificati congiuntamente dagli Stati membri. Ai sensi dell'art. 2 della Costituzione ITU, vengono previste due tipologie di membership: i membri a pieno titolo possono essere esclusivamente gli Stati, che detengono il potere di voto su ogni decisione da adottare in seno all'ITU; tra i *sector member*, che sono ammessi ad assistere ai lavori relativi ad argomenti generali e sono legittimati ad avanzare proposte con riguardo ai tre settori di competenza dell'organizzazione (comunicazioni radio, standardizzazione, sviluppo delle telecomunicazioni), rientrano organizzazioni con competenze in materia di telecomunicazioni, associazioni internazionali di operatori di settore e operatori commerciali di telecomunicazioni, sia pubblici che privati.

[221] G.M. Ruotolo, op. cit., pag. 107.

La World Conference on International Telecommunications (WCIT) si è tenuta a Dubai dal 3 al 14 dicembre 2012. La preparazione della Conferenza è stata affidata a un gruppo di lavoro del Consiglio dell'ITU, che l'11 luglio 2012 ha diffuso una bozza delle future ITRs. Alcune delle norme contenute nella bozza codificavano dei principi che sono al momento contenuti in strumenti giuridici non vincolanti, come l'obbligo di cooperazione nella gestione della Rete. In particolare, la proposta negoziale rubricata col numero ADD CWG/4/224, relativa alla riscrittura dell'art. 5 delle ITRs, prevedeva che gli Stati membri cooperassero fra di loro e con gli altri stakeholder al fine di rafforzare la sicurezza online, sviluppare una legislazione adeguata per le indagini e i procedimenti penali della criminalità cibernetica, prendere delle misure per combattere lo spam e assicurare la stabilità e la sicurezza di Internet, proteggendo e rispettando le norme sulla privacy e sulla libertà d'espressione contenute nella Dichiarazione universale dei diritti dell'uomo.

Da più parti si temeva, tuttavia, che estendere l'applicazione delle ITRs al Web potesse significare l'assoggettamento di Internet al principio del *sending network pays*, con il conseguente incremento dei costi di connessione. In base a questo principio, il gestore della rete nazionale che affida determinati dati a un'altra rete per la loro consegna al destinatario è gravato dal versamento di una *fee*.

Anche gli Stati Uniti hanno assunto una posizione fortemente contraria rispetto all'esplicita estensione delle ITRs a Internet: nella loro visione, Internet si è sviluppato per operare in un ambiente separato e distinto che va oltre lo scopo o mandato delle ITRs o dell'ITU, e lo sviluppo di un regime regolatorio formale rischierebbe di minare la crescita di Internet, inteso come rete decentralizzata di reti che ha conseguito l'interconnessione globale in completa autonomia.

Il 14 dicembre 2012 la WCIT si è conclusa con la firma degli accordi di modifica delle ITRs[222]. Il nuovo trattato, piuttosto vago, è entrato in vigore nel 2015 ed è stato sottoscritto da 89 membri delle Nazioni Unite, fra cui i Paesi BRICS (Brasile, Russia, India, Cina, Sudafrica), gli Stati CSI e l'Arabia Saudita, contrari al monopolio statunitense di Internet. Altri 55 membri dell'ONU, fra cui Stati Uniti, Regno Unito, Australia e Canada, ne hanno apertamente contestato l'adozione, adducendo che il trattato rappresenti un mezzo per censurare Internet da parte dei governi non democratici; per loro rimarranno in vigore le regole risalenti al 1988. Anche Google si è schierata a favore dei

[222] Gli atti finali della conferenza sono disponibili all'indirizzo www.itu.int/pub/S-CONF-WCIT-2012/en.

Paesi che si sono rifiutati di firmare il trattato, dichiarandosi a favore di una Rete libera e aperta.

Nell'affermare l'importanza della Rete quale elemento centrale dell'infrastruttura della società dell'informazione, il trattato si limita a ribadire i principi contenuti nella Dichiarazione di Ginevra e nell'Agenda di Tunisi, fra cui quello per cui tutti i governi sono ugualmente importanti per garantire la stabilità, la sicurezza, la continuità e il futuro sviluppo della Rete. Agli Stati è rivolto l'invito ad approfondire le proprie posizioni sulle questioni internazionali relative a Internet in occasione dei vari forum preparati dall'ITU (come il World Telecommunication/ICT Policy Forum, la Broadband Commission for Digital Development e i gruppi di studio in seno all'ITU) e sotto il suo mandato. Il Segretario generale dell'ITU viene incaricato di continuare a muovere i passi necessari perché l'organizzazione giochi un ruolo attivo e costruttivo all'interno del modello multistakeholder di Internet, e di supportare la partecipazione degli Stati membri e tutti gli altri attori nelle attività dell'Unione.

Stando così le cose, ad oggi non esiste ancora un trattato per regolare in modo condiviso le questioni relative alle reti di telecomunicazioni, e Internet specialmente. Una cortina divide i Pesi che hanno firmato gli accordi di revisione delle ITRs da coloro che non l'hanno fatto.

6.1. La categoria dei beni patrimonio comune dell'umanità

La mancanza di norme pattizie specificamente rivolte a regolare il funzionamento di base di Internet, tuttavia, non esclude la possibilità che norme di diritto internazionale consuetudinario preesistenti all'avvento di Internet per disciplinare fattispecie da questa differenti possano, in considerazione del loro oggetto e del loro scopo, essere applicate alla Rete. Le norme che più di altre si prestano a questo impiego sono quelle nate per disciplinare l'uso da parte degli Stati di risorse su cui non è possibile esercitare in maniera esclusiva il diritto di sovranità e il cui sfruttamento presuppone il possesso di elevate competenze tecnologiche, ovvero le norme relative ai beni patrimonio comune dell'immunità.

La nozione di patrimonio comune dell'umanità, che si fonda su quella di *res communis omnium* elaborata da Grozio nel XVII secolo, è stata riattualizzata nel 1967 in occasione della Terza conferenza delle Nazioni Unite sul diritto di mare a seguito del discorso pronunciato dal rappresentante maltese Arvid Pardo: la risoluzione 25/2749

dell'Assemblea generale, del 17 dicembre 1970, e la Convenzione di Montego Bay sul diritto del mare del 1982 dichiarano che i fondi marini e i loro sottosuoli oltre i limiti delle giurisdizioni nazionali sono patrimonio comune dell'umanità.

Prima di allora, il medesimo concetto, benché non ancora definito in questi termini, era apparso nel Trattato sull'Antartide del 1959, finalizzato a garantire nell'interesse del genere umano che l'Antartide continui ad essere usato esclusivamente per scopi pacifici e che non divenga oggetto di contesa internazionale, e nel Trattato del 1967 relativo alle attività degli Stati nell'esplorazione e l'utilizzazione dello spazio, le cui norme impongono il divieto agli Stati firmatari di stazionare armi nucleari e ogni altro genere di armi di distruzione di massa nello spazio extra-atmosferico e proibiscono espressamente di rivendicare risorse poste nello spazio.

Applicazioni più recenti di questo principio sono contenute nel Trattato relativo alle attività degli Stati sulla Luna e gli altri corpi celesti del 1979, che vieta ad ogni Stato di dichiarare la propria sovranità su qualsiasi territorio dei corpi celesti e richiede che tutte le estrazioni di risorse siano svolte sotto regime internazionale, nonché nella Dichiarazione universale sul genoma umano adottata dall'UNESCO l'11 novembre 1997, il cui art. 4 ne proibisce la commercializzazione.

Sono state identificate cinque componenti essenziali del concetto di patrimonio comune dell'umanità: i beni patrimonio dell'umanità non possono essere oggetto di appropriazione da parte degli Stati; le loro risorse devono essere gestite collettivamente; i benefici acquisiti dal loro sfruttamento devono essere condivisi fra tutte le nazioni; devono essere utilizzati solo per scopi pacifici; devono essere preservati nell'interesse delle future generazioni[223].

6.2. (segue): Internet come patrimonio comune dell'umanità

Il primo ad avanzare la proposta di proclamare Internet patrimonio dell'umanità è stato il giurista Arroyo sulle pagine di El País[224], in cui afferma che, se i problemi relativi ad Internet e alle sue applicazioni non verranno risolti in modo condiviso, verranno messi a repentaglio la comunicazione umana senza frontiere, l'accesso libero e gratuito alla cultura e al sapere, l'esercizio della libertà di espressione; per questo motivo ritiene doveroso

[223] Cfr. J. Frakes, *The common heritage of mankind principle and the deep seabed, outer space, and Antarctica: will developed and developing Nations reach a compromise?*, in *Wisconsin International Law Journal*, 2003, pag. 409.

[224] Cfr. I. Arroyo Martínez, *Descargas en Internet*, 23 dicembre 2009, elpais.com/diario/2009/12/23/opinion/1261522804_850215.html.

convocare una conferenza internazionale con l'obiettivo di arrivare a una convenzione sul Web.

Naturalmente, l'estensione ad Internet di obblighi di diritto internazionale a esso preesistenti deve rispettare la logica delle c.d. geometrie variabili, in base a cui materie differenti vanno trattate diversamente sula base delle loro disuguaglianze. Il principio di non appropriazione verrebbe così interpretato nel senso d'impedire a ogni Stato di trattare la Rete come se fosse sottoposta alla propria giurisdizione e di realizzare azioni che non permettano agli altri Stati di utilizzarla. Si ammetterebbe poi l'esistenza di un divieto in capo a tutti gli Stati di compiere qualsiasi genere di atto che possa mettere in pericolo l'efficienza del sistema. Analogamente, l'obbligo di cooperazione dovrebbe essere inteso come l'impegno positivo, da parte degli Stati, a creare meccanismi o utilizzare fora già esistenti per discutere delle tematiche legate all'uso di Internet.

