Le fonti dell'ordinamento internazionale e la disciplina della Rete

di Gianpaolo Maria Ruotolo

Abstract: **Internet regulation and the international legal order sources** – The paper frames the international law regulation of the Internet through the study of some of its specific issues such as, in particular, the Requests for comments (RFCs), the legal consequences of the qualification of the Internet as common heritage of mankind and/or as a global public good, and the domain name system (DNS) regulation, in order to understand if it this fits into a broader trend towards the informalization of the international legal order, that is to say of both its normative procedures and sources

Keywords: Internet; international law; international organization; informal law.

"There's a point. Far out there.
When the structures fail you. When the rules aren't weapons anymore,
they're shackles, letting the bad get ahead. Maybe one day you'll have
such a moment of crisis. And in that moment, I hope you have a friend like I did.
To plunge their hands into the filth so you can keep yours clean"

(James Worthington "Jim" Gordon in C. Nolan, The Dark Knight Rises*, 2012).*

1. La disciplina giuridica di Internet, l'approccio non-regolatorio e le norme "autonome": l'esempio delle *Requests for comments* (RFC)

Le difficoltà di dettare una disciplina giuridica compiuta ed efficace per la Rete si sono palesate sin dalla sua diffusione a livello planetario, avvenuta a partire dagli inizi degli anni '90, quando sono iniziati ad emergere differenti approcci alla questione[1].

Un primo orientamento, peraltro successivamente ridimensionato, appuntava la sua attenzione sulle peculiarità del fenomeno e ne faceva discendere l'inapplicabilità delle tradizionali categorie giuridiche e, più in generale, del diritto come strumento di regolamentazione sia della Rete in

[1] Per un'analisi della rilevanza complessiva del diritto rispetto al fenomeno in esame cfr. J. Goldsmith, T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, 2006; J. Kulesza, *International Internet Law*, New York, 2012.

DPCE online
ISSN: 2037-6677

quanto infrastruttura sia dei comportamenti umani che vi hanno luogo[2]. Le motivazioni che avrebbero giustificato un siffatto approccio sarebbero state molteplici: in primo luogo l'assenza di frontiere fisiche nel cyberspazio avrebbe impedito l'individuazione del diritto (statale) applicabile a una determinata fattispecie e, per il medesimo motivo, il giudice competente a dirimere le relative controversie; inoltre, e proprio per le difficoltà di localizzazione dei comportamenti che vi hanno luogo, la Rete implicherebbe il rischio costante dell'applicazione extraterritoriale del diritto statale. Da più parti si sottolineavano, quindi, rischi di *spillover*[3]: sottoporre Internet al dominio del diritto (statale ancora una volta) avrebbe comportato la concreta possibilità di avere tante differenti regolamentazioni del medesimo fenomeno, tra loro probabilmente confliggenti, quanti sono i legislatori statali stessi.

Pertanto gli aderenti a questo orientamento, complessivamente anche se con differenti sfumature, suggerivano di utilizzare meccanismi di disciplina per così dire autonomi[4], le cui regole fossero cioè prodotte dagli stessi utenti della Rete e incorporate in un nuovo *genus* di diritto, né statale né internazionale, il c.d. *cyber-law*. Al riguardo si faceva, tra gli altri, l'esempio della *netiquette*[5], l'insieme delle 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 *e-mail*.

Tutto l'approccio appena illustrato, oltre a concepire Internet come "legal void"[6], uno spazio "senza legge" – per alcuni versi analogo all'alto mare

---

[2] Si veda, al riguardo, la nota Dichiarazione di indipendenza del Cyberspazio, reperibile all'indirizzo www.eff.org/it/cyberspace-independence, e pubblicata nel 1996 da John Perry Barlow, già autore di numerosi testi per i *Grateful Dead*, band californiana di rock psichedelico. L'approccio non-regolatorio, infatti, mutua le sue posizioni dagli ideali dei movimenti hippie e flower-power degli anni '60, al quale alcuni suoi esponenti appartenevano infatti in passato. Per un'esposizione dell'orientamento citato cfr., per tutti, D. R. Johnson, D.J. Post, *Law and Borders. The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, 1367; D.J. Post, *In Search for Jefferson's Moose*, Oxford, 2009, *passim*.

[3] L'uso dell'espressione *spillover* in questa accezione è di D. R. Johnson, D.J. Post, *Law and Borders*, cit., 1374. Sul problema cfr. anche A. Segura Serrano, *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, 2006, 1374.

[4] In merito basti citare la ormai abusata "Dichiarazione di indipendenza del cyberspazio" che, rivolgendosi agli Stati, afferma: "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"; cfr. J.P. Barlow, *A Cyberspace Independence Declaration*, San Francisco, 1996. La Dichiarazione è integralmente pubblicata all'indirizzo projects.eff.org/~barlow/Declaration-Final.html.

[5] La *netiquette* è oggigiorno ormai di generale condivisione da parte degli utenti della Rete e implica, in caso di ripetute violazioni, la probabile estromissione del responsabile dalla comunità che ne pretende il rispetto. Per quanto attiene ai profili strettamente giuridici, peraltro, alla *netiquette* fanno spesso rinvio i contratti di fornitura di servizi di accesso da parte dei *provider*, che ne impongono così giuridicamente il rispetto agli utenti loro clienti.

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

o agli spazi extraatmosferici, in cui è assente la sovranità statale, ma non, come noto, il diritto internazionale – concepiva insomma le uniche regole ivi applicabili, in quanto generate spontaneamente dai suoi utenti, alla stregua della tradizionale *lex mercatoria*, sistema di norme elaborate dalla comunità che se ne deve servire le quali, in quanto diritto (per così dire) transazionale delle relazioni economiche[7], lette come il primo caso di "diritto globale senza Stato"[8].

Una ricostruzione siffatta, però, sollevava più dubbi di quanti non ne risolvesse, dal momento che poneva, senza però affrontarlo consapevolmente e risolverlo compiutamente, il difficile problema dell'esistenza di un terzo *genus* di norme giuridiche oltre a diritto internazionale e diritto interno, problema che occupa da tempo la dogmatica giuridica anche con riguardo alla *lex mercatoria*, appunto[9].

È il caso di chiarire da subito (e vedremo poi come ciò sia rilevante per la nostra analisi) come le regole di funzionamento di Internet generate "dal basso" siano spesso contenute in strumenti denominati *Request For Comments* (RFC)[10], espressione con cui si fa riferimento a testi che contengono informazioni o specifiche tecniche, elaborate da esperti, studiosi, operatori del settore, sulla scorta delle pratiche che si sono via via dimostrate più efficaci.

Tali documenti vengono "offerti" alla comunità del Web per il tramite della *Internet Engineering Task Force* (IETF), che ne promuove il rispetto al fine di farli divenire dei veri e propri *standard*[11].

Ricordiamo che l'IETF è un'organizzazione internazionale non governativa (ONG) che riunisce tecnici e ricercatori interessati a titolo individuale all'evoluzione tecnica e tecnologica del Web[12] e che, per l'appunto,

---

[7] Si veda, al riguardo, per tutti, F. Marrella, *La nuova* lex mercatoria. *Principi* Unidroit *ed usi dei contratti del commercio internazionale*, Padova, 2003, il quale usa il modello dei "cerchi concentrici" per spiegare l'impatto della *lex mercatoria* sul diritto del commercio internazionale; cfr. 709 ss. Utilizzeremo (e lo abbiamo già fatto in alcuni nostri scritti precedenti) un modello analogo.

[8] Cfr. G. Teubner, *Breaking Frames: Economic Globalisation and the Emergence of* Lex Mercatoria, in *European Journal of Social Theory*, 2002, 199 ss.

[9] Si veda U. Draetta, *Internet e commercio elettronico nel diritto internazionale dei privati*, Milano, 2001, 19 ss.

[10] A mero titolo di esempio, ricordiamo che esistono due RFC relative alla *netiquette*: la RFC 1855 ("Netiquette Guidelines"), reperibile all'indirizzo www.ietf.org/rfc/rfc1855.txt, e la RFC 2635 ("A Set of Guidelines for Mass Unsolicited Mailings and Postings").

[11] Con l'espressione *standard*, nella letteratura giuridica internazionalistica, si fa riferimento sia a regole "di contenuto prescrittivo preciso, ma, per così dire, "tipizzato"" sia a normative tecniche adottate "per fissare (in via diretta o tramite riferimento a fonti esterne al sistema) i parametri più strettamente operativi e materiali dei comportamenti degli Stati"; così A. Ligustro, *La normativa di base del sistema degli scambi di merci*, in P. Picone, A. Ligustro, *Diritto dell'Organizzazione mondiale del commercio*, Padova, 2002, 95. Evidente come l'esempio fatto nel testo, quanto meno per i suoi contenuti, sia assimilabile alla seconda tipologia di *standard*.

[12] "The IETF is completely open to newcomers. There is no formal membership, no membership fee, and nothing to sign. By participating, you do automatically accept the IETF's rules, including the rules about intellectual property (patents, copyrights and trademarks). If

DPCE online
ISSN: 2037-6677

ha tra i suoi obiettivi la standardizzazione tecnica della Rete, che viene promossa anche mediante la cooperazione con altre organizzazioni, sia di stampo non governativo, come il *World Wide Web Consortium* (c.d. W3C) – ONG fondata nel 1994 presso il *Massachussets Institute of Technology* (MIT) con lo scopo di sviluppare tutte le potenzialità del Web[13] – sia con organizzazioni internazionali di tipo tradizionale, come l'*International Organization for Standardization* (ISO)[14] e l'*International Electrotechnical Commission* (IEC), che si occupa di definire standard in materia di elettricità, elettronica e tecnologie connesse.

I testi così predisposti ottengono una differente classificazione in base al loro "successo" presso comunità della Rete, che ne influenza la portata normativa. Si distinguono, infatti, i *proposed standards*, specifiche sufficientemente stabili e che hanno riscontrato un certo successo da parte degli utenti ma che non sono ancora ritenute sufficientemente mature per essere definitivamente formalizzate, i *draft standard*, che hanno ottenuto per lo meno due implementazioni che ne hanno dimostrato l'efficacia operativa, e che per questo l'*Internet Engineering Steering Group* (IEEG, un gruppo di lavoro di IETF) ritiene sufficientemente maturi e, infine, gli *standard* veri e propri, i quali richiedono la presenza di un numero significativo di applicazioni. Solo a questi ultimi viene assegnato un numero progressivo in una lista formale rubricata STD, e il loro rispetto è raccomandato a tutti gli utenti della Rete perché possano beneficiare della c.d. interoperatività.

I documenti che, invece, non sono valutati come idonei a divenire *standard*, vengono classificati, a seconda dei casi, come *experimental*, qualora si tratti di testi concernenti oggetti e tematiche ancora in fase di sviluppo e ricerca, i quali possono essere stati elaborati da gruppi di lavoro istituzionali – che possono essere istituiti sia in seno all'IETF, sia in seno ad altri gruppi di studio, come l'*Internet Research Task Force* (IRTF) – oppure essere frutto del lavoro di singoli operatori, *informational*, qualora si tratti di documenti che contengono mere informazioni su un determinato argomento e che non mirano in alcun modo a divenire neppure delle raccomandazioni, *historic*, nel caso contengano *standard* che sono ormai divenuti obsoleti perché completamente rimpiazzati da nuove specifiche, o comunque in disuso, e, infine, *best common practice* (BCP), nel caso di istruzioni che si limitano a

you work for a company and the IETF will be part of your job, you must obviously clear this with your manager. However, the IETF will always view you as an individual, and never as a company representative"; cfr. www.ietf.org.

[13] L'organizzazione in questione ha formalizzato tutti i principali protocolli (html, http, https, ecc…) che garantiscono la c.d. interoperabilità, cioè la comunicazione tra macchine diverse, e quindi, in ultima analisi, la trasmissione efficace dei dati su Internet. Cfr. www.w3.org.

[14] Chiariamo che abbiamo ritenuto di dover distinguere l'ISO dalle altre ONG citate pur nella consapevolezza della sua natura non governativa, dal momento che, a differenza delle altre organizzazioni citate nel testo, 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 interno, mediante il rinvio ad essi effettuato da norme nazionali.

suggerire determinate modalità di configurazione.

Ebbene, i testi in questione, e in particolare gli *standard*, hanno certamente portata e contenuto normativi nel senso che, sotto il profilo *materiale*, quanto meno, suggeriscono ai loro destinatari un determinato comportamento. Essi, però, secondo alcuni, difetterebbero del requisito della giuridicità, in quanto meri suggerimenti di comportamento, inidonei a produrre alcun effetto regolato dal diritto, e la cui osservanza sarebbe lasciata alla libera scelta degli operatori della Rete.

Va detto da subito, però, che, analogamente con quanto avviene con la figura dell'onere, il mancato rispetto di queste regole esclude dalla possibilità di utilizzare la risorsa che le stesse disciplinano e che, quindi, *tutti coloro i quali decidono di utilizzarla* sono tenuti o a rispettarle o, in alternativa, ad accettare l'esclusione.

2. La concorrenza di diritto internazionale "pubblico", privato, e "codice" come strumento di regolazione della Rete

Un altro orientamento, per così dire più tradizionalista, e che oggi ci pare abbia assunto consistenza maggioritaria, muovendo dalla considerazione che la Rete rappresenta un nuovo mezzo di comunicazione, seppure di portata rivoluzionaria, la ritiene giuridicamente regolabile[15], ma sottolinea, al contempo, l'opportunità di armonizzare, tra i vari ordinamenti statali, per il tramite del diritto internazionale, alcuni principi di portata generale che consentano di creare un quadro giuridico comune nel quale i legislatori nazionali possano poi muoversi con l'adozione di normative di dettaglio[16].

La dottrina in questione, peraltro, ridimensiona, a nostro giudizio condivisibilmente, anche i timori di *spillover* di cui dicevamo al par. 1, facendo notare come i medesimi non rappresentino affatto un problema peculiare di Internet quanto, piuttosto, un fenomeno connesso a tutte le fattispecie caratterizzate da elementi di transnazionalità, cioè non riconducibili ad un solo ordinamento interno, che sarebbe quindi governabile, a seconda dei casi, attraverso il diritto internazionale "pubblico" o le norme di conflitto dei sistemi di diritto internazionale privato.

In effetti la compiuta regolamentazione giuridica dei vari aspetti di Internet (gestione delle infrastrutture, disciplina dei contenuti, regolamentazione dei comportamenti umani che vi hanno luogo) non può prescindere, per essere veramente efficace ed onnicomprensiva, dall'uso concorrente di strumenti di diritto internazionale "pubblico" e privato (siano

[15] Per una illustrazione di tale approccio cfr., per tutti, J. L. Goldsmith, *Internet and the Abiding Significance of Territorial Sovereignty*, in *Ind. J. Global Legal Stud.*, 1998, 475 ss.
[16] J.L. Goldsmith, *Against Cyberanarchy*, in *University of Chicago Law Review*, 1998, 1240 ss.; J.P. Trachtman, *Cyberspace, Sovereignity, Jurisdiction and Modernism*, in *Indiana Journal of Global Legal Studies*, 1998, 568 ss.; S.S. Mody, *National Cyberspace Regulation: Unbounding the Concept of Jurisdiction*, in *Stanford Journal Int'l Law*, 2001, 382 ss.

DPCE online
ISSN: 2037-6677

essi uniformi o comuni)[17]: mentre i primi, infatti, possono idoneamente disciplinare il regime di gestione della Rete come infrastruttura, le seconde soccorrono nell'individuazione della giurisdizione nazionale competente a dirimere una determinata controversia tra privati relativa ad una fattispecie che ha luogo online e il diritto ad essa applicabile. E, sia detto *en passant*, forme di intelligenza artificiale potrebbero semplificare alcuni dei processi in questione, come è stato evidenziato in una recentissima relazione del Parlamento europeo, che dedica all'automazione dei sistemi di diritto internazionale privato alcune interessanti pagine[18].

Passando poi ad una terza modalità di lettura del problema che ci occupa, e che ci pare degna di attenzione in quanto idonea a fornire un ponte tra i due approcci già illustrati, sarebbe addirittura privo di senso parlare di natura ontologicamente "regolabile" o "non regolabile" di Internet *in quanto tale*, dal momento che la Rete non avrebbe una sua natura immodificabile, che sarebbe invece contingentemente determinata dal "codice" che le dà forma, cioè dall'insieme di apparecchiature che la compongono (*hardware*) e, soprattutto, dal *software* (il "codice", appunto) che ne consente e regola l'uso.

Secondo questa visione, quindi, il cyberspazio sarebbe compiutamente regolabile per il tramite del suo codice informatico il quale, a sua volta, dovrebbe essere informato da norme giuridiche uniformi, volte essenzialmente a decidere quali siano i valori che devono essere assunti come parametro di riferimento dal primo[19]. Ed è appena il caso di evidenziare come, sotto il profilo meramente terminologico, "codice" sia espressione comune a giuristi e informatici e faccia riferimento, in entrambi i casi, ad una sequenza di istruzioni che devono essere applicate…

Ora, sebbene i rapporti tra tecnologia e diritto sollevino numerosi problemi, relativi alle modalità di sfruttamento di strumenti "che sono

[17] Sul rapporto tra diritto internazionale pubblico e sistemi di conflitto nel contesto in esame cfr. J. G. Castel, *The Internet In Light Of Traditional Public And Private International Law Principles And Rules Applied In Canada*, in *The Canadian yearbook of international law*, 2001, 3 ss.; T. Schultz, *Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface* in *European Journal of International Law*, 2008, 799 ss.; D.J.B. Svantesson, *The Relation between Public International Law and Private International Law in the Internet Context*, Conference Paper presentato alla Australian Law Teachers' Association Conference, Luglio 2005, Hamilton, New Zealand, reperibile su www.svantesson.org. Per un'analisi della disciplina internazionalprivatistica della Rete v., per tutti, S. Bariatti, *Internet – Diritto internazionale privato e processuale*, in *Enc. Giur. Treccani, Aggiornamento*, Vol. X, Roma, 2002, 1 ss. e la bibliografia ivi citata.

[18] *Intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale.* Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI)), reperibile online.

[19] Cfr. L. Lessig, *Code – Version 2.0*, Cambridge, 2006, xv, il quale sostiene che Internet può essere controllata mediante forze "in large part exercised by technologies (…), backed by the rule of law (or at least what's left of the rule of law). The challenge for our generation is to reconcile these two forces".

utilizzabili come poteri" ma rispetto ai quali l'ordinamento internazionale non ha sistematicamente attivato le opportune garanzie[20], la ricostruzione appena illustrata, a nostro parere, riesce ad offrire chiavi interessanti di lettura.

E l'influenza degli aspetti tecnici della Rete sulle sue stesse modalità di disciplina, come vedremo, è dimostrata dal fatto che, ad esempio, le tecnologie che consentono la geolocalizzazione degli apparati connessi (e quindi degli utenti, anche, ovviamente, di quelli connessi mediante dispositivi mobili) hanno ridimensionato non di poco le obiezioni sollevate con riguardo alle difficoltà di localizzazione dei comportamenti umani che si svolgono *online*.

Tecnologie siffatte, ormai di applicazione diffusa, consentono infatti di identificare la posizione geografica di coloro che operano sul Web e, sebbene attualmente vengano utilizzate, sotto il profilo commerciale, al fine offrire contenuti mirati – ad esempio mostrare pubblicità rilevanti per la posizione del particolare utente o limitare l'accesso a contenuti ritenuti non appropriati per un determinato contesto[21] – il loro sfruttamento potrebbe essere utile anche per individuare l'ordinamento statale che presenta un collegamento (più) stretto con la fattispecie che si verifica *online*, al fine di ritenerne applicabili le norme e/o competenti i giudici[22].

3. La convergenza digitale

Oltre alle difficoltà e agli ostacoli illustrati, l'individuazione di una disciplina giuridica, sia di diritto interno sia di diritto internazionale, per la Rete è resa ancor più complessa dal fatto che sulla stessa transitano informazioni relative ai servizi e ai *media* più disparati (editoria, televisione, radio, telefonia, comunicazioni private e di rilevanza pubblica, ecc.).

A questa capacità di inglobare in sé contenuti e strumenti anche molto differenti si fa riferimento con l'espressione "convergenza digitale" ("digital" o anche "technological convergence"[23]), con la quale, in ambito informatico, si intende proprio la fusione, resa possibile dalla tecnologia digitale, di una pluralità di strumenti diversi, tutti atti a trasmettere informazioni[24].

---

[20] Parafrasiamo M. Tallacchini, *Giudici, esperti, cittadini: scienza e diritto tra validità metodologica e credibilità civile*, in *Politeia*, 2003, 83 ss.

[21] Sulla disciplina adottata dall'Unione europea al riguardo, anche solo per ulteriori riferimenti bibliografici, ci permettiamo di rinviare a G.M. Ruotolo, *La lotta alla frammentazione geografica del mercato unico digitale: tutela della concorrenza, diritto internazionale privato, uniformità*, in *Diritto del commercio internazionale*, 2018, 501 ss.