6.3. (segue): il divieto di inquinamento

In base al Principio n. 21 della Dichiarazione di Stoccolma, adottata al termine della Conferenza delle Nazioni Unite del 1973 sull'Ambiente Umano, gli Stati hanno, in conformità con la carta delle Nazioni Unite e i principi di diritto internazionale, il diritto sovrano di sfruttare le proprie risorse secondo le proprie politiche ambientali, e la responsabilità di assicurare che le attività svolte all'interno della loro giurisdizione o sotto il loro controllo non arrechino danni all'ambiente degli altri Stati o di aree oltre i confini della giurisdizione nazionale .

La Dichiarazione di principi di Stoccolma, benché non costituisca una fonte di diritto internazionale vincolante, riconosce per la prima volta l'esistenza di un divieto gravante sugli Stati di mettere in atto comportamenti che danneggino un dato ambiente naturale, alterandone gli equilibri. Esso non varrebbe solo per le zone sottoposte alla sovranità di altri soggetti di diritto internazionale, ma anche per quelle che non sono sottoposte alla sovranità di alcuno Stato, ovvero le zone dichiarate bene comune dell'umanità. La Convenzione di Montego Bay sul diritto del mare del 1982 provvede poi a conferire al divieto di inquinamento una portata positiva, prescrivendo agli Stati di adottare misure preventive e repressive dell'inquinamento stesso.

Nel rispetto della logica delle geometrie variabili, l'applicazione del divieto d'inquinamento a Internet impedirebbe la diffusione diretta da parte degli Stati di strumenti, quali software malevoli, in grado di alterare l'ambiente informatico e porre in pericolo

l’esistenza stessa della Rete, e imporrebbe l’attuazione di misure nazionali preventive e repressive per impedire la trasmissione di strumenti siffatti da parte dei privati.

* * *

La ricerca di una disciplina giuridica per la Rete ha evidenziato la contrapposizione, nell’ordinamento internazionale, tra la povertà di fonti vincolanti e l’abbondanza di fonti non vincolanti specificamente volte a imporre agli Stati determinati comportamenti rispetto all’uso di Internet. La prevalenza di fonti non vincolanti, come gli atti di soft law delle organizzazioni internazionali e i codici di condotta delle multinazionali, è un indicatore del coinvolgimento nella governance di Internet di una pluralità di attori, sia di rilevanza pubblicistica, sia di rilevanza privatistica, ognuno dei quali è chiamato a offrire il proprio contributo nel rispettivo ambito di competenza. La mancanza di obbligatorietà di queste fonti non rappresenta tuttavia un limite alla loro efficacia: in primo luogo, la regolazione di alcuni aspetti di Internet potrebbe addirittura limitarne l’utilità; in secondo luogo, è più facile costruire una regola non vincolante, poiché non si pone il problema di imporne l’applicazione; in terzo luogo, la flessibilità di una norma di soft law ne consente variazioni senza grandi difficoltà, e, se la regola è già buona, la sua applicazione può rappresentare il primo passo verso la creazione di una norma vincolante.

APPENDICE II

Internet e i diritti umani

Il rapporto intercorrente tra Internet e i diritti umani va analizzato in una duplice ottica: se, da un lato, la Rete costituisce l'*enabler* di alcuni diritti, quali le libertà d'espressione e d'informazione[225], dall'altro lato, l'accesso a Internet potrebbe configurarsi esso stesso come un autonomo diritto di ultima generazione (quarta)[226].

1. La tutela dei diritti digitali

Nel contesto delle nuove tecnologie, e specialmente di Internet, si usa il termine "diritti digitali" per indicare i diritti umani già esistenti che consentono agli individui di creare e pubblicare contenuti digitali, e di accedere agli stessi, o di usare apparecchi elettronici, come i computer, e le reti di telecomunicazioni. Quella dei diritti digitali è una categoria giuridica assai eterogenea, che ricomprende al suo interno la libertà di associazione, la protezione dei dati personali, il diritto all'educazione ecc. Al di sopra di tutti gli altri diritti rilevanti in ambito digitale, spiccano, per la loro rilevanza, la libertà di espressione e informazione, il diritto allo sviluppo[227] e la tutela della privacy.

1.1. La libertà di espressione online nella prassi delle OO.II…

Nell'ordinamento internazionale, la libertà di espressione è disciplinata dall'art. 19 del Patto sui diritti civili e politici. L'art. 19 sancisce, al primo comma, il diritto individuale di formarsi un'opinione, e, al secondo comma, il diritto di esprimersi liberamente:

[225] Cfr. G.M. Ruotolo, op. cit., p. 113.

[226] La dottrina distingue tra i diritti umani di prima generazione (civili e politici), di seconda generazione (economici e sociali) e di terza generazione (quelli relativi alla bioetica, alla genetica, alle nuove tecnologie in genere).

[227] Il diritto allo sviluppo è abitualmente assimilato al diritto di partecipazione alla vita culturale, tutelato dall'art. 15 del Patto sui diritti economici, sociali e culturali: «1. Gli Stati parte del presente Patto riconoscono il diritto di ogni individuo: […] (b) a godere dei benefici del progresso scientifico e delle sue applicazioni». Internet costituisce una delle maggiori applicazioni del progresso scientifico cui fa riferimento la disposizione. Nella risoluzione 66/184, del 22 dicembre 2011, l'Assemblea generale ha riconosciuto alle tecnologie dell'informazione la capacità di fornire nuove soluzioni alle sfide per lo sviluppo e promuovere una crescita economica equa e sostenibile, competitività, l'accesso alla conoscenza, l'eradicazione della povertà e l'inclusione sociale, al fine di accelerare l'integrazione dei Paesi meno sviluppati nell'economia globale.

1. Ogni individuo ha diritto a non essere molestato per le proprie opinioni.
2. Ogni individuo ha il diritto alla libertà di espressione; tale diritto comprende la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, senza riguardo a frontiere, oralmente, per iscritto, attraverso la stampa, in forma artistica o attraverso qualsiasi altro mezzo di sua scelta.

Con specifico riguardo al settore delle telecomunicazioni, l'art. 3.4 delle ITRs del 1988 garantisce il diritto di "inviare traffico", il quale va sostanzialmente interpretato come l'applicazione del diritto alla libertà di comunicazione e informazione tramite le reti internazionali di telecomunicazioni.

Il diritto di accedere ai servizi internazionali di telecomunicazioni è riconosciuto anche dalla Costituzione ITU, il cui art. 33 (The Right of the Public to Use the International Telecommunications Service) prevede che gli Stati membri riconoscano il diritto degli utenti di comunicare tramite i mezzi del servizio internazionale della pubblica corrispondenza, e che i servizi, le tasse e le garanzie siano uguali per tutti gli utenti in ogni categoria di corrispondenza, senza alcuna priorità o preferenza.

Così formulate, queste disposizioni furono concepite, sin dal momento della loro redazione, perché includessero «anche tutti i futuri mezzi tecnologici idonei a consentire l'esercizio dei diritti tutelati»[228]. Un simile accorgimento normativo renderebbe del tutto superfluo qualsivoglia aggiustamento al quadro normativo internazionale, preesistente all'avvento di Internet, volto a prescrivere la vigenza delle disposizioni sulla libertà di espressione anche sul Web. Questo assunto viene confermato dalla prassi recente di numerosi organi delle Nazioni Unite competenti in materia di diritti umani.

Nel 2009, il Consiglio dei diritti dell'uomo[229] ha adottato una risoluzione[230] con la quale, dopo aver ricordato agli Stati gli obblighi assunti con la ratifica del Patto sui diritti civili e politici, ha chiesto loro di farsi promotori di un accesso diffuso alle nuove tecnologie di comunicazione, riconoscendo il contributo che l'esercizio del diritto di

[228] G.M. Ruotolo, op. cit., p. 115.

[229] Con la risoluzione 60/251 dell'Assemblea generale, del 3 aprile 2006, il Consiglio ha sostituito la vecchia Commissione per i diritti dell'uomo. A differenza di quest'ultima, il Consiglio è un organismo più snello (conta 47 membri anziché 53) e incisivo. Esso viene eletto direttamente dall'Assemblea generale a maggioranza dei membri della stessa. Oltre ad assumere i mandati e le responsabilità precedentemente spettanti alla Commissione, il Consiglio può formulare raccomandazioni all'Assemblea generale ai fini di promuovere lo sviluppo del diritto internazionale e svolge una revisione universale periodica in relazione al rispetto degli obblighi internazionali in materia di diritti dell'uomo.

[230] Risoluzione 12/16 del Consiglio dei diritti dell'uomo, *Freedom of opinion and expression*, A/HRC/12/16 (2 ottobre 2009).

espressione, in modo particolare attraverso i media, incluso per mezzo delle ICT, come Internet, e il pieno rispetto per la libertà di cercare, ricevere e impartire informazioni possono apportare alla lotta contro il razzismo e alla prevenzione degli abusi dei diritti umani.

Il rapporto[231] che Frank La Rue, il Relatore speciale sulla promozione e protezione del diritto alla libertà di espressione e opinione, ha inviato al Consiglio dei diritti dell'uomo, in adempimento di una sua risoluzione[232], ribadisce l'importanza che riveste Internet nella realizzazione del diritto alla libertà di espressione, la quale a sua volta permette il godimento di altri diritti fondamentali. Internet, poi, consente agli individui di cercare, ricevere e divulgare informazioni oltre le frontiere nazionali in maniera istantanea ed economica, stimola lo sviluppo economico, sociale e politico, e contribuisce al progresso del genere umano in generale.