[22] D.J.B. Svantesson, *How Does The Accuracy Of Geo-Location Technologies Affect The Law?*, in *Masaryk University Journal of Law and Technology*, 2008, 11 s.

[23] Cfr. Iosifidis, *Digital Convergence: Challenges for European Regulation*, in *Javnost - The Public*, 2002, 3, 27 ss.

[24] Per comprendere concretamente la portata della teoria della convergenza, si pensi a come uno *smartphone* sia oggi in grado di telefonare (con sistema tradizionali o VoIP), riprodurre e trasmettere musica e video, leggere *files* di testo, scattare, inviare e visualizzare foto, eseguire

Ebbene, ognuno di detti *media*, nella sua forma, per così dire, tradizionale, è notoriamente oggetto di regolamentazione giuridica autonoma – sia essa di diritto internazionale o di diritto interno – che differisce da quelle previste per gli altri; e finché i detti mezzi restavano separati gli uni dagli altri una loro differente regolamentazione era non solo giustificata, ma finanche auspicabile, per tener conto delle loro peculiarità[25]. La loro fusione mediante Internet potrebbe implicare anche una sovrapposizione di discipline giuridiche, almeno per alcuni aspetti: e infatti la dottrina che si è occupata del problema suggerisce che, in seguito a tale fusione dei vari *media* su Internet, e quindi con l'avvento della convergenza digitale, le differenziazioni normative dovrebbero essere mantenute esclusivamente per quanto riguarda i contenuti, ma non per quanto concerne il mezzo che li veicola[26].

In realtà, neppure così delineata la questione appare di semplice soluzione, dal momento che, in particolare in alcune peculiari situazioni di confine, in cui la Rete viene utilizzata per offrire servizi che sono difficilmente inquadrabili con riferimento esclusivo all'uno o all'altro *media* tradizionalmente inteso – si pensi, a mero titolo di esempio, ad alcuni servizi di *hosting* video o al c.d. giornalismo diffuso – si potrebbe assistere al fenomeno per il quale, nel dubbio di quale disciplina sia *in concreto* applicabile – disciplina che, ad esempio, potrebbe prevedere regole più o meno rigide in merito alla responsabilità dell'utente o del fornitore di servizi, alle condizioni per l'accesso al servizio, alle modalità di gestione della *privacy* o del trattamento dei dati e così via – i vari ordinamenti nazionali potenzialmente competenti decidano di selezionare, caso per caso, quella maggiormente restrittiva delle prerogative degli individui.

L'elemento della convergenza è stato, peraltro, finanche invocato dall'*International Telecommunications Union* (ITU), in occasione della revisione delle *International Telecommunications Regulations* (ITRs) del 2012, come titolo legittimante la sua competenza a regolamentare la Rete, dal momento che su di essa transiterebbero anche informazioni relative a mezzi di telecomunicazioni più tradizionali, da tempo sotto la sua egida (si pensi, ad esempio, alla telefonia).

Ora, deve essere chiarito da subito che al trasferimento della *governance* di Internet a un'organizzazione internazionale di stampo classico, cioè intergovernativo, si oppongono numerosi fattori, tra cui, in particolare, la volontà di molti Stati (volontà che, a scapito di alcuni recenti elementi di

codice, e così via; uno dei primi teorici di tale teoria è stato N. Negroponte, *Being Digital*, London, 1995.

[25] Cfr. Carey, J. Sanders, *Media Law*, London, 2004; J. Krämer, S. Seifert (Eds), *Communications Regulation in the Age of Digital Convergence – Legal and Economic Perspectives*, Karlsruhe, 2009.

[26] J. Kühling, *Convergence and Regulatory Challenges at National and Supranational Level*, in J. Krämer, S. Seifert (Eds), *Communications Regulation in the Age of Digital Convergence – Legal and Economic Perspectives*, Karlsruhe, 2009, 9 ss.

prassi, gioca ancora un ruolo determinante nell'ordinamento internazionale contemporaneo), specie industrializzati, che temono l'eccessiva rilevanza dei governi nazionali, in particolare di quelli di stampo non democratico. D'altro canto, come è stato efficacemente evidenziato "in addition to being seen as an instrumental governance mode which gave the United States dominance over the Internet and its development, multi- stakeholderism also meant, for numerous developing countries, *a move away from intergovernmental decision-making* and international law"[27].

4. Le difficoltà di una regolamentazione unilaterale di Internet. Il rapporto bilaterale tra Internet e il diritto internazionale

Un'analisi della prassi degli ultimi anni evidenzia, poi, come gli strumenti di diritto interno si siano spesso dimostrati inidonei a disciplinare efficacemente la Rete *da soli*.

Si pensi, per limitarci a qualche esempio, a come le pur importanti restrizioni all'accesso ad Internet adottate da alcuni Paesi del Nord Africa e del Medio Oriente non abbiano in alcun modo impedito le comunicazioni interne e con l'estero via Web, in particolare per il tramite dei *social network* che, assieme ad altri fattori, hanno reso possibili le rivoluzioni della c.d. onda verde dell'inizio del 2011[28].

Anche in occasione della rivoluzione che ha condotto in Egitto alla caduta del regime di Mubarak, il governo locale ha cercato di bloccare i contatti fra gli insorti e di questi con l'esterno tagliando le connessioni Web; tuttavia il blocco è stato aggirato con l'uso di vecchie connessioni di tipo *dial-up*[29] o di telefoni satellitari o, ancora, per il tramite di ponti radio messi a disposizione dall'estero.

A partire dalla fine del 2012, poi, anche l'Iran ha disposto importanti limitazioni all'accesso, da parte degli utenti connessi dal proprio territorio nazionale ad Internet e, in particolare a *Google* e al suo servizio di posta elettronica *Gmail*: e non è un caso che il blocco in questione sia stato disposto con esclusivo riguardo al protocollo di trasmissione (*Hyper Text Transfer Protocol over Secure socket layer*, https), che viene utilizzato per effettuare trasferimenti riservati di dati, che potrebbero invece essere intercettati più facilmente se inviati mediante protocolli differenti (come, ad esempio, l'http "semplice").

---

[27] R. Radu, *Negotiating Internet Governance*, Oxford, 2019, 109, corsivo aggiunto.

[28] Sottolinea l'importanza della Rete per lo sviluppo di questi eventi il rapporto stilato dal relatore speciale del Comitato per i diritti umani delle Nazioni Unite Frank La Rue *"on the promotion and protection of the right to freedom of opinion and expression*" doc. A/HRC/17/27 in www.ohchr.org. Sul fenomeno dei *social network* in una prospettiva di diritto internazionale ed europeo, anche solo per riferimenti bibliografici, ci permettiamo di rinviare a G.M. Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, 229 ss.

[29] Sono così chiamate le connessioni ad Internet, ormai in disuso nei Paesi industrializzati, che utilizzavano un apparecchio che trasformava i dati in suoni da trasmettere per il tramite della tradizionale rete telefonica a bassa frequenza.

DPCE online
ISSN: 2037-6677

Secondo le notizie trapelate, peraltro, pare che l'operazione di oscuramento posta in essere dal governo iraniano fosse prodromica a quella, ben più complessa, ambiziosa e illiberale, di realizzare una rete autonoma, il cui progetto di attuazione avrebbe visto una forte accelerazione dopo alcuni attacchi informatici contro il programma nucleare iraniano. Tuttavia, dal momento che la misura di oscuramento imposta dal governo pare fosse stata materialmente attuata, sotto il profilo tecnico, impartendo ai server situati sul territorio iraniano e che si occupano di risolvere i nomi di dominio in indirizzi IP[30], l'ordine di non effettuare tale operazione con riferimento ai siti indesiderati, tale misura sarebbe, a tutt'oggi, raggirabile semplicemente digitando, come destinazione da raggiungere, l'indirizzo IP del sito anziché il suo nome di dominio oppure utilizzando server di risoluzione DNS esterni al territorio iraniano e quindi non raggiunti dal detto ordine[31].

Come si vede, insomma, il dato tecnico (…il Codice di cui dicevamo) influisce su quello normativo.

E proprio sull'incapacità dei sistemi nazionali di disciplinare unilateralmente le questioni che ci occupano si era già pronunciato il *World Summit on Information Society* (WSIS) delle Nazioni Unite del 2003 (di cui diremo più diffusamente *infra*, nel par. 12) che aveva adottato, alla sua conclusione, una Dichiarazione di principi che riconosce alla *governance* di Internet una natura "multilivello", che necessita cioè del coinvolgimento di una pluralità di attori, sia di rilevanza pubblica, come Stati e organizzazioni internazionali (per l'individuazione di standard tecnici uniformi), sia di tipo privatistico, come operatori economici, ONG e individui, i quali vi esercitano competenze e funzioni differenziate[32].

Questo approccio, peraltro, rievoca alcuni dei temi oggetto di studi di *global administrative law*[33] che, come vedremo nel par. 12, potrebbero fornirci

[30] Per una spiegazione più dettagliata del modo di operare del sistema dei nomi di dominio rinviamo a G.M. Ruotolo, *Il sistema dei nomi di dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, in *Diritto dell'informazione e dell'informatica*, 2016, 33 ss.

[31] Ad esempio digitando http://64.233.183.104/ in luogo di www.google.it.

[32] World Summit on the Information Society, *Declaration of Principles*, WSIS-03/GENEVA/DOC/4-E, 12 December, 2003, Article 49, in www.itu.int.

[33] L. Boisson de Chazournes, *Changing Roles of International Organizations: Global Administrative Law and the Interplay of Legitimacies*, in *International Organizations Law Review*, 2009, 655 ss.; S. Cassese, *Il diritto amministrativo globale: una introduzione*, in *Rivista trimestrale di diritto pubblico*, 2005, 331 ss.; Id., *Administrative Law without the State? The Challenge of Global Regulation* in *New York University Journal of International Law and Politics*, 2005, 663 ss.; S. Chesterman, *Globalisation and Public Law: a Global Administrative Law?*, in J. Farrall, K. Rubenstein (Eds), *Sanctions, Accountability and Governance in a Globalised World*, Cambridge University Press, Cambridge, 2009, 75 ss.; M. D'Alberti, *Administrative Law and the Public Regulation of Markets in a Global Age*, in S.Rose-Ackerman, P.L. Lindseth (Eds), *Comparative Administrative Law*, Cheltenham, 2010, 63 ss.; D. C. Esty, *Good Governance at the Supranational Scale: Globalizing Administrative Law*, in *Yale Law Journal*, 2006, 1490 ss.; C. Harol, *Accountability as a Value in Global Governance and for Global Administrative Law*, in A. Gordon (Ed.), *Values in Global Administrative Law*, Oxford, 2011, 173 ss.; B. Kingsbury, L. Casini, *Global Administrative Law Dimensions of International Organizations Law*, in *International*

ulteriori chiavi di lettura del fenomeno in esame[34], assieme a quelli elaborati nel contesto del c.d. *informal international law*, di cui pure diremo.