Il Comitato dei diritti dell'uomo[233], nel corso della sua 102° sessione, ha confermato che l'art. 19, secondo comma, del Patto tutela tutte le forme di audiovisivo, così come i modi di espressione elettronici e basati su Internet[234].

Nel luglio 2011, l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) ha pubblicato un rapporto[235] che esamina la regolazione di Internet negli Stati membri. Nelle sue conclusioni, viene riconfermata l'applicazione della libertà di espressione a tutti i mezzi di comunicazione, incluso Internet. Pertanto, le restrizioni a questo diritto, anche quando si realizza attraverso le nuove tecnologie, sono accettabili solo se in conformità con le norme e gli standard internazionali e devono essere valutate in rapporto

---

[231] Risoluzione 17/27 del Consiglio dei diritti dell'uomo, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue,* A/HRC/17/27 (16 maggio 2011).

[232] Risoluzione 7/36 del Consiglio dei diritti dell'uomo, *Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/7/36 (28 marzo 2008).

[233] Il Comitato per i diritti dell'uomo è stato istituito dal Patto sui diritti civili e politici (art. 26) ed è l'organo di controllo sull'esecuzione degli obblighi convenzionali. Il Comitato esamina il rapporto che ciascuno Stato contraente deve presentare periodicamente, indicando i motivi di eventuali divergenze della legislazione interna rispetto alle disposizioni del Patto (art. 40). Al termine dell'esame il Comitato può formulare dei "rapporti" e "osservazioni generali", a cui lo Stato può replicare. Qualora gli Stati abbaino accettato la competenza del Comitato a ricevere ed esaminare "comunicazioni" (una sorta di ricorso) di uno Stato contro un altro che abbia violato il Patto, il Comitato favorisce una soluzione amichevole e redige un rapporto, altrimenti designa una Commissione di conciliazione ad hoc (artt. 41, 42). Il Protocollo facoltativo al Patto sui diritti civili e politici riconosce (art. 1) la competenza del Comitato a ricevere ed esaminare "comunicazioni" provenienti da individui, cittadini, o no, dello Stato parte contraente del Patto o del Protocollo, riguardanti la violazione di qualsiasi diritto enunciato nel Patto stesso.

[234] Cfr. Nazioni Unite, Comitato per i diritti dell'uomo, *General comment No. 34. Article 19: Freedoms of opinion and expression*, CCPR/C/GC/34 (12 settembre 2011), par. 12.

[235] Y. Akdeniz, *Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States*, 11 luglio 2011, www.osce.org/files/f/documents/e/f/80723.pdf.

al pubblico interesse. Yaman Akdeniz, autore del rapporto OSCE, si spinge addirittura ad affermare che l'accesso a Internet dovrebbe essere riconosciuto un diritto dell'uomo in sé, in quanto costituisce il requisito principale per partecipare alla Società dell'Informazione e per godere del diritto alla libertà di espressione e del diritto a inviare e ricevere informazioni senza riguardo alle frontiere[236].

Nel 2012, il Consiglio dei diritti dell'uomo delle Nazioni Unite ha chiarito definitivamente che gli stessi diritti che le persone hanno offline devono essere protetti anche online, in particolare la libertà di espressione[237]. È l'ammissione della necessità di adottare misure di protezione di tali diritti da illegittime limitazioni statali dell'accesso a Internet. La risoluzione riconosce altresì la natura globale e aperta di Internet, come forza motrice nell'accelerare il progresso verso lo sviluppo nelle sue varie forme, e invita gli Stati a promuovere e facilitare l'accesso a Internet e la cooperazione internazionale finalizzata allo sviluppo dei media e delle strutture dell'informazione e della comunicazione in tutto il mondo.

1.2. …e nella giurisprudenza della Corte EDU

Negli ultimi anni, la Corte europea dei diritti dell'uomo (Corte EDU) si è occupata più volte del rapporto tra libertà di espressione e nuove tecnologie. All'interno della CEDU, la libertà di espressione è enunciata dall'art. 10, il quale illustra, al secondo comma, anche le condizioni che devono essere soddisfatte da eventuali misure statali legittime di restringere la libertà in questione:

> 1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi posa essere ingerenza da parte delle autorità pubbliche e sena limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive.
> 2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario».

[236] Cfr. ivi, pag. 34.

[237] Cfr. risoluzione 20/8 del Consiglio dei diritti dell'uomo, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/8 (5 luglio 2012).

Una svolta importante nella giurisprudenza della Corte EDU in materia di libertà di espressione è rappresentata dalla decisione relativa alla causa *Times Newspaper Ltd* c. *Regno Unito*[238], in cui si ammette che Internet, in vista della sua accessibilità e del ruolo che gioca e nel facilitare la divulgazione delle notizie, debba essere considerato a tutti gli effetti un mezzo tutelato dalla CEDU al fine di impartire informazioni al pubblico[239].

Nel 2010, la Corte EDU ha rinvenuto per la prima una violazione dell'art. 10 CEDU all'interno di una fattispecie collegata a Internet[240], a seguito del ricorso di Patrice Renaud dopo la sua condanna nel 2005 per aver diffamato e insultato pubblicamente il sindaco di Sens sul sito Internet dell'associazione di cui era presidente e webmaster: il signor Renaud aveva insinuato che il sindaco stesse stimolando e incoraggiando la delinquenza in città al fine di legittimare la propria politica di sicurezza, e l'articolo in cui descriveva il primo cittadino come cinico, schizofrenico e bugiardo era stato ritenuto un pubblico insulto. Per questi motivi, il ricorrente era stato costretto a pagare un'ammenda di 500 euro e altri 1.000 euro di danni civili al sindaco. La Corte ha riconosciuto che, per quanto la fraseologia del signor Renaud fosse particolarmente polemica e aggressiva, egli, nel momento in cui criticava l'operato del sindaco, stava partecipando a un dibattito pubblico, essenziale per il corretto funzionamento di una democrazia, ed ha sostenuto che gli eletti devono far prova di una tolleranza particolare quanto alle critiche di cui essi sono l'oggetto e, all'occorrenza, agli straripamenti verbali o scritti che le accompagnano. Tenuto conto dell'interesse della società democratica ad assicurare e a mantenere la libertà d'espressione, la Corte ha ritenuto che la sanzione imposta al signor Renaud fosse stata sproporzionata rispetto al fine legittimo di proteggere la reputazione e i diritti altrui, e ha pertanto riscontrato una violazione dell'art. 10 CEDU.

Nel 2011, la Corte EDU ha chiesto l'immunità per i giornalisti che riprendono notizie tratte da Internet e le pubblicano con una precisa citazione della fonte, condannando l'Ucraina per una doppia violazione dell'art. 10 della CEDU[241]. Alla Corte di Strasburgo si erano rivolti il comitato editoriale e il redattore capo del giornale ucraino Pra-

[238] Corte EDU 10 marzo 2009, ricorsi n. 3002/03 e 23676/03, *Times Newspaper Ltd* c. *Regno Unito*.

[239] Cfr. ivi, par. 37.

[240] Cfr. Corte EDU 25 febbraio 2010, ricorso n. 13290/07, *Patrice Renaud* c. *Francia*.

[241] Cfr. Corte EDU 5 maggio 2011, ricorso n. 33014/05, *Comitato editoriale di Pravoye Delo e Shtekel* c. *Ucraina*.

voye Delo, su cui era stata pubblicata una lettera anonima tratta da un sito Internet. L'autore della lettera, un presunto impiegato dei servizi di sicurezza ucraini, affermava che alti funzionari del dipartimento dei servizi di sicurezza della regione di Odessa erano stati coinvolti in fatti di corruzione e in altre attività delittuose, di concerto con esponenti della criminalità organizzata. Nella lettera compariva anche il nome del presidente della federazione nazionale ucraina di thai boxing, che aveva citato in giudizio la rivista, che era stata condannata a pubblicare una rettifica, una lettera di scuse e a corrispondere oltre 2.000 euro di danni.

La Corte EDU, dopo aver osservato che le decisioni dei tribunali interni interferivano con il diritto alla libertà di espressione dei ricorrenti, ha esaminato se le misure in questione fossero giustificate in conformità all'art. 10, secondo comma, della CEDU. Questo prescrive che ogni restrizione al diritto alla libertà di espressione deve essere prevista per legge. È stata così accertata una prima violazione dell'art. 10 CEDU, dal momento che l'obbligo di pubblicazione delle scuse, a cui è stato condannato il caporedattore del giornale, non era una misura prevista dal diritto ucraino.

La Corte ha successivamente ripreso quanto affermato da giudici interni, ovvero che nella legislazione ucraina non è sancita un'esclusione della responsabilità civile nei procedimenti per diffamazione per i giornalisti che utilizzano informazioni pubblicate su Internet, diversamente da quanto previsto per i giornalisti che pubblicano notizie da altri giornali. La Corte ha quindi rilevato che proprio la mancanza di garanzie per i giornalisti che utilizzano le informazioni tratte da Internet dia luogo a una seconda violazione dell'art. 10 CEDU: considerata l'importanza che riveste Internet nel contesto delle attività dei media professionali e la sua rilevanza per l'esercizio del diritto alla libertà di espressione in generale, l'assenza di un sufficiente quadro normativo a livello nazionale che consenta ai giornalisti di usare informazioni ottenute online senza paura di incorrere in sanzioni ostacola gravemente la funzione di sorveglianza esercitata della stampa.

La Corte ha infine affermato che i tribunali nazionali non avevano adeguatamente preso in considerazione la circostanza, contemplata dal diritto ucraino, per cui non possono essere chiamati a rispondere di diffamazione i giornalisti che abbiano agito in buona fede e senza l'intenzione di diffondere notizie false. Inoltre, l'assenza di una normativa chiara impediva di sostenere che i ricorrenti potessero prevedere le conseguenze che la pubblicazione in questione avrebbe comportato. Per questi motivi, la Corte ha condannato lo Stato ucraino al pagamento di 6.000 euro come risarcimento al redattore capo di Pravoye Delo.

Nella causa *Yildirim* c. *Turchia*[242], la Corte EDU ha fatto luce sul margine di discrezionalità concesso agli Stati negli interventi che limitano l'accesso a Internet. Il 23 giugno 2009, la Corte criminale di prima istanza di Denizli aveva oscurato, come misura preventiva, un sito Internet il cui proprietario aveva pubblicato alcuni testi che, secondo le autorità giudiziarie turche, offendevano la memoria di Atatürk. L'ordine di bloccare il sito era stato inviato per l'esecuzione al Telecommunications Directorate (TIB). Quest'organi aveva successivamente chiesto al tribunale di estendere lo scopo del suo mandato per interrompere anche l'accesso a Google Sites, che ospitava non solo il sito in questione, ma anche quello del ricorrente alla Corte EDU. Il TIB aveva sostenuto che si trattava dell'unico mezzo tecnico per rendere effettivo il blocco del sito incriminato, dal momento che il suo proprietario viveva all'estero. La Corte di Denizli aveva accolto la richiesta e il TIB, bloccando tutti gli accessi a Google Sites, aveva impedito al docente turco Ahmet Yildirim di accedere al proprio sito, benché esso non fosse in alcun modo coinvolto nel procedimento giudiziario del caso.

La Corte EDU, cui si è appellato Yildirim, ha affermato che una restrizione dell'accesso a una fonte di informazioni non è necessariamente incompatibile con la CEDU, a condizione che una precisa cornice legale regoli lo scopo del divieto, e garantisca la *judicial review* per prevenire eventuali abusi. In virtù della legge n. 5651, contenuta nell'ordinamento turco, un tribunale può ordinare che venga bloccato l'accesso al contenuto di un sito Internet se sussistono ragioni sufficienti per sospettare che esso dia origine a un reato. La legge non prevedeva, tuttavia, una così ampia sospensione dell'accesso come quella ordinata dal giudice, né autorizzava il blocco di un intero dominio Internet come Google Sites. Inoltre, la Corte di Denizli, quando aveva deciso di bloccare tutti gli accessi a Google Sites, non si era preoccupata di verificare l'esistenza di misure di portata minore per bloccare specificamente l'accesso del sito sotto accusa. La misura adottata dal tribunale turco era pertanto stata arbitraria e la *judicial review* era stato insufficiente a prevenire gli abusi. La Corte di Strasburgo ha conseguentemente constatato una violazione dell'art. 10 CEDU e imposto alla Turchia il versamento di 7.500 euro per i danni non patrimoniali subiti dal ricorrente.

[242] Corte EDU 18 dicembre 2012, ricorso n. 3111/10, *Ahmet Yildirim* c. *Turchia*.

1.3. Il divieto dei filtri antipirateria nella giurisprudenza della CGUE

Nel 2011, la Corte di giustizia dell'Unione europea (CGUE) ha preso una decisione storica in direzione della protezione dei diritti e delle libertà su Internet, segnatamente la tutela della privacy e la libertà di ricevere e scambiare informazioni. Il caso ha origine nel 2004, quando i rappresentanti legali della SABAM, corrispettivo belga della SIAE, avevano accusato il provider locale Tiscali, successivamente diventato Scarlet Extended SA, di aver lucrato sulle violazioni del diritto d'autore commesse dai suoi abbonati, interessati alle attività di condivisione illecita dei contenuti. Il giudice locale aveva dichiarato l'Internet provider responsabile delle violazioni commesse dai suoi utenti e lo aveva obbligato a dotarsi, entro sei mesi, delle tecnologie necessarie a bloccare l'accesso ai siti impegnati in attività illegali di file sharing. Per ogni giorno di ritardo nell'implementazione dei meccanismi di filtraggio, il provider avrebbe dovuto pagare una sanzione pecuniaria pari a 2.500 euro. Nel 2008 un tribunale di Bruxelles aveva bloccato le sanzioni a carico di Scarlet per l'inefficacia della tecnologia di filtraggio prevista dai vertici della SABAM e prodotta dalla società Audible Magic: essa non distingueva al meglio tra materiale lecito e illecito; in aggiunta, gli abbonati non potevano sottrarsi alle attività di monitoraggio delle loro attività.

Agli inizi del 2010, la Corte d'appello di Bruxelles ha proposto alla CGUE una domanda di pronuncia pregiudiziale sulla questione. Con la sentenza emessa l'ano successivo[243], la CGUE, considerando che la tutela del diritto fondamentale di proprietà deve essere bilanciata con quella di altri diritti fondamentali e che è compito dei giudici nazionali operare un giusto equilibrio, ha stabilito che il sistema di filtraggio imposto a Scarlet, che prevedeva un controllo indiscriminato di tutte le comunicazioni elettroniche dei suoi clienti, violava i loro diritti e la legge comunitaria:

> Pertanto, occorre dichiarare che, adottando l'ingiunzione che costringe il FAI a predisporre il sistema di filtraggio controverso, il giudice nazionale in questione non rispetterebbe l'obbligo di garantire un giusto equilibrio tra, da un lato, il diritto di proprietà intellettuale, e, dall'altro, la libertà di impresa, il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni[244].

[243] CGUE 24 novembre 2011, causa C-70/10, *Scarlet Extended SA* c. *Société belge des auteurs, compositeurs et éditeurs SCRL*.

[244] Ivi, par. 53.

Nel 2012, la CGUE ha confermato il proprio orientamento in una causa che ha visto nuovamente coinvolta la SABAM. Nel giugno 2009 i vertici della SABAM avevano chiesto al Tribunale di primo grado di Bruxelles un'ingiunzione per costringere la Netlog NV a interrompere immediatamente le attività di condivisione delle opere musicali o audiovisive sui profili degli utenti iscritti al social network. Il tribunale aveva azionato un rinvio pregiudiziale dinanzi alla CGUE per esaminare se le richieste della SABAM, volte ad affidare a un intermediario l'attività di sorveglianza e monitoraggio delle attività degli utenti, non andassero contro la Direttiva europea sul commercio elettronico[245].

Nella sentenza depositata il 16 febbraio 2012[246], la CGUE, riscontrando che l'ingiunzione di predisporre il sistema di filtraggio controverso obbligherebbe il prestatore di servizi di hosting a procedere a una sorveglianza generalizzata e illimitata nel tempo, ha stabilito che le esigenze di tutela dei diritti fondamentali ostano a un simile obbligo:

> 49. Infatti, l'ingiunzione di predisporre il sistema di filtraggio controverso implicherebbe, da un lato, l'identificazione, l'analisi sistematica e l'elaborazione delle informazioni relative ai profili creati sulla rete sociale dagli utenti della medesima, informazioni, queste, che costituiscono dati personali protetti, in quanto consentono, in linea di principio, di identificare i suddetti utenti.
> 50. Dall'altro, detta ingiunzione rischierebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto illecito ed un contenuto lecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito. Infatti, è indiscusso che la questione della liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto d'autore che variano da uno Stato membro all'altro. Inoltre, in determinati Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea a titolo gratuito da parte dei relativi autori.

2. Il diritto all'accesso a Internet

In un articolo pubblicato nel 2009 sul sito web del New York Times[247], Eric Pfanner si domandava se l'accesso a Internet fosse da considerare un diritto umano fondamentale, o piuttosto un privilegio che porta con sé la responsabilità di una buona condotta. D'al-

[245] CGUE 16 febbraio 2012, causa C-360/10, *SABAM* c. *Netlog NV*.

[246] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000.

[247] E. Pfanner, *Should Online Scofflaws Be Denied Web Access?*, 12 aprile 2009, www.nytimes.com/2009/04/13/technology/internet/13iht-piracy13.html.

tronde, se da una parte Internet migliora le condizioni di esercizio di alcune libertà "classiche", dall'altra offre nuovi strumenti per metterle a repentaglio. Proprio l'esigenza di combattere i fenomeni criminali online (pirateria informatica, violazione della privacy, pedopornografia) è uno degli elementi che si oppongono maggiormente alla tesi che invoca il conferimento all'accesso a Internet dello status di diritto fondamentale.

Invero, i rischi che provengono da un uso illecito di Internet non possono certamente compensare l'insieme dei vantaggi di cui l'umanità ha potuto beneficiare con l'avvento della Rete: Internet ha cambiato il modo di comunicare, ha influenzato l'economia, la politica e il diritto, ha abbassato le barriere spaziali e temporali, ha intensificato lo scambio di conoscenze grazie alla sua libertà da forme di proprietà. Del resto, negli ultimi anni si è registrato un numero crescente di richieste che si levano per far riconoscere l'accesso a Internet come diritto fondamentale. I risultati di alcune indagini condotte tra il 2009 e il 2012 testimoniano chiaramente questa volontà da parte della società.

In un sondaggio realizzato da BBC World Service dal 30 novembre 2009 al 7 febbraio 2010 su un campione di 27.973 adulti in 26 paesi, inclusi 14.306 utenti Internet, è emerso che quasi quattro intervistati su cinque consideravano l'accesso a Internet un diritto fondamentale: il 50% era assolutamente d'accordo, il 29% era abbastanza d'accordo, il 9% non era d'accordo, il 6% era fortemente in disaccordo, e il restante 6% non lo sapeva[248].