Di certo c'è che da tempo, insomma, l'ordinamento internazionale è da più parti, e a vario titolo, chiamato a governare la Rete o, quanto meno, a fissare alcuni principi generali, così da (de)limitare la *domestic jurisdiction* degli Stati.

Peraltro non si può non sottolineare come il rapporto tra ordinamento internazionale e Internet sia bilaterale: se da un lato, infatti, il primo è chiamato a disciplinare la Rete e, per certi versi almeno, i comportamenti umani che vi si svolgono, d'altro canto lo stesso ordinamento, come vedremo, ha già subito delle modificazioni in conseguenza della diffusione delle informazioni da parte dei suoi operatori (funzionari governativi, di ONG, studiosi, avvocati) attraverso la Rete stessa[35].

Non si tratta, va detto, di un fenomeno del tutto nuovo.

Da sempre il progresso tecnologico informa di sé gli ordinamenti giuridici, compreso quello internazionale: si pensi alle numerose norme adottate per disciplinare i comportamenti degli Stati nello spazio extra-atmosferico[36], l'uso dell'orbita geostazionaria[37], l'aviazione civile[38], l'energia nucleare[39], la ricerca scientifica nell'alto mare[40], sorte solo quando il progresso tecnologico le ha rese necessarie[41].

Organizations Law Review, 2009, 319 ss.; B. Kingsbury, *The Concept of "Law" in Global Administrative Law*, in *European Journal of International Law*, 2009, 23 ss.; B. Kingsbury, N. Kirsch, R.B. Stewart, *The Emergence of Global Administrative Law*, in *New York University Public Law and Legal Theory Working Papers*, 2005; N. Krisch, B. Kingsbury (Eds), *Symposium on "Global Governance and Global Administrative Law in the International Legal Order"*, in *European Journal of International Law*, 2006, 1 ss.; M. Macchia, *Global Administrative Law Compliance : the Aarhus Convention Compliance Review System*, in *Revue européenne de droit public*, 2008, 1317 ss.; R. B. Stewart, *Il diritto amministrativo globale*, in *Rivista trimestrale di diritto pubblico*, 2005, 633 ss.

[34] G. Mayer, *Das Internet im öffentlichen Recht*, Berlin, 1999, *passim*.

[35] H.H. Perrit Jr., *The Internet Is Changing International Law*, in *Chicago-Kent Law Review*, 1998, 997 ss.

[36] Si pensi, ad esempio, alla Convenzione sulla responsabilità internazionale per danni causati da oggetti spaziali, aperta alla firma il 29 marzo 1972 ed entrata in vigore l'1 settembre dello stesso anno.

[37] Si veda l'Accordo sull'Organizzazione internazionale per i satelliti per telecomunicazioni, c.d. Convenzione, Intelsat, aperta alla firma il 20 agosto 1971 ed entrata in vigore il 12 febbraio 1973.

[38] Cfr. la Convenzione sull'Organizzazione internazionale per l'aviazione civile (ICAO).

[39] Cfr. lo Statuto dell'Agenzia internazionale per l'energia atomica, entrato in vigore il 29 luglio 1957, il Trattato che bandisce i test nucleari nell'atmosfera, nello spazio e sottacqua, entrato in vigore il 10 ottobre 1963, il Trattato sulla non proliferazione delle armi nucleari, entrato in vigore il 5 marzo 1970, il Trattato che vieta il collocamento di armi nucleari o di altre armi di distruzione di massa sul fondo e sul sottosuolo dei mari, entrato in vigore il 18 maggio 1972.

[40] Convenzione delle Nazioni Unite sul diritto del mare §§ 87(1)(f), 143, 238-65, in *U.N. series*, 1983.

[41] J. W. Dellapenna, *Law in a Shrinking World: The Interaction of Science and Technology with International Law*, in *Kentucky Law Journal*, 2000, 809 ss.

Tuttavia, mentre nei casi appena descritti le peculiarità "tecniche" dell'oggetto disciplinato hanno influenzato esclusivamente il contenuto *materiale* delle relative norme, nel caso di Internet l'influenza, a nostro modo di vedere, si è estesa, non solo al contenuto della disciplina di determinati settori particolarmente sensibili all'avvento della Rete (si pensi al caso del commercio elettronico o a nuove esigenze di disciplina di determinati servizi[42]), ma finanche al modo di operare *alcune funzioni* dell'ordinamento internazionale, in particolare con riguardo ai procedimenti di formazione e applicazione delle norme[43].

Peraltro, la qualificazione di Internet come bene pubblico globale (almeno in quanto infrastruttura; discorso differente andrebbe invece fatto con riguardo ai servizi ivi offerti da operatori privati) appare abbastanza consolidata in letteratura, sebbene con alcune distinzioni metodologiche e di approccio: mentre alcuni Autori concepiscono infatti la Rete come un bene pubblico globale "finale", altri vi vedono un bene "intermedio", strumentale per il perseguimento di altri e ulteriori beni come le "comunicazioni internazionali"[44].

I due distinti approcci, peraltro, a noi paiono essere anche alla base delle due differenti concezioni del diritto di accesso a Internet come strumentale per la tutela di altri diritti fondamentali (come quello all'informazione, all'espressione, allo sviluppo) e del diritto di accesso ad Internet in quanto diritto fondamentale autonomo[45].

Dal canto nostro, in alcuni scritti precedenti[46], avevamo già provato a inquadrare Internet come parte del *patrimonio comune dell'umanità*, al quale si applica, quindi, il relativo regime di diritto internazionale, che presenta non

---

[42] Sulle esigenze peculiari della prestazione di servizi *online* ci permettiamo di rinviare a G.M. Ruotolo, *Scritti di diritto internazionale*, cit., 61 ss.

[43] H.H. Perrit Jr, *The Internet is Changing the Public International Legal System*, in *Kentucky Law Journal*, 2000, 885 ss.; per un'analisi di taglio per così dire classico dell'influenza di Internet sulle attività del giurista contemporaneo v. S. Sica, V. Zeno-Zencovich, *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Il diritto dell'informatica*, 2010, 377 ss.

[44] Per i due approcci v. J. H. Sy, *Global Communications for a More Equitable World*, in I. Kaul, I. Grundberg, M.A. Sternd (Eds), *Global Public Goods. International Cooperation in The 21st Century*, New York/Oxford, 1999, 326 ss. e D.L. Spar, *The Public Face Of Cyberspace*, *ivi*, 344 ss.

[45] Ci è impossibile ricostruire in questa sede, anche solo per sommi capi, la prassi pertinente. Per limitarci ad un elemento recente, segnaliamo come la Corte suprema indiana, in una sentenza del 10 gennaio 2020, abbia fatto discendere il diritto fondamentale all'accesso ad Internet dalle norme relative alle libertà d'opinione ed espressione, sancendo come, di conseguenza, ogni restrizione al primo debba seguire i medesimi criteri e rispettare le medesime condizioni previste per le seconde. In generale, sul tema v. M. Bassini, *Internet e libertà d'espressione*, Roma, 2019; O. Pollicino, G. Pirtuzzella, *Hate speech and Fake news. A Comparative Constitutional Perspective*, Milano, 2020; G.M. Ruotolo, A little hate, worldwide! *Di libertà d'opinione e discorsi politici d'odio on-line nel diritto internazionale ed europeo*, in *Diritti umani e diritto internazionale*, 2020, 592 ss.

[46] Cfr. G.M. Ruotolo, *Internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012, 83 ss.

pochi punti di contatto con la categoria dei *beni pubblici globali*. Per una parte della dottrina, anzi, le due categorie addirittura coincidono[47].

Chiariamo che con la prima espressione faremo riferimento al regime giuridico di diritto internazionale applicabile e con la seconda ai beni ai quali il medesimo si applica; svilupperemo queste considerazioni più avanti, nei parr. 6-12.

Proviamo ora a capire se, allo stato di sviluppo attuale, l'ordinamento internazionale contenga norme di diritto internazionale generale, pattizio o derivato, in particolare prodotte da organizzazioni internazionali[48], specificamente rivolte a governare la Rete, oppure quali norme preesistenti possano ad essa essere applicate.

Inizieremo da queste ultime.

A tal fine, nella consapevolezza dei limiti materiali del presente lavoro, dopo una analisi delle conseguenze giuridiche dell'applicazione, ad Internet, della categoria dei beni patrimonio comune dell'umanità oggetto di norme di diritto internazionale generale, passeremo ad analizzare il meccanismo di gestione del sistema dei nomi di dominio, in quanto elemento fondamentale per l'esistenza di Internet e in quanto modello normativo di particolare interesse e rilevanza.

5. Le norme di diritto internazionale preesistenti e l'*interventionist approach*

Cerchiamo quindi ora di comprendere se vi siano norme di diritto internazionale preesistenti all'avvento di Internet, nate cioé per disciplinare fattispecie da questa differenti, che, in considerazione del loro oggetto e del loro scopo, possano essere applicate anche alla Rete.

Sotto il profilo dogmatico, l'approccio secondo il quale lo studio di fattispecie giuridiche connesse ad Internet può essere condotto alla luce di categorie e concetti "tradizionali" dell'ordinamento internazionale è stato criticamente definito *interventionitst approach* proprio qualora conduca all'applicazione analogica, a fattispecie *online*, di norme di diritto internazionale precedentemente concepite per disciplinare situazioni "reali".

Secondo tale critica l'analogia sarebbe, infatti, conseguenza ingiustificata del fatto che, per supplire all'assenza di un quadro normativo specificamente concepito, la dottrina internazionalistica verrebbe spinta, dall'*horror vacui* giuridico, ad affrontare le questioni con i propri strumenti,

[47] E. Egede *Common Heritage of Mankind*, in Oxford Bibliografies, reperibile online, dichiara la sostanziale coincidenza tra la categoria e quella dei beni pubblci globali: la prima, infatti, "represents the notion that certain *global commons* or elements regarded as beneficial to humanity as a whole should not be unilaterally exploited by individual states or their nationals, nor by corporations or other entities, but rather *should be exploited under some sort of international* arrangement or *regime* for the benefit of mankind as a whole". Corsivo aggiunto.