In un'altra serie di interviste condotte online dall'ISOC nel luglio e nell'agosto 2012 su più di 10.000 utenti Internet in 20 paesi, rispetto alla frase «L'accesso ad Internet dovrebbe essere considerato un diritto umano primario», l'83% dei partecipanti ha risposto di essere d'accordo, il 14% ha risposto di non essere d'accordo, e il 3% non ha risposto[249].

Queste cifre, insieme ad alcune decisioni pronunciate da giudici interni e alle norme di alcuni ordinamenti nazionali, fotografano una realtà che sta evolvendo, una nuova dimensione in cui Internet è considerato qualcosa di più di un semplice mezzo di comunicazione. Eppure, ad oggi non si può ancora davvero parlare di un diritto autonomo all'accesso a Internet, men che meno nei termini di un diritto fondamentale.

---

[248] Cfr. BBC, *Internet access is 'a fundamental right'*, 8 marzo 2010, news.bbc.co.uk/2/hi/8548190.stm.

[249] Cfr. Internet Society, *Global Internet User Survey*, 20 novembre 2012, wayback.archive-it.org/9367/20170911022514/https://www.internetsociety.org/internet/global-internet-user-survey-2012.

2.1. Il diritto all'accesso a Internet negli ordinamenti sovranazionali…

In tutti i trattati internazionali sui diritti umani manca l'enunciazione espressa del diritto all'accesso a Internet. È una circostanza del tutto comprensibile, considerando il fatto che le principali convenzioni in materia (la Dichiarazione universale dei diritti dell'uomo del 1948, il Patto internazionale sui diritti civili e politici e il Patto internazionale sui diritti economici, sociali e culturali, entrambi del 1966) furono redatte quando Internet ancora non esisteva.

Dei riferimenti all'accesso a Internet compaiono, tuttavia, in alcuni trattati internazionali recenti in cui si afferma che la possibilità di usufruire delle nuove tecnologie, compreso Internet, da parte di minoranze e categorie di individui svantaggiati, costituisce uno strumento per garantirne la non discriminazione e lo sviluppo. Si tratta della Convenzione sui diritti delle persone con disabilità, adottata il 13 dicembre 2006 dall'Assemblea generale, e della Dichiarazione dei diritti dei popoli indigeni delle Nazioni Unite, approvata il 13 settembre 2007. La prima, all'art. 9, secondo comma, lettera g), impone agli Stati arte di prendere appropriate misure per promuovere l'accesso per le persone con disabilità alle nuove tecnologie e ai sistemi di informazione e comunicazione, compreso Internet. La seconda, all'art. 16, primo comma, riconosce che i popoli indigeni hanno il diritto a avere accesso a tutte le forme mediatiche non indigene senza discriminazione.
Questi trattati affermano che negare l'accesso alla Rete significherebbe ledere diritti umani fondamentali, quali il diritto all'istruzione e all'uguaglianza. In questo senso, potrebbero costituire il primo passo verso la piena affermazione del diritto all'accesso a Internet all'interno dell'ordinamento internazionale.

L'accesso a Internet non compare neanche all'interno della Carta dei diritti fondamentali dell'Unione europea[250]. Il Parlamento europeo ha tuttavia approvato, il 26 marzo 2009, la raccomandazione Lambridis sul rafforzamento della sicurezza e delle li-

[250] La Carta dei diritti fondamentali dell'Unione europea, che riconosce una serie di diritti personali, civili, politici, economici e sociali dei cittadini e dei residenti dell'UE, fu proclamata ufficialmente a Nizza nel dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione. Nel dicembre 2009, con l'entrata in vigore del Trattato di Lisbona, è stato conferito alla Carta lo stesso effetto giuridico vincolante dei trattati (art. 6, par. 1, del TUE). La Carta comprende un preambolo introduttivo e 54 articoli, suddivisi in sette capi: dignità, libertà, uguaglianza, solidarietà, cittadinanza, giustizia, disposizioni generali. La Carta si applica alle istituzioni europee nel rispetto del principio della sussidiarietà e in nessun caso può ampliare le competenze ed i compiti a queste attribuite dai trattati. Qualora uno qualsiasi dei diritti corrisponda ai diritti garantiti dalla Convenzione europea dei diritti dell'uomo, il suo significato e campo d'applicazione deve essere uguale a quello definito dalla convenzione, anche se il diritto comunitario può prevedere una maggiore tutela.

bertà fondamentali in Rete, che invita gli Stati a escludere misure preventive e generalizzate dirette a limitare i diritti dei cittadini in Rete, inclusa la disconnessione da Internet. In conformità alla raccomandazione Lambridis, nel maggio 2009 il Parlamento europeo ha proposto l'adozione dell'emendamento n. 138/46 al Telecoms Package. L'emendamento 138, qualora approvato insieme al pacchetto, avrebbe condotto al riconoscimento nell'ordinamento dell'Unione del diritto fondamentale all'accesso a Internet. L'emendamento, con cui di fatto si escludeva la possibilità delle disconnessioni ad opera della authority governative attribuendone la facoltà soltanto a un'autorità giudiziaria, previo svolgimento di regolare e giusto processo, è stato tuttavia respinto dal Consiglio a tutela del diritto d'autore.

2.2. …e negli ordinamenti nazionali

In mancanza di trattati internazionali sui diritti umani che enuncino espressamente il diritto all'accesso a Internet, alcuni ordinamenti nazionali indicano comunque una tendenza nel senso di qualificare l'accesso a esso come diritto autonomo, indipendentemente dal suo uso per attuare altri diritti fondamentali.

L'Estonia è stata il primo Paese ad adottare una legge, nel 2000, che stabiliva il diritto alla connessione. Il 7 aprile 2004 questo principio è stato elevato al rango costituzionale.

Il diritto alla connessione alla Rete è stato introdotto anche nella Costituzione greca, a seguito della revisione cui è stata sottoposta nel 2001: il secondo comma del nuovo articolo 5a attribuisce a tutti gli individui il diritto a partecipare alla Società dell'Informazione e impone allo Stato l'obbligo di agevolare la produzione, lo scambio e la diffusione delle informazioni trasmesse elettronicamente e l'accesso alle medesime.

Le disposizioni costituzionali più avanzate sull'accesso a Internet sono quelle ecuadoregne: l'art. 16 della Costituzione del 2008 prevede che tutte gli individui, e non i soli cittadini dell'Ecuador, in forma individuale o collettiva, abbiano il diritto di accedere alle tecnologie dell'informazione e della comunicazione; il successivo art. 17 garantisce l'effettività del diritto all'accesso alle tecnologie dell'informazione includendo una serie di obblighi in capo allo Stato perché rimuova le cause che limitano il diritto in questione e ponga in essere tutte le misure idonee a rafforzarlo.

2.3. (segue): l'approccio costituzionalistico italiano

Le coordinate poste dalla Costituzione italiana del 1947 difficilmente si prestano alla deduzione di un potenziale diritto all'accesso a Internet: benché la felice formulazione degli artt. 15 e 21, che affermano rispettivamente la libertà e segretezza della corrispondenza e la libera manifestazione del pensiero, li renda permeabili all'avvento di nuove tecnologie diffusive e comunicative[251], all'art. 21 non è possibile rinvenire l'esistenza di un autonomo diritto di stampa o di accesso alla stessa.

D'altra parte, escludendo la possibilità di un'interpretazione in via evolutiva di alcuni articoli costituzionali, alcuni giuristi credono che sarebbe altrettanto difficile «attribuire alle pur straordinarie caratteristiche di internet capacità nosopoietiche tali da accreditare senz'altro la comparsa nell'ordinamento di un nuovo, autonomo e, secondo taluni, fondamentale diritto individuale, identificabile con quello di accedere al mezzo»[252], in quanto non sussisterebbero le ragioni per cui la libera utilizzazione di Internet dovrebbe godere di un simile stato giuridico rispetto ad altri mezzi analoghi.

Il 26 settembre 2012 è stato presentato al Senato italiano un disegno di legge per l'introduzione dell'articolo 21-bis della Costituzione recante il riconoscimento del diritto all'accesso a Internet[253]. Il nuovo art. 21-bis prevede che «tutti hanno eguale diritto di accedere alla rete internet ovvero ad ogni altra forma di diffusione di contenuti a distanza per via telematica. La legge assicura l'eguaglianza di accesso, rimuovendo ogni ostacolo e predisponendo i necessari interventi per lo sviluppo della rete internet e la fruizione del servizio».

L'idea d'inserire nella Costituzione una norma che stabilisse l'equale diritto di accedere alla Rete era stata lanciata da Stefano Rodotà in occasione dell'edizione italiana dell'IGF 2010. Secondo Rodotà, una cittadinanza amputata della dimensione digitale non sarebbe più una cittadinanza, perché escluderebbe la persona dalla dimensione globale. L'accesso a Internet sarebbe quindi l'ineliminabile punto di partenza perché ogni persona possa essere nella condizione di godere delle opportunità del Web.

---

[251] All'art. 15 Cost. si fa riferimento a «ogni altra forma di comunicazione», mentre all'art. 21 Cost. si ragiona in termini «ogni mezzo di diffusione».

[252] P. Costanzo, *Miti e realtà dell'accesso a Internet (una prospettiva costituzionalistica)*, in G. Cassano, G. Vaciago, G. Scorza (a cura di), *Diritto dell'internet. Manuale operativo – Casi, legislazione, giurisprudenza*, 2012, p. XXVI.

[253] Senato della Repubblica, XVI Legislatura n. 3487.

Rodotà si era anche già fatto promotore per la redazione di una Costituzione per Internet, un documento in cui definire i principi che possono trasformare in diritti le situazioni di quanti usano la Rete. La proposta di un Internet Bill of Rights, il cui progetto era nato in occasione della seconda fase del WSIS a Tunisi nel 2005, scaturiva dalla constatazione che Internet stava realizzando una nuova redistribuzione del potere e sorgeva pertanto la necessità di fissare alcuni principi costituzionali (fra gli altri, libertà di accesso, libertà di utilizzazione, diritto alla conoscenza, rispetto della privacy, riconoscimento di nuovi beni comuni) per evitare che prevalessero le logiche censorie degli Stati.

Benché la proposta di legge sia caduta nel nulla, il lavoro di Rodotà è sfociato nella Dichiarazione dei diritti di Internet, adottata il 28 luglio 2015 dalla Commissione per i diritti e i doveri in Internet istituita presso la Camera dei deputati.

Qualora in futuro si procedesse concretamente nella direzione di conferire a Internet il rango di situazione costituzionalmente prevista e garantita, la formulazione normativa più efficace «dovrebbe contestualmente comportare l'erogazione della connessione alla Rete nei termini di un'obbligazione categorica a carico di qualcuno (pubblici poteri e/o operatori privati)»[254]. Solo in questi termini, infatti, l'accesso a Internet sarebbe pienamente qualificato come un servizio universale, al pari dell'istruzione, della sanità e della previdenza, da garantire attraverso investimenti statali, politiche sociali ed educative, e scelte di spesa pubblica.

2.4. La prassi giurisprudenziale nazionale

Il problema del diritto all'accesso a Internet e la sua rilevanza costituzionale sono emersi anche in alcuni procedimenti giudiziari che hanno messo in luce l'esigenza di tutelare il libero uso di Internet a garanzia della libertà fondamentale di espressione.

Nella sentenza relativa alla causa *Reno* c. *American Civil Liberties Union*[255], la Corte suprema degli Stati Uniti ha giudicato incostituzionale il Communications Decency Act (Titolo V del Telecommunications Act del 1996)[256]. Questo consentiva l'adozione di sanzioni nei confronti degli utenti che immettevano in Rete contenuti considerati moralmente sconvenienti e era già stato dichiarato incostituzionale dalla Corte distrettuale della

[254] P. Costanzo, op. cit., pag. XXVII.

[255] Supreme Court of the United States 26 giugno 1997, n. 521 U.S. 844, *Reno* c. *American Civil Liberties Union*.

[256] 47 U.S.C. § 151 et seq.

Pennsylvania. La Corte suprema, dopo essere stata investita della questione, ha confermato la pronuncia dei giudici federali nella decisione del 26 giugno 1997. Argomentando che l'interesse a proteggere i bambini da materiali indecenti non poteva giustificare la soppressione della libertà di manifestazione del pensiero, la Corte è arrivata alla conclusione che eventuali limitazioni ingiustificate all'accesso alla Rete fossero in contrasto con il primo emendamento della Costituzione statunitense, relativo alle libertà di culto, parola e stampa. La Corte, utilizzando il primo emendamento come parametro per l'incostituzionalità della legge repressiva della libertà in Rete e reinterpretandolo alla luce del ventesimo secolo, avrebbe implicitamente qualificato il diritto all'accesso a Internet come un diritto fondamentale, sebbene la tutela garantita sia fondamentalmente considerata come strumentale alla tutela delle libertà contenute nella Costituzione.

Altrettanto innovativa è stata la decisione del Consiglio costituzionale francese sulla legittimità della legge HADOPI[257] (acronimo di Haute Autorité pour la diffusion de œuvre set la protection des droits sur Internet), relativa alla diffusione e protezione delle creazioni in Internet[258]. Il Consiglio, muovendo dalla considerazione per cui i servizi di comunicazione online rivestono una crescente importanza per l'espressione delle idee e delle opinioni, ha ritenuto che la libertà di comunicazione e di espressione presupponga necessariamente anche la libertà di accedere a tali servizi. La decisione del giudice, che identificherebbe una sorta di diritto fondamentale all'accesso a Internet, è giunta a equiparare le limitazioni imposte alla libertà sulla Rete con le limitazioni alla libertà garantita dall'articolo 11 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789[259]. Pertanto, secondo il Consiglio, le misure di disconnessione dalla Rete decise autoritativamente dall'Esecutivo per sanzionare accertate violazioni di diritti di proprietà intellettuale commesse dai privati devono considerarsi illegittime, in quanto non sottoposte preventivamente al vaglio dell'autorità giudiziaria, come invece avviene per la limitazione delle altre libertà personali.

Ancora più oltre si spinge la Corte suprema di giustizia del Costa Rica[260]. La Sala Constitucional della Corte ha sancito che l'accesso a Internet è un diritto fondamentale,

[257] Legge 10 giugno 2009, n. 2009-669.

[258] Conseil Constitutionnel de la République Française 10 giugno 2009, n. 2009-580 DC, *Loi favorisant la diffusion et la protection de la création sur Internet*.

[259] «La libera manifestazione dei pensieri e delle opinioni è uno dei diritti più preziosi dell'uomo; ogni cittadino può dunque parlare, scrivere, stampare liberamente, salvo a rispondere dell'abuso di questa libertà nei casi determinati dalla Legge».

[260] Cfr. Corte Suprema de Justicia de Costa Rica 30 luglio 2010, n. 12790.

insieme al più generale diritto costituzionale all'accesso alle tecnologie dell'informazione e al diritto alla parità e all'eliminazione del digital divide. Questa decisione, richiamandosi esplicitamente a quanto affermato dal Consiglio costituzionale francese, si fonda sul presupposto che le tecnologie dell'informazione hanno influenzato il modo di comunicare delle persone, eliminando le barriere dello spazio e del tempo, e che la possibilità di accedere alla Rete ha facilitato l'esercizio di diritti fondamentali come la partecipazione democratica, l'educazione, la libertà di espressione e di pensiero. Così la Corte, pur muovendo da una lettura strumentale del diritto all'accesso a Internet come mezzo per la realizzazione di altri diritti fondamentali, è giunta ad affermarne l'autonomia rispetto a questi ultimi e a qualificarlo come diritto fondamentale indipendente.

2.5. L'infrastruttura necessaria all'accesso a Internet

Le disposizioni legislative e le decisioni giurisprudenziali che intendono rendere effettivo il diritto all'accesso a Internet pongono spesso l'accento sull'aspetto concreto della questione: la realizzazione di un'infrastruttura che supporti la connessione alla Rete.

Specialmente nei paesi meno sviluppati, e in parte anche nei paesi emergenti e nei c.d. BRICS, si pone il problema del "digital divide", termine che indica le «limitazioni concrete di accesso alle nuove tecnologie dell'informazione derivanti da cause per così dire materiali, che possono consistere nell'arretratezza delle infrastrutture, nelle difficili condizioni economiche dei cittadini, nel loro scarso livello di alfabetizzazione (non solo) informatica o, ancora, nelle particolarità geomorfologiche del territorio dello Stato»[261].

Il divario digitale non sussiste solo fra i paesi sviluppati e quelli in via di sviluppo, ma anche all'interno dello stesso paese, lungo le linee sociali, geografiche, di genere e di ricchezza: soprattutto nelle zone in cui la penetrazione di Internet è bassa, l'accesso alla Rete è generalmente concentrato fra le élite socioeconomiche, mentre coloro che abitano nelle zone rurali patiscono la mancanza di disponibilità tecnologica, una connessione a Internet più lenta e costi maggiori.

Il rapporto del Relatore speciale sulla promozione e protezione del diritto alla libertà di opinione ed espressione[262] contiene alcune raccomandazioni rivolte agli Stati per ridurre il divario digitale, di cui fornisce una definizione operativa: esso consiste nella

[261] G.M. Ruotolo, op. cit., p. 40.

[262] V. nota 190.

disparità tra le persone con un accesso effettivo alle tecnologie digitali e dell'informazione, in particolare Internet, e le persone con un accesso limitato o senza alcun accesso alle stesse[263].

Senza l'accesso a Internet, gruppi marginalizzati e paesi in via di sviluppo rischiano di rimanere intrappolati in una condizione svantaggiosa, che perpetua la disparità esistente sia fra gli Stati sia al loro interno. Per combattere le situazioni d'ineguaglianza, è necessario assicurare ai segmenti svantaggiati della società l'opportunità di esprimere in modo effettivo le proprie rimostranze. In questo senso, Internet offre l'opportunità ai gruppi più svantaggiati di ottenere informazioni, far valere i propri diritti e partecipare ai dibattiti pubblici che riguardano i cambiamenti sociali, economici e politici per migliorare la loro condizione. In aggiunta, Internet rende disponibile una vasta e crescente fonte di conoscenza prima inaccessibile per le persone negli Stati in via di sviluppo[264].

Per queste ragioni, La Rue rinnovava l'invito agli Stati affinché facilitassero il trasferimento di tecnologia verso i paesi emergenti e inserissero, all'interno delle proprie politiche di assistenza, programmi che favorissero l'accesso universale a Internet.

Il Relatore speciale, pur conscio delle difficoltà nel conseguire pienamente l'accesso a Internet in tutto il mondo, concludeva il rapporto ricordando agli Stati il loro impegno a garantire la libertà di espressione, da cui discende l'obbligo di facilitare la disponibilità dei mezzi che rendono possibile il suo esercizio, incluso Internet. Pertanto, gli Stati dovrebbero adottare politiche e strategie effettive e concrete, sviluppate in consultazione con i rappresentanti di tutti i segmenti della società, per rendere Internet disponibile, accessibile ed economico per tutti[265].