[48] Cfr. T. Fuentes-Camacho (Ed.), *Les dimensions internationales du droit du cyberspace*, Paris, 2000, *passim*; G.M. Ruotolo, *Internet (diritto internazionale)*, in *Enciclopedia del diritto*, Annali, VII, 545 ss.

per assicurarsi che le fattispecie "digitali" siano regolate mediante le norme di cui è esperta, nel tentativo di intervenire nei problemi del mondo, al fine di gestirli[49].

In questo contesto ci è preclusa un'analisi più approfondita di questo orientamento e delle critiche ad esso sottese, ma è quanto meno il caso di sottolineare come esse, che riguardano in essenza il modo in cui gli internazionalisti concepiscono la loro professione e la loro funzione[50], non ci pare siano comunque applicabili a tutti i casi in cui vi sia stata un'esplicita attività normativa di rilevanza internazionalistica, da parte di Stati o organizzazioni internazionali competenti.

6. *(Segue)*: Internet come patrimonio comune dell'umanità e/o bene pubblico globale

Come abbiamo accennato nel par. 4, le caratteristiche di Internet ci spingono ad andare a cercare, in primo luogo, tra le norme di diritto internazionale che, nel corso del tempo, sono sorte nella prassi o sono state adottate, con l'obbiettivo di disciplinare l'uso da parte degli Stati di risorse da questi non appropriabili in modo unilaterale – cioè sulle quali non è possibile o legittimo esercitare in maniera *esclusiva* la sovranità – e il cui sfruttamento, al contempo, presuppone il possesso di elevate competenze tecnologiche.

Le norme dotate di queste caratteristiche sono, nella maggior parte dei casi, relative a beni che sono stati ritenuti parte del patrimonio comune dell'umanità[51] e ai quali, quindi, è applicabile il relativo regime di diritto internazionale[52].

---

[49] J. d'Aspremont, *Cyber Operations and International Law: An Interventionist Legal Thought*, in *Jou. Conf. Sec. L*, 2016, *ACIL Research Paper* 2016-11, reperibile su ssrn.com.

[50] «Short of conferral of any new express responsibilities, international lawyers have nowadays found themselves ostracized, their fate being reduced to either being the bored experts of overly discussed fields or the distant observers of phenomena deemed better addressed through non-legal regulatory tools»; così d'Aspremont, *Cyber Operations*, cit. Per un'affascinante analisi della funzione del diritto internazionale nella storia e del modo di concepire il "mestiere" di internazionalista si veda Koskenniemi, *The Gentle Civilizer of Nations. The Rise and Fall of International Law 1870-1960*, Cambridge, 2001, trad. it. a cura di Gozzi, Gradoni, Turrini, Bari, 2012, *passim*.

[51] Con riguardo ad Internet avevamo già proceduto a siffatta qualificazione in G.M. Ruotolo, *Internet-ional Law*, cit., nonché in Id., *Internet (diritto internazionale)*, cit., 545 ss. Nel medesimo senso, da ultimo, si veda A. Segura Serrano, *The Cyberspace as Common Heritage of Mankind*, in M. Iovane, F.M. Palombino, D. Amoroso, G. Zarra (Eds), *The Protection of General Interests in Contemporary International Law. A Theoretical and Empirical Inquiry*, Oxford, 2021, 189 ss.

[52] Sul concetto cfr. A.C. Kiss, *La notion de patrimoine commun de l'humanité*, in *Recueil des Cours del l'Académie de droit International de la Haye*, 1989, nonché K. Baslar, *The Concept of the Common Heritage of Mankind in International Law*, The Hague, 1998, il quale, però, pur riconoscendo esplicitamente di aver utilizzato Internet per reperire *tutte* le fonti utilizzate per scrivere il suo libro, non si pone affatto il problema di comprendere se quello strumento da lui utilizzato così diffusamente abbia caratteristiche tali da poter essere ricompreso nell'oggetto della sua analisi. J. Buttigieg, *The Common Heritage of Mankind from the Law of the Sea to the*

È il caso di ricordare come norme siffatte siano state spesso segnalate come un indice del passaggio dal c.d. diritto internazionale della coesistenza tra Stati – cui fa da corollario la sostanziale coincidenza degli obblighi che gravano sugli stessi alla luce del diritto internazionale – al diritto internazionale c.d. della cooperazione, basato invece su principi improntati ad una parità "di partecipazione" alla vita della Comunità internazionale, ma che consentirebbe la differenziazione degli obblighi gravanti sugli Stati in base alle "funzioni" da questi assunte all'interno di un particolare regime giuridico, anche in funzione del differente livello di sviluppo dei medesimi[53].

A queste due categorie, peraltro, è stata poi affiancata quella del c.d. diritto internazionale dell'integrazione: secondo una parte della dottrina, infatti, l'ordinamento internazionale contemporaneo si caratterizzerebbe come una struttura integrata, organizzata in cerchi concentrici[54], nella quale ordinamenti di vario genere (internazionale in senso "tradizionale", interni, ordinamenti speciali delle organizzazioni internazionali, strutture informali), composti a loro volta da fonti giuridiche di vario genere e idonee a produrre effetti differenziati, trovano coordinamento e integrazione in un sistema giuridico che si rivolge ad una società transnazionale e *multistakeholder*[55],

---

Human Genome and Cyberspace, reperibile online.

[53] Si pensi, ad esempio, al c.d. trattamento differenziale per i Paesi in via di sviluppo. Tra gli altri, sul punto, si veda G. Abi Saab, *Whither the International Community?*, in *European Journal of International Law*, 1998, 248 ss.

[54] Non è affatto un caso, secondo noi, che F. Marella, *op. loc. cit.*, usi il medesimo modello per la *lex mercatoria*.

[55] Varie e differenti sono le premesse teoriche e le prospettive adottate con riguardo a quello che per alcuni è il c.d. diritto "globale" o "transnazionale": ci limitiamo a registrare come a una prima elaborazione che concepiva il diritto transnazionale come una sorta di somma di diritto pubblico nazionale e diritto internazionale si sono poi affiancati approcci che hanno ricondotto il fenomeno al pluralismo giuridico, e in particolare alla frammentazione dell'ordinamento internazionale in numerosi sub-regimi , altri che hanno interpretato la società civile come una sorta di "nuovo" legislatore e, di conseguenza, tra le altre cose, hanno affermato l'emersione di un "transnational private legal ordering" dal quale il diritto internazionale sarebbe escluso , mentre altri ancora, per cercare di dare senso a processi giuridici che non sarebbero adeguatamente rilevati dal diritto internazionale – in quanto connessi a norme create mediante meccanismi differenti da quest'ultimo, il quale contempla la centralità degli Stati – hanno concepito il fenomeno della regolamentazione giuridica di beni di rilevanza transnazionale come il prodotto dell'inte(g)razione tra i vari ordinamenti interni . Insomma, la frammentazione del diritto globale sarebbe più radicale di quanto possa essere compreso da ogni singola prospettiva – giuridica, politica, economica o culturale – che ne tenti una riconduzione ad unità; in particolare la frammentazione giuridica che ne consegue sarebbe il riflesso di una frammentazione multidimensionale della società globale in quanto tale. Tuttavia un tentativo di ricondurre ad unità normativa il diritto globale (cioè il diritto che regolamenta i detti beni di rilevanza "globale", appunto) potrebbe essere effettuato mediante la ricostruzione della compatibilità normativa dei frammenti che lo compongono, da perseguire mediante "conflicts law to establish a specific network logic, which can effect a loose coupling of colliding units"; così A. Fischer-Lescano, G. Teubner, *Regime-Collisions: The Vain Search For Legal Unity In The Fragmentation Of Global Law*, in *Michigan Journal of International Law*, 2004, 999 ss., in part. 1004. Tra gli altri si vedano anche P.S. Berman, *Global Legal Pluralism: A Jurisprudence of Law beyond Borders*, New York, 2012; W.W. Burke-White,

DPCE online
ISSN: 2037-6677

Vedremo come si tratti di un modello particolarmente interessante per la comprensione dei fenomeni che stiamo studiando.

Ricordiamo che la nozione di patrimonio comune dell'umanità, che è rintracciabile già nel diritto internazionale classico del XVII secolo[56], fu, come noto, riattualizzata nel 1967 dall'ambasciatore maltese Arvid Pardo in occasione della Terza conferenza delle Nazioni Unite sul diritto del mare, e venne quindi inserita dapprima nella risoluzione dell'Assemblea generale n. 2749 (XXV) del 17 dicembre 1970 – secondo la quale l'Area dei fondi marini e degli oceani e il loro sottosuolo, che si trovano oltre i limiti delle giurisdizioni nazionali, così come le loro risorse, sono patrimonio comune dell'umanità e, pertanto, la loro esplorazione e il loro sfruttamento devono essere condotti a beneficio di tutta l'umanità – e successivamente nella Parte XI della Convenzione delle Nazioni Unite sul diritto del mare (CNUDM), relativa proprio alla detta Area[57].

Un concetto analogo, in realtà, anche se non così definito, era già apparso nel Trattato sull'Antartico del 1959, e in una ancor precedente

International Legal Pluralism, in Michigan Journal of International Law, 2004, 979 ss.; O.K. Fauchald, A. Nollkaemper (Eds), *The Practice of International and National Courts and the (De-) Fragmentation of International Law*, Oxford/Portland, 2012;.; G.P. Calliess, *Transnational Law*, in M. Juergensmeyer, H. Anheier, V. Faessel (Eds), *The Encyclopedia of Global Studies*, Thousand Oaks, CA, 2012, 1035 ss.; T. C. Hallidfay, G. Shaffer (Eds), *Researching Transnational Legal Orders*, Cambridge, 2015; V. Jackson, *Constitutional Engagement in a Transnational Era*, Oxford, 2012, p, 50 ss.; P.C. Jessup, *Transnational Law*, New Haven, 1956; J. Klabbers, G. Palombella (Eds), *The Challenge of Inter-Legality*, Cambridge, 2019; N. Krisch, *Beyond Constitutionalism: The Pluralist Structure Of Postnational Law*, Oxford, 2012; G.C. Shaffer (Ed.), *Transnational Legal Ordering and State Change*, Cambridge, 2013; G.C. Shaffer, C. Coye, *From International Law to Jessup's Transnational Law, from Transnational Law to Transnational Legal Order*, in Zumbansen (Ed.), *The Many Lives of Transnational Law. Critical Engagements with Jessup's Bold Proposa*l, Cambridge, 2020, 126 ss.; B. Tamanaha, *Understanding Legal Pluralism: Past to Present, Local to Global*, in *Sydney Law Review*, 2007, 374 ss.; G. Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization*, New York, 2012; W. Twining, *Globalisation and Legal Theory. Evanston*, 2000; Zumbansen, *Transnational Legal Pluralism*, in Transnational Legal Theory, 2010, 141 ss. Noi ci siamo occupati della questione, con riguardo alla disciplina del sistema dei nomi di dominio, in G.M. Ruotolo, *Fragments of Fragments. The Domain Name System Regulation: "Global" Law or Informalization of the International Legal Order?*, in *Computer Law & Security Review*, 2017, 159 ss. al quale facciamo rinvio. *Adde*, da ultimo, per la letteratura italiana, R. Tarchi, *Diritto transnazionale o diritti transnazionali? Il carattere enigmatico di una categoria giuridica debole ancora alla ricerca di un proprio statuto*, in *Osservatorio sulle fonti*, 2021, 6 ss. il quale definisce il tema "complesso, sfuggente, poliedrico, enigmatico e, comunque, trasversale ad una molteplicità di settori giuridici" e si pone dubbi in merito al fatto che "quanto viene ricondotto sotto l'etichetta di diritto(i) transnazional(e) possa effettivamente acquistare anche una valenza prescrittiva e, quindi, qualificarsi come diritto in senso proprio".