2.6. Il dibattito sul diritto all'accesso a Internet

In un articolo pubblicato sul sito del New York Times[266], Vinton Cerf, uno dei "padri di Internet", contestò fortemente l'idea che l'accesso a Internet debba considerarsi un diritto umano. Cerf, pur riconoscendo che le proteste che infiammarono il Medioriente e il Nord Africa nel 2011 non si sarebbero mai svolte nello stesso modo senza le possibilità che Internet offre per comunicare, organizzare e pubblicizzare dovunque e istantaneamente,

[263] Cfr. ivi, par. 61.

[264] Cfr. ivi, par. 62.

[265] Cfr. ivi, par. 66.

[266] V. Cerf, *Internet access is not a human right*, 5 gennaio 2012, www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

scrisse che la tecnologia rende possibili alcuni diritti, ma non è essa stessa un dritto. Secondo Cerf, sarebbe un errore inserire qualsiasi tecnologia in questa elevata categoria, poiché col tempo si finirebbe per dare valore alle cose sbagliate.

L'articolo di Cerf generò un grande dibattito sullo scopo dei diritti umani e sui motivi per cui all'accesso a Internet debba essere conferito quello status.

L'organizzazione no-profit A Human Right è in parte d'accordo con l'affermazione di Cerf per cui l'accesso a Internet non possa appartenere alla stessa classe di diritti quali la libertà dalla tortura e la libertà di pensiero. Non trova tuttavia difficile immaginare che il diritto di accedere alla Rete, che unisce tutte le persone come se fossero uguali, possa stare fra una serie di altre necessità incluse nella Dichiarazione universale dei dell'uomo, come l'accesso all'alimentazione, al vestiario, all'abitazione e alle cure mediche[267].

Scott Edwards, rispondendo al pezzo di Cerf sul blog statunitense di Amnesty International[268], sostiene che la crescente necessità dell'accesso a Internet nelle zone più povere del mondo (per il godimento dei diritti relativi alla salute, all'educazione, all'impiego, alle arti, all'uguaglianza di genere) è un indizio dell'inseparabilità delle ICT dai diritti di cui esse permettono la fruizione. Le garanzie originariamente previste nella Dichiarazione universale dei diritti dell'uomo non sarebbero più sufficienti e ci sarebbe bisogno di nuovi strumenti per la protezione dei diritti fondamentali.

Anche l'attivista egiziano per i diritti umani Sherif Elsayed-Ali non concorda con l'opinione di Cerf[269]. Egli afferma che l'accesso a Internet è una parte integrante dei diritti umani, dal momento che la libertà di parola e la libertà di accesso alle informazioni sarebbero insignificanti se i governi non proteggessero i mezzi per il loro godimento. Benché i diritti umani siano per definizione intrinseci all'umanità di una persona, e non vengono quindi concessi per volontà uno Stato, i governi hanno due obblighi principali nei loro confronti: non solo devono astenersi dall'intromettersi nel loro godimento, ma devono soprattutto fornire i mezzi per la loro fruizione, e ciò implica dotare i propri cittadini di un accesso diffuso alla Rete.

---

[267] Cfr. K. Grammatis, *Our Response To Vint Cerf*, 16 gennaio 2012, ahumanright.org/blog/2012/01/vint-cerf-internet-access-is-a-human-right-2/.

[268] Cfr. S. Edwards, *Is Internet Access A Human Right?*, 10 gennaio 2012, www.amnestyusa.org/is-internet-access-a-human-right/.

[269] Cfr. S. Elsayed-Ali, *Internet access is integral to human rights*, 15 gennaio 2012, egyptindependent.com/internet-access-integral-human-rights/.

Mentre prosegue il dibattito sul diritto di accesso a Internet, la tecnologia ha compiuto progressi notevoli nel campo delle telecomunicazioni e oggi si dovrebbe piuttosto parlare del diritto fondamentale alla banda larga, perché una connessione lenta alla Rete equivale a nessun accesso.

* * *

Lo studio, da una parte, della prassi delle organizzazioni internazionali, e, dall'altra, della giurisprudenza nazionale e internazionale sembrerebbe non lasciare dubbi all'interpretazione evolutiva da dare alle norme internazionali in materia di diritti umani: la loro tutela, e le restrizioni al loro esercizio, vanno applicate anche nei casi in cui il loro godimento si realizza per mezzo delle nuove tecnologie. Questa nuova definizione condivisa, perlomeno dai paesi che in primo luogo rispettano i diritti fondamentali nel mondo reale, e poi in quello digitale, qualifica l'accesso a Internet come un diritto strumentale indispensabile per la piena realizzazione degli individui nella realtà globalizzata. Ad oggi, tuttavia, non si può ancora parlare dell'accesso a Internet nei termini di un diritto fondamentale autonomo, e la situazione non è destinata a cambiare almeno finché non verrà realizzata un'infrastruttura in grado di supportare la connessione alla Rete in tutto il mondo.

Bibliografia

ARTICOLI E CONTRIBUTI DI DOTTRINA

I. ARROYO MARTÍNEZ, *Descargas en Internet*, 23 dicembre 2009, elpais.com/diario/2009/12/23/opinion/1261522804_850215.html

BBC, *Internet access is 'a fundamental right'*, 8 marzo 2010, news.bbc.co.uk/2/hi/8548190.stm

A. BONFANTI, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Rivista di diritto internazionale*, 2019, pag. 694 ss.

F. CACCAVELLA, *Il CERN festeggia i 20 anni del Web e rimette on line la prima home page*, 30 aprile 2013, www.repubblica.it/tecnologia/2013/04/30/news/il_cern_festeggia_i_20_anni_del_web_e_rimette_on_line_la_prima_home_page-57805889/

L. CASINI, *Diritto amministrativo globale*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006

L. CHIRCOP, *A Due Diligence Standard of Attribution in Cyberspace*, in *International and Comparative Law Quarterly*, 2018, pag. 643 ss.

V. CERF, *Internet access is not a human right*, 5 gennaio 2012, www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html

J.W. DELLAPENNA, *Law in a Shrinking World: The Interaction of Science and Technology in International Law*, in *Kentucky Law Journal*, 2000, pag. 809 ss.

F. DELERUE, F. DOUZET, A. GÉRY, *Building Cyber Peace While Preparing Cyber War*, in C. ANKERSEN, F. DOUZET, S. SHACKELFORD (a cura di), *Cyber Peace: Charting a Path toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge, 2022, pag. 170 ss.

F. DELERUE, *The Application of the Norms of International Law to Cyber Operations: Reinterpretation or Contestation of International Law in Cyberspace?*, in *Israel Law Review*, 2019, pag. 295 ss.

F. DELERUE, *International Cooperation on the International Law Applicable to Cyber Operations*, in *European Foreign Affairs Review*, 2019, pag. 203 ss.

F. DELERUE, *Attribution to State of Cyber Operations Conducted by Non-State Actors*, in E. CARPANELLI E N. LAZZERINI (a cura di), *Use and Misuse of New Technologies*, 2019, pag. 233 ss.

F. DELERUE, *The Right to Respond? States and the Cyber Arena*, in *Turkish Policy Quarterly*, 2018, pag. 145 ss.

S. EDWARDS, *Is Internet Access A Human Right?*, 10 gennaio 2012, www.amnestyusa.org/is-internet-access-a-human-right/

S. ELSAYED-ALI, *Internet access is integral to human rights*, 15 gennaio 2012, egyptindependent.com/internet-access-integral-human-rights/

M. FACKLER, *North Korea Accuses U.S. of Staging Internet Failure*, 27 dicembre 2014, www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html

J. FRAKES, *The common heritage of mankind principle and the deep seabed, outer space, and Antarctica: will developed and developing Nations reach a compromise?*, in *Wisconsin International Law Journal*, 2003, pag. 409 ss.

M. GIAMPIETRO, *Twenty years of a free, open web*, 30 aprile 2013, home.cern/news/news/computing/twenty-years-free-open-web

A. GIGANTE, *Blackhole in Cyberspace: The Legal Void in the Internet*, in *John Marshall Journal of Computer and Information Law*, 1997, pag. 413 ss.

K. GRAMMATIS, *Our Response To Vint Cerf*, 16 gennaio 2012, ahuman-right.org/blog/2012/01/vint-cerf-internet-access-is-a-human-right-2/

INTERNET SOCIETY, *Global Internet User Survey*, 20 novembre 2012, wayback.archive-it.org/9367/20170911022514/https://www.internetsociety.org/internet/global-internet-user-survey-2012

C.C. JOYNER, C. LOTRIONTE, *Information Warfare as International Coercion: Elements of a Legal Framework*, in *European Journal of International Law*, vol. 12, 2001, pag. 825 ss.

S. LI, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, in *Yale Journal of International Law*, 2013, pag. 179 ss.

D. MANDRIOLI, *Alcune riflessioni sul cyber attack subito dall'Australia: oltre i problemi di attribuzione dell'illecito*, in *Rivista di diritto internazionale*, 2021, pag. 188 ss.

S. MELE, *La prima volta delle cybersanzioni Ue*, 3 agosto 2020, formiche.net/2020/08/quadro-giuridico-mele-sanzioni-cyber/

SHIN-YI PENG, *Cybersecurity Threats and the WTO National Security Exceptions*, in *Journal of International Economic Law*, 2015, pag. 449 ss.

E. PFANNER, *Should Online Scofflaws Be Denied Web Access?*, 12 aprile 2009, www.nytimes.com/2009/04/13/technology/internet/13iht-piracy13.html

M. ROSCINI, *World Wide Warfare* - Jus ad bellum *and the Use of Force*, in *Max Planck Yearbook of United Nations Law*, 2010, pag. 85 ss.