[56] Si pensi, ad esempio, alle *res communes omnium* di Hugo Grotius. Cfr. M. Schermaier, *Res Communes Omnium: The History of an Idea from Greek Philosophy to Grotian Jurisprudence*, in *Grotiana*, 2009, 1, 20 ss.

[57] T. Scovazzi, *Fondi marini e patrimonio comune dell'umanità*, in *Rivista di diritto internazionale*, 1984, 249 ss.; A.G.O. Elferink, E. J. Molenaar (Eds), *The International Legal Regime of Areas Beyond National Jurisdiction*, Leiden, 2010.

dichiarazione dell'Assemblea generale relativa ai "principi giuridici governanti le attività degli Stati nell'esplorazione e nell'uso dello spazio esterno", adottata il 13 dicembre 1963, che faceva riferimento agli "interessi comuni dell'umanità" nell'esplorazione del cosmo ed indicava che "ogni Stato ha assoluta libertà di movimento, e nessuno può dichiarare la propria sovranità su parti di esso", nonché, ancora, nel successivo Trattato del 1967 relativo alle attività degli Stati nell'esplorazione e l'utilizzazione dello spazio.

Anche il Trattato del 1979relativo alle attività degli Stati sulla Luna e gli altri corpi celesti, all'art. 11 provvede a definire patrimonio comune dell'umanità la Luna e le sue risorse naturali.

Ulteriori applicazioni del concetto sono poi contenute nella Convenzione UNESCO del 16 novembre 1972 sui beni culturali e nazionali di eccezionale valore nonché, nella Dichiarazione universale sul genoma umano adottata, ancora dall'UNESCO, l'11 novembre 1997, secondo la quale esso non può essere oggetto di appropriazione da parte di Stati o di privati[58].

Quest'ultima dichiarazione, in particolare, conferma una volta di più l'estrema versatilità della categoria in esame, utilizzabile per la tutela di beni tra loro anche molto diversi per caratteristiche e funzioni.

Nell'impossibilità di analizzare compiutamente le norme alle quali abbiamo fatto riferimento, ci limiteremo ad individuarne i tratti distintivi comuni: esse comportano l'assoggettamento dei beni tutelati a un regime di diritto internazionale volto a limitare la libertà di sfruttamento degli Stati[59], essenzialmente imponendo loro quattro distinte restrizioni: *a)* un divieto di estensione della sovranità statale ai beni patrimonio comune e, in particolare, il divieto di appropriazione unilaterale; *b)* l'obbligo di assoggettamento dei beni in questione ad un regime internazionale di cooperazione in ordine alla loro gestione; *c)* il divieto di una loro utilizzazione, anche per interessi generali, tale da arrecare pregiudizio all'ambiente; *d)* l'obbligo di utilizzare tali beni esclusivamente per fini pacifici e, quindi, il divieto di porvi in essere attività che siano irrispettose del diritto internazionale e, in particolare, dei principi di diritto internazionale generale e di quelli contenuti nella Carta delle Nazioni Unite relativi al mantenimento della pace e della sicurezza internazionale.

Quindi, nel momento in cui un determinato bene è individuato come parte del patrimonio comune dell'umanità, viene *in re ipsa* assoggettato *quanto meno* ai quattro principi appena illustrati; tale regime, peraltro, nel suo complesso, sarebbe ormai incorporato nel diritto internazionale generale, di

[58] C. Kuppuswamy, *The International Legal Governance of the Human Genome*, London, 2012; S. Marchisio, *Patrimonio comune dell'umanità (Dir. Internaz)*, in *Enciclopedia Il Sole 24 Ore*, Milano, 2007, 728 ss; Id., *L'ONU – Il diritto delle Nazioni Unite*, Bologna, 2012, 83 ss.; J.M. Spectar, *The fruit of the human genome tree: cautionary tales about technology, investment, and the heritage of humankind*, in *Loyola of Los Angeles*, 2001, 1 ss.

[59] Sulle particolarità del regime relativo al patrimonio comune dell'umanità cfr. U. Villani, *Il regime di sfruttamento dei fondi marini*, in Istituto Italo-latinoamericano, *Prospettive del diritto del mare all'alba del XXI secolo*, Roma, 1999, 149 ss., in part. 162.

cui rappresenterebbe finanche un "basic principle"[60], per alcuni Autori addirittura di *ius cogens*[61].

Abbiamo già visto come il concetto di bene patrimonio comune dell'umanità sia andato incontro a un progressivo ampliamento, in considerazione, in particolare, del progresso tecnologico, e sia passato a ricomprendere finanche il genoma umano, "oggetto" quanto mai distante dall'Area dei fondi marini o dai corpi celesti per i quali il regime era originariamente stato pensato, ma che con questi ha in comune una serie di caratteristiche intrinseche che ne giustificano l'assoggettamento alla medesima disciplina[62].

Ebbene, Internet, come da noi evidenziato anche in scritti di dieci anni or sono, a nostro giudizio, possiede tutti i requisiti necessari per essere il più giovane membro della famiglia dei beni sottoposti a questo regime: essa, infatti, rappresenta una risorsa esauribile – per una prova dell'esauribilità basti pensare al problema relativo agli indirizzi IPv4 – non appropriabile da parte di un singolo Stato, e in merito all'opportunità della cui conservazione, in quanto di interesse comune, si sono già registrate numerose prese di posizione degli Stati[63]; sotto quest'ultimo profilo, peraltro, già nel 1999 l'Assemblea generale delle Nazioni Unite aveva avuto modo di notare che "the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation"[64]. E nel medesimo senso si veda anche lo *Statement* del 15 dicembre 2015 del delegato maltese alle Nazioni Unite in occasione del World Summit on Information Society Review Process.

A queste conclusioni ci conducono, da un lato, la riconosciuta importanza globale del bene in questione e dell'esistenza di un interesse "collettivo" degli Stati al mantenimento delle sue piene funzionalità (sul punto si vedano anche le dichiarazioni relative alla gestione del sistema dei nomi di dominio, *infra*, par. 12), dall'altro i numerosi atti adottati in seno a svariate organizzazioni internazionali, dai quali emerge un *consensus* in merito alla necessità di fare in modo che la disciplina della Rete sia oggetto di una condivisione da parte di tutti i soggetti interessati, pubblici e privati:

---

[60] L'analisi della consuetudinarizzazione del principio in parola è svolta da R. Wolfrum, *The Principle of Common Heritage of Mankind*, in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 1983, 312 ss., reperibile all'indirizzo www.hjil.de.

[61] Attribuisce al principio natura di *ius cogens* già E. Salamanca Aguado, *La Zona Internacional de los Fondos Marinos – Patrimonio Común de la Humanidad*, Madrid, 2003, 298.

[62] Cfr. C. Kuppuswamy, *op. cit.*, 95 ss.

[63] J. Malcolm, *The Space Law Analogy to Internet Governance*, in *Journal of Law, Information and Science*, 2007, 57 ss. Su Internet come patrimonio comune dell'umanità cfr. A. Segura Serrano, *Internet Regulation*, cit., 231 *ss.*, nonché H. Spang-Hanssen, *Public International Computer Network Law Issues*, 2006, *passim.*

[64] Risoluzione A/RES/53/70 del 4 gennaio 1999, "Developments in the field of information and telecommunications in the context of international security".

e non a caso gli atti adottati già più di dieci anni or sono nel corso del dodicesimo Congresso delle Nazioni Unite sulla prevenzione dei crimini e la giustizia penale svoltosi in Brasile dal 12 al 19 aprile 2010 definivano esplicitamente il cyberspazio "the fifth common space — after land, sea, air, and outer space"[65].

Sotto il profilo metodologico, poi, è il caso di chiarire come l'estensione ad Internet di obblighi di diritto internazionale previgenti, conseguenza dell'applicazione del regime dei beni patrimonio comune dell'umanità, debba necessariamente tenere in costante considerazione la logica secondo la quale "to treat unequal matters differently according to their inequality is not only permitted but required"[66] e come, di conseguenza, sarà necessario procedere in via interpretativa al "riadattamento" delle norme da applicare.

7. *(Segue)*: *a)* il divieto di appropriazione unilaterale di Internet da parte di singoli Stati

L'applicazione ad Internet del principio di non appropriazione, come già avviene per altri spazi comuni come l'alto mare o gli spazi extra-atmosferici, vieta agli Stati di trattare la Rete – e quindi anche le parti di essa che, fisicamente, sono collocate in zone sottoposte alla loro sovranità – come se fosse sotto il loro dominio esclusivo e, quindi, di porvi in essere unilateralmente comportamenti che impediscano in tutto o in parte agli altri Stati di utilizzarla o, ancora, di limitare la loro discrezionalità in merito al suo uso. Ciò ci induce a concludere per l'esistenza, quanto meno, di un divieto, in capo a tutti gli Stati, a porre in essere qualunque azione o comportamento idonei a mettere in pericolo l'esistenza del Web come è oggi inteso, contro il quale si sta muovendo, tuttavia, una certa tendenza alla frammentazione di Internet ("Splinternet").

8. *(Segue)*: *b)* l'obbligo internazionale di cooperazione tra gli Stati in ordine alla gestione di Internet

In secondo luogo l'esistenza di un obbligo, di natura procedurale, di cooperazione – che a noi pare assumere la triplice forma di obbligo di informazione, consultazione e *de negotiando*, ma non, si badi, *de contrahendo* – impone agli Stati di creare meccanismi, o utilizzare *fora* già esistenti, per dibattere le problematiche connesse all'uso della Rete e quindi, quanto meno cercare, in quelle sedi, di raggiungere una qualche forma di *consensus* in merito alle misure di disciplina e di uso del bene comune.

[65] Cfr. doc. UN A/conf.213/IE/7 del 23 marzo 2010.
[66] Cfr., in questo senso, l'opinione dissenziente del Giudice Tanaka nel caso *South West Africa* deciso dalla Corte internazionale di giustizia, in *ICJ Reports*, 1996, 306.

DPCE online
ISSN: 2037-6677

9. *(Segue)*: *c)* il divieto di inquinamento di Internet

Il divieto di inquinamento, forse più degli altri, va fatto oggetto di un'interpretazione che consenta di adattarlo alle peculiarità di Internet: lasciando da parte ogni considerazione sul fatto che è stato calcolato che ogni secondo di consultazione del Web da parte di un singolo utente rilascia nell'atmosfera 0,2 grammi di anidride carbonica, generati dall'utilizzo del combustibile necessario alla produzione della corrente elettrica impiegata per alimentare le apparecchiature connesse, e che quindi la Rete è fonte di inquinamento ambientale *reale*, dobbiamo qui comprendere quali potrebbero essere i comportamenti che hanno luogo *online*, inibiti agli Stati in forza di tale divieto.

A tal fine procederemo a ricostruire, brevemente, come il medesimo si atteggi con riferimento agli spazi reali, per poi procedere al suo riadattamento alle caratteristiche di Internet.

Il divieto di inquinamento, per così dire, tradizionale, delle zone dichiarate bene comune dell'umanità estende a queste ultime il più generale divieto di inquinamento delle zone sottoposte alla sovranità di altri soggetti di diritto internazionale[67]. Quest'ultimo divieto, come noto, appare costruito come un corollario del divieto di ingerenza e del diritto degli Stati all'integrità e si sostanzia nella "obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability"[68] gravante su tutti gli altri Stati. La sentenza arbitrale resa il 16 novembre 1957 nella controversia tra Francia e Spagna relativa al lago *Lanoux* ha altresì affermato l'esistenza di un "principle which prohibits the upstream State from altering the waters of a river in such a fashion as seriously to prejudice the downstream State"[69], e la *Declaration of the United Nations Conference on the Human Environment* adottata a Stoccolma nel 1972, al principio 21, riconosce che, in conformità alla Carta delle Nazioni Unite e ai principi del diritto internazionale, gli Stati hanno "the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction", ribadendo con ciò l'esistenza di un divieto di diritto internazionale generale di porre in essere, anche all'interno dei propri confini nazionali, comportamenti che danneggino l'ambiente in altri Stati o in zone non sottoposte alla sovranità esclusiva di alcuno Stato[70].

---

[67] E. Egede, *Africa and the Deep Seabed Regime: Politics and International Law of the Common Heritage of Mankind*, Berlin-Heidelberg, 2011, 55 ss.
[68] Arbitrato sull'isola di Palmas (Paesi Bassi c. Stati Uniti), decisione del 4 aprile 1928, in UNRIAA, II, 839
[69] In dottrina P.M. Dupuy, J.E. Viñuales, *International Environmental Law*, Cambridge, 2015, 5 ss; Wehling, *Nile Water Rights. An international law perspective*, Berlin, 2020, 26 ss.
[70] La dichiarazione è reperibile all'indirizzo legal.un.org/avl/pdf/ha/dunche/dunche_e.pdf.

Anche la CNUDM, dopo aver ricordato, all'art. 193, che gli Stati sono titolari di un "sovereign right to exploit their natural resources pursuant to their environmental policies and in accordance with their duty to protect and preserve the marine environment", al par. 2 dell' art. 194, impone loro di adottare "all measures necessary to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment, and that pollution arising from incidents or activities under their jurisdiction or control does not spread beyond the areas where they exercise sovereign rights in accordance with this Convention". La Convenzione, che sul punto dovrebbe avere valore di codificazione del diritto internazionale generale, conferisce quindi al divieto di inquinamento una portata non solo *negativa*, ma anche *positiva*, imponendo agli Stati di adottare misure preventive e repressive dell'inquinamento stesso.

Infine, ricordiamo che il principio n. 2 della Dichiarazione di Rio su sviluppo e ambiente del 1992 sottolinea che "States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental and developmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national".

Anche la Corte internazionale di giustizia, nel parere consultivo sulla liceità dell'uso e della minaccia delle armi nucleari dell'8 luglio 1996, ha riconosciuto che "the environment is under daily threat and that the use of nuclear weapons could constitute a catastrophe for the environment. The Court also recognizes that the environment is not an abstraction but represents the living space, the quality of life and the very health of human beings, including generations unborn. *The existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of other States or of areas beyond national control is now part of the corpus of international law* relating to the environment"[71].

Si tratta ora di cercare di adattare questi concetti all'ambiente di Internet: e allora, se per inquinamento si intende la sua alterazione per il tramite di fattori patogeni di origine umana, nel caso di Internet si può fare riferimento all'inquinamento "virtuale" dell'ambiente informatico posto in essere mediante software malevolo. Il divieto in questione, peraltro, a nostro giudizio, va letto non solo come relativo alla diffusione *diretta*, da parte degli Stati, di strumenti siffatti in misura e con caratteristiche tali da porre in pericolo l'esistenza della Rete, ma anche come obbligo gravante sugli stessi

In dottrina cfr. T. Stevens, *International Courts and Environmental Protection*, Cambridge, 2009, 3 ss.

[71] ICJ Reports, 1996, pp. 241-242, par. 29; corsivo nostro. In dottrina v. M. Fitzmaurice, *Contemporary Issues in International Environmental Law*, Cheltenham/Notrhampton, 2009; E. Louka, *International Environmental Law – Fairness, Effectiveness and World Order*, Cambridge, 2006.

di porre in essere misure preventive e repressive per evitare che strumenti siffatti siano diffusi *in maniera massiva* da privati sottoposti alla loro *jurisdiction*.

Va chiarito che i divieti in questione non ci paiono però avere contenuto e portata tali da vietare *ogni* comportamento statale che implichi la progettazione e/o la diffusione di *ogni* strumento informatico malevolo, ma solo, e più limitatamente, di quelli dotati di un livello di offensività tale da bloccare il funzionamento della Rete stessa o di suoi importanti rami (si pensi, a mero titolo di esempio, al blocco di uno o più d'uno dei *root server*)[72].

10 *(Segue)*: *d)* l'obbligo di uso pacifico: guerra informatica e legittimità delle reazioni

Passiamo ora a esaminare quali sono le conseguenze dell'applicazione alla Rete dell'obbligo gravante sugli Stati di un suo uso esclusivamente pacifico, il quale pure discende dalla qualificazione di Internet come bene comune (oltre che, come ovvio, dal divieto generalizzato della minaccia e dell'uso della forza). Questo profilo, evidentemente, presuppone la possibilità di inquadrare determinati strumenti informatici volti esclusivamente a danneggiare i sistemi sui quali vengono eseguiti come forma di uso della forza, vietato dal diritto internazionale, la c.d. *cyber war*, nonché con il tema del c.d. *cyber terrorismo* (su cui cfr. *infra*, il par. 11) e delle possibili legittime reazioni statali[73].

[72] Nel febbraio 2012 l'organizzazione di *hacker* nota come "Anonymous" ha dichiarato che, al fine di impedire tutte le transazioni finanziare *online*, avrebbe posto in essere un "global blackout" della Rete, anche se volutamente solo temporaneo, mediante un attacco contemporaneo a tutti i 13 *root server* come reazione di rappresaglia alla crisi economica globale; tuttavia o l'attacco non c'è stato oppure i congegni di sicurezza del sistema DNS hanno resistito egregiamente, dal momento che non si sono registrate significative interruzioni al DNS medesimo. Sulla *governance* del sistema DNS nel diritto internazionale, anche solo per ulteriori riferimenti bibliografici, ci permettiamo di rinviare a G.M. Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, 5 ss.

[73] Si tratta di tema complesso, sul quale si è sviluppata un'imponente letteratura e in relazione al quale non abbiamo alcuna pretesa di completezza. Cfr., oltre all'imponente tentativo di "codificazione" della prassi svolto da Schmitt (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2013, anche per riferimenti, H. Diniss, *Cyber Warfare and the Laws of War*, Cambridge, 2012; H. Lobel, *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, in *Texas International Law Journal*, 2012, 617 ss.; J. Goldsmith, *How Cyber Changes the Laws of War*, in *European Journal of International Law*, 2013, 129 ss.; J.A. Green (Ed.), *Cyber Warfare. A Multidisciplinary Analysis*, Oxon/New York, 2015; H.J. Heintze, Thielbörger (Eds), *From Cold War to Cyber War. The Evolution of the International Law of Peace and Armed Conflict over the Last 25 Years*, New York/Dodrecht/London, 2016; U. Pagallo, *Cyber Force and the Role of Sovereign States in Informational Warfare*, in *Philosophy and Technology*, 2015, 407 ss.; T. Rid, *Cyber War Will Not Take Place*, Oxford, 2013; M. Roscini, *Cyber Operations and the Use of Force*, Oxford, 2014; S. Shackleford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, in *Berkeley Journal of International Law*, 2009, 192 ss.; M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; H. Lahmann, *Unilateral remedies to Cyber Operations. Self-Defence Countermeasures, Necessity and the Question of Attribution*,Cambridge, 2020.

Dobbiamo innanzitutto chiarire che con la prima espressione (*cyber war* o guerra informatica) facciamo riferimento all'uso di strumenti informatici, più di frequente, ma non esclusivamente, di tipo *software*, da parte di uno Stato, con l'intento di ledere altri soggetti di diritto internazionale, con un approccio analogo a quello della guerra cinetica, ma senza necessariamente mirare alla loro *debellatio*. La definizione tradizionale di guerra nel diritto internazionale che, come noto, concepisce la stessa come "a contention between two or more States , through their armed forces, for the purposes of overpowering each other and imposing such conditions of peace as the victor pleases"[74] e ritiene quindi connaturata con la stessa l'intenzione di ogni belligerante di annientare l'avversario, sembrerebbe escludere dall'idea stessa di "guerra" comportamenti con obbiettivi più limitati, come avverrebbe nel caso di una *cyber war*. Tuttavia definizioni più recenti di guerra, come quella elaborata dal Tribunale penale internazionale per l'ex Yugoslavia nel caso *Tadić*, secondo la quale un "armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organised armed groups or between such groups within a State"[75], sono idonee a comprendere nel concetto delineato anche conflitti armati con obiettivi meno "ambiziosi". Peraltro, una guerra informatica e una cinetica differiscono tra loro anche per ulteriori elementi, legati alla difficoltà di individuare concretamente, nel caso di attacchi informatici, lo Stato aggressore[76], nonché in quella di limitarne gli effetti collaterali e, di conseguenza, di rispettare le norme del *jus in bello*.