D.E. SANGER, N. PERLROTH, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, 17 dicembre 2014, www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html

M.N. SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, pag. 835 ss.

M.N. SCHMITT, *In Defense of Due Diligence in Cyberspace*, in *The Yale Law Journal Forum*, 2015, pag. 68 ss.

M.N. SCHMITT, *The Sixth United Nations GGE and International Law in Cyberspace*, 10 giugno 2021, www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

MANUALI E MONOGRAFIE

I. BROWNLIE, *International Law and the Use of Force by States*, 1963

S.M. CARBONE, R. LUZZATTO, A. SANTA MARIA (a cura di), *Istituzioni di diritto internazionale*, Torino, 2011

G. CASSANO, G. VACIAGO, G. SCORZA (a cura di), *Diritto dell'internet. Manuale operativo – Casi, legislazione, giurisprudenza*, 2012

F. DELRUE, *Cyber Operations and International Law*, Regno Unito, 2020

C. FOCARELLI, *Diritto internazionale*, 2021

F. MUNARI, L. SCHIANO DI PEPE, *Tutela transnazionale dell'ambiente*, Urbino, 2012,

G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2010

M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, 2014

G.M. RUOTOLO, *Internet-ional law. Profili di diritto internazionale pubblico per la Rete*, Bari, 2012

M.N. SCHMITT, L. VIHUL (a cura di), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Oxford, 2017

SENTENZE

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

24 novembre 2011, causa C-70/10, *Scarlet Extended SA* c. *Société belge des auteurs, compositeurs et éditeurs SCRL*

16 febbraio 2012, causa C-360/10, *SABAM* c. *Netlog NV*

CORTE INTERNAZIONALE DI GIUSTIZIA

9 aprile 1949, *Stretto di Corfù* (*Albania* c. *Regno Unito*)

27 giugno 1986, *Attività militari e paramilitari degli Stati Uniti in Nicaragua e contro il Nicaragua* (*Nicaragua* c. *Stati Uniti*)

12 ottobre 1994, *Delimitazione della frontiera marittima nella regione del golfo del Maine*

25 settembre 1997 nel caso del *Progetto Gabčíkovo-Nagymaros* (*Ungheria* c. *Slovacchia*)

6 novembre 2003, *Piattaforme petrolifere* (*Iran* c. *Stati Uniti*)

19 dicembre 2005, *Attività armate sul territorio del Congo* (*Repubblica Democratica del Congo* c. *Uganda*)

26 febbraio 2007, *Applicazione della Convenzione per la prevenzione e la re-pressione del crimine di genocidio* (*Bosnia-Erzegovina* c. *Serbia e Montenegro*)

CORTE EUROPEA DEI DIRITTI DELL'UOMO

10 marzo 2009, ricorsi n. 3002/03 e 23676/03, *Times Newspaper Ltd* c. *Regno Unito*

25 febbraio 2010, ricorso n. 13290/07, *Patrice Renaud* c. *Francia*

5 maggio 2011, ricorso n. 33014/05, *Comitato editoriale di Pravoye Delo e Shtekel* c. *Ucraina*

18 dicembre 2012, ricorso n. 3111/10, *Ahmet Yildirim* c. *Turchia*

25 maggio 2021, ricorsi n. 58170/13, n. 62322/14 e n. 24960/15, *Big Brother Watch e altri* c. *Regno Unito*

TRIBUNALE PENALE INTERNAZIONALE PER L'EX-JUGOSLAVIA

15 luglio 1999, *Tadić*

CORTI NAZIONALI

Supreme Court of the United States 26 giugno 1997, n. 521 U.S. 844, *Reno* c. *American Civil Liberties Union*

Conseil Constitutionnel de la République Française 10 giugno 2009, n. 2009-580 DC, *Loi favorisant la diffusion et la protection de la création sur Internet*

Corte Suprema de Justicia de Costa Rica 30 luglio 2010, n. 12790

TRATTATI

International Telecommunication Regulations, 9 dicembre 1988

Constitution and Convention of the International Telecommunication Union, 22 dicembre 1992, in UNTS 1825, 1826

Convenzione sulla criminalità informatica, 23 novembre 2001, in UNTS 2296, pag. 167 ss.

International Telecommunication Regulations, 14 dicembre 2012

ALTRE FONTI

NAZIONI UNITE

(2001) Risoluzione 56/83 dell'Assemblea generale, *Responsibility of States for internationally wrongful acts*, A/RES/56/83 (12 dicembre 2001)

(2005) *Report of the Working Group on Internet Governance* (giugno 2005), www.wgig.org/docs/WGIGREPORT.pdf

(2006) Risoluzione 60/251 dell'Assemblea generale, *Human Rights Council*, A/RES/60/251 (3 aprile 2006)

(2008) Risoluzione 7/36 del Consiglio dei diritti dell'uomo, *Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/7/36 (28 marzo 2008)

(2009) Risoluzione 12/16 del Consiglio dei diritti dell'uomo, *Freedom of opinion and expression*, A/HRC/12/16 (2 ottobre 2009)

(2010) Risoluzione 64/187 dell'Assemblea generale, *Information and communication technologies for development*, A/RES/64/187 (9 febbraio 2010)

(2011) Risoluzione 17/27 del Consiglio dei diritti dell'uomo, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27 (16 maggio 2011)

Comitato per i diritti dell'uomo, *General comment No. 34. Article 19: Freedoms of opinion and expression*, CCPR/C/GC/34 (12 settembre 2011)

(2012) Risoluzione 56/83 dell'Assemblea generale, *Responsibility of States for internationally wrongful acts*, A/RES/56/83 (28 gennaio 2012)

Risoluzione 20/8 del Consiglio dei diritti dell'uomo, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/8 (5 luglio 2012)

(2013) Assemblea generale, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 giugno 2013)

(2015) Assemblea generale, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 luglio 2015)

(2021) Assemblea generale, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States*, A/76/136 (13 luglio 2021)

Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135 (14 luglio 2021)

ORGANIZZAZIONE PER LA SICUREZZA E LA COOPERAZIONE IN EUROPA

Y. Akdeniz, *Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States*, 11 luglio 2011, www.osce.org/files/f/documents/e/f/80723.pdf

UNIONE EUROPEA

(1999) Conclusioni del Consiglio del 27 settembre 1999 sul ruolo dell'autoregolamentazione alla luce dello sviluppo di nuovi servizi nel settore dei media, in GU L 283, del 6 ottobre 1999

(2000) Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), in GU L 178, del 17 luglio 2000, pag. 1 ss.

(2009) Risoluzione del Parlamento europeo, del 17 gennaio 2008, *Risultati del forum sulla governance di internet, svoltosi a Rio de Janeiro dal 12 al 15 novembre 2007*, in GU C 41E, del 12 febbraio 2009, pagg. 80-81

Comunicazione della Commissione al Parlamento europeo e al Consiglio, del 18 giugno 2009, *Governance di Internet: le prossime tappe* [non pubblicata nella Gazzetta ufficiale]

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, del 18 giugno 2009, *L'internet degli oggetti - Un piano d'azione per l'Europa* [non pubblicata nella Gazzetta ufficiale]

Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia d reti e di servizi di comunicazione elettronica, delle direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, in GUUE L 337, del 18 dicembre 2009, pag. 11 ss.

Direttiva 2009/140/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica delle direttive 2002/21/CE che istituisce un quadro

normativo comune per le reti di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica, in GU L 337, del 18 dicembre 2009, pag. 37 ss.

Regolamento (CE) n. 1211/2009 del Parlamento europeo e del Consiglio, del 25 novembre 2009, in GUUE L 337, del 18 dicembre 2009, pag. 1 ss.

Dichiarazione della Commissione sulla neutralità della Rete, in GU C 308, del 18 dicembre 2009, pag. 2

(2019) Decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, in GU L 129I, del 17 maggio 2019, pag. 13 ss.

Regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, in GU L 129I, del 17 maggio 2019, pag. 1 ss.

DOCUMENTI NAZIONALI

(Australia) Minister for Foreign Affairs, *Attribution of a pattern of malicious cyber activity to Russia*, 4 ottobre 2018, www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-pattern-malicious-cyber-activity-russia

Government of Australia, *International Law applicable in cyberspace*, aprile 2022, www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

(Germania) Federal Government of Germany, *On the Application of International Law in Cyberspace*, mar-zo 2021, www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

(Giappone) Ministry of Foreign Affairs, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, 16 giugno 2021, www.mofa.go.jp/files/100200935.pdf

(Italia) Ministero degli Affari Esteri e della Cooperazione Internazionale, *Italian position paper on 'international law and cyberspace'*, novembre 2021, www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

(Nuova Zelanda) Government Communications Security Bureau, *Malicious cyber activity attributed to Russia*, 4 ottobre 2018, www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/

(Regno Unito) National Cyber Security Centre, *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, 4 ottobre 2018, www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

Foreign, Commonwealth & Development Office, *Application of international law to states' conduct in cyberspace: UK statement*, 3 giugno 2021, www.gov.uk/government/publications/application-

of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement

(Stati Uniti) Department of Commerce, National Telecommunications and Information Administration, *U.S. Principles on the Internet's Domain Name and Addressing System*, 30 giugno 2005, www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system

House Permanent Select Committee on Intelligence, *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 8 ottobre 2012, republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

Executive Office of the President, *Executive Order 13757. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*, 28 dicembre 2016, www.govinfo.gov/content/pkg/FR-2017-01-03/pdf/2016-31922.pdf

Department of Homeland Security, Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, 29 dicembre 2016, www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Department of the Treasury, *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*, 15 marzo 2018, home.treasury.gov/news/press-releases/sm0312