Cerchiamo ora di comprendere se i comportamenti appena descritti, qualora fossero riconducibili a Stati, rientrino tra quelli vietati dal diritto internazionale contemporaneo in quanto forme di minaccia o, addirittura, di uso della forza; ricordiamo che, come noto, l'interpretazione maggioritaria dell'art. 2, par. 4 della Carta delle Nazioni Unite e della corrispondente norma di diritto internazionale generale, ritiene che il divieto della minaccia e dell'uso della forza ivi previsto sia esclusivamente relativo alla forza *militare*[77].

Tuttavia il divieto in questione potrebbe esser fatto oggetto di un'interpretazione evolutiva che includa anche comportamenti quali quelli di cui ci stiamo occupando, o almeno alcuni di essi. Ricordiamo infatti come la

[74] L.F.L. Oppenheim, *International Law*, Roxburgh, 1920, 67.
[75] Jurisdiction Decision, International Criminal Tribunal for Former Yugoslavia (ICTY) Case No. IT-94-1-AR72, para 70.
[76] Sulla questione dell'attribuzione dei comportamenti v. H. Lahmann, op. cit., 65 ss. e T. Rid, B. Buchanan, *Attributing Cyber Attacks*, in *The Journal of Strategic Studies*, 2015, 4 ss. Si veda anche B.J. Egan, *International Law and Stability in Cyberspace*, in *Berkeley Journal of International Law*, 2017, 169 ss.
[77] B. Conforti, M. Iovane, *Diritto internazionale*, XII ed., Napoli, 2021, 450 ss.; C. Focarelli, *Diritto internazionale*, VI ed., Padova, 2021, 636 ss.; F.M. Palombino, *Introduzione al diritto internazionale*, Bari/Roma, 2019, 36 ss.; J. Klabbers, *International Law*, 3rd ed., Cambridge, 2021, 206 ss.; U. Villani, *Lezioni di diritto internazionale*, Bari, 2021, 241 ss.

DPCE online
ISSN: 2037-6677

Corte internazionale di giustizia, nel noto caso delle *Attività militari e paramilitari in Nicaragua*, abbia fatto rientrare nel divieto della minaccia e dell'uso della forza – ma, come noto, non in quello di attacco armato – anche attività che non sono direttamente riconducibili all'uso della forza militare in senso stretto, come l'addestramento e la mera fornitura di armi a milizie irregolari operanti sul territorio di una altro Stato[78]. Ancora, nel parere del 1996 relativo alla *Legittimità dell'uso della forza*, la Corte ha altresì chiarito come il sistema della Carta non contenga alcuna elencazione o elencazione tassativa del concetto di "arma" rispetto al divieto dell'uso della forza.

Sulla base di questi elementi una parte la dottrina, al fine di aggiornare l'ordinamento internazionale alle evoluzioni tecnologiche e all'esigenza di combattere nuove forme di minaccia alla pace e alla sicurezza internazionale, ha avanzato l'ipotesi di considerare quanto meno *alcuni* attacchi informatici come vere e proprie armi e, di conseguenza, il loro uso vietato dal diritto internazionale, appuntando l'attenzione non già sulla *modalità* di realizzazione dell'attacco quanto, piuttosto, sugli *effetti* da questo prodotti[79].

Non tutti gli attacchi informatici compiuti da uno Stato nei confronti di un altro, per quanto su larga scala, potrebbero quindi ritenersi *sic et simpliciter* vietati sulla base delle norme sull'uso della forza: il criterio discriminante ci pare vada individuato negli *effetti* prodotti dall'attacco in questione, i quali, per essere paragonabili a quelli di un attacco armato cinetico, con la conseguente estensione ai primi della relativa disciplina giuridica, dovrebbero causare la distruzione di beni e la perdita di vite umane[80].

Al riguardo è stato affermato che "per poter qualificare l'impiego di tecniche informatiche come una violazione dell'art. 2, par. 4, occorre pensare ad ipotesi quali un bombardamento ad opera di missili dello Stato territoriale o di un terzo Stato ottenuto mediante la manipolazione a distanza del sistema di lancio. Taluno ha fatto l'esempio della messa fuori uso dei computers che controllano le riserve d'acqua o le dighe per provocare una catastrofe e la morte di centinaia di persone"[81].

Peraltro, anche gli attacchi informatici che non raggiungono una tale

[78] CIG, sentenza 27 giugno 1986, *Nicaragua c. Stati Uniti*, par. 195.
[79] T.A. Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2 (4) of the U.N. Charter*, in *Case Western Res. J. Int'l L.*, 1998, 567 ss.; M.N. Schmitt, *Computer Network Attack And The Use Of Force In International Law: Thoughts On A Normative Framework*, in *The Columbia Journal of Transnational Law*, 1999, 885 ss. Si veda anche J.M. Beard, *Law and War in the Virtual Era*, in *AJIL*, 2009, 1 ss.
[80] Sul requisito in parola, richiesto in genere a qualunque comportamento statale perché possa essere fatto ricadere sotto la vigenza del divieto in parola cfr. I. Brownlie, *International Law and the Use of Force by States*, Oxford, 1963, 362, disponibile anche all'indirizzo www.questia.com.
[81] N. Ronzitti, *Diritto internazionale*, Torino, 2019, 398: pertanto, anche per questo A. pare che sia astrattamente possibile una qualificazione come quella da noi ipotizzata, a condizioni non dissimili da quelle da noi delineate già nel 2012. Si veda anche C. Focarelli, *op. cit.*, 636.

soglia di aggressività, comunque, potrebbero ritenersi vietati dal diritto internazionale alla luce del principio di non ingerenza negli affari interni di uno Stato, fino a poter integrare, in casi limite – ma che, lo ribadiamo, non devono comportare la distruzione di beni e la perdita di vite umane – la *minaccia* dell'uso della forza. Come noto, infatti, la *Dichiarazione relativa ai principi di diritto internazionale concernenti le relazioni amichevoli* vieta agli Stati di applicare "misure economiche, politiche o *di qualsiasi altra natura* o incoraggiarne l'uso, al fine di costringere un altro Stato a subordinare l'esercizio dei suoi diritti sovrani e per ottenere da esso vantaggi di qualsiasi genere"[82].

Questione differente, e parimenti complessa, poi, è quella che riguarda la possibilità di una reazione in legittima difesa armata a un attacco informatico; come già ricordato l'ordinamento internazionale distingue le violazioni *minoris generis* del divieto dell'uso della forza da quelle, particolarmente qualificate, che si sostanziano in un attacco armato[83] e consente solo in quest'ultimo caso, come chiarito dalla CIG nel caso *Nicaragua c. Stati Uniti*, una reazione armata in legittima difesa ai sensi dell'art. 51 della Carta delle Nazioni Unite e della corrispondente norma di diritto internazionale consuetudinario.

L'attenzione, allora, va spostata sui *mezzi* che possono essere legittimamente utilizzati dallo Stato che reagisce ad un attacco informatico, e, in particolare, se essi possano assumere *esclusivamente* la *medesima forma* dell'attacco subito, e cioè possano essere solo informatici, o possano anche sostanziarsi in misure di tipo cinetico.

A nostro parere il criterio da utilizzare va individuato nel principio di proporzionalità o, quanto meno, di non eccessiva sproporzionalità delle misure di reazione[84]: e allora ci pare possibile concepire come legittima una reazione cinetica dello Stato che abbia subìto un attacco informatico su larga scala, il quale abbia prodotto danni paragonabili a quelli di un attacco militare convenzionale, sempreché la reazione sia rispettosa del diritto internazionale cogente e del diritto internazionale umanitario[85].

---

[82] Dichiarazione relativa ai principi di diritto internazionale concernenti le relazioni amichevoli tra gli Stati, corsivo aggiunto, risoluzione dell'Assemblea generale delle Nazioni Unite n. 2625 del 24 ottobre 1970, doc. A/RES/2625 (XXV), in www.un.org. Corsivo aggiunto.

[83] Nel medesimo senso anche la sentenza della CIG del 23 novembre 2003 relativa al caso *Iran c. Stati Uniti – Oil Platforms*, 27. Si tratta, va detto, di una distinzione che è stata però criticata da una parte della dottrina, specie anglofona, secondo la quale sarebbe legittima la reazione militare anche nel caso di una precedente violazione di entità minore, sempre che la reazione sia necessaria e rispettosa del principio di proporzionalità.

[84] Cfr. B. Conforti, M. Iovane, *op. cit.*, 452.

[85] Specificamente sul tema M. Hoisington, *Cyberwarfare and the Use of Force: Giving Rise to the Right of Self-Defense*, in *Boston College International and Comparative Law Review*, 2009, 439 ss.; M. C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal of International Law*, 2011, In generale sulle condizioni per l'uso legittimo della forza nell'ordinamento internazionale v. Picone, *Obblighi "erga omnes" e uso della forza*, Napoli, 2017, 461 ss.

DPCE online
ISSN: 2037-6677

E in questo senso vanno citati alcuni elementi della prassi: già il rapporto 2011 sulla *cybersecurity* trasmesso dal Pentagono al Congresso statunitense dichiarava esplicitamente gli Stati Uniti si ritengono legittimati a reagire con l'uso della forza militare ad attacchi informatici particolarmente virulenti: "when warranted, we will respond to hostile attacks in cyberspace as we would to any other threat to our country (…) We reserve the right to use *all necessary means* – diplomatic, informational, military and economic – to defend our nation, our allies, our partners and our interests"[86]. Secondo tale rapporto, nella categoria che legittimerebbe l'uso della forza rientrerebbero tutti i "significant cyber attacks directed against the U.S. economy, government or military" e la reazione potrebbe quindi comportare sia l'uso di mezzi elettronici sia opzioni militari convenzionali.

E nel medesimo senso si è mossa anche la prassi statunitense successiva: i vari *National Defense Authorization Acts* (NDAA)[87] che si sono susseguiti negli anni contengono infatti numerose disposizioni che impattano sulla difesa cibernetica statunitense[88].

Altrettanto interessante è la prassi che si è sviluppata in seno alla NATO in occasione degli attacchi subiti nel 2007 da numerosi siti governativi, di banche e di importanti imprese estoni, partiti da indirizzi IP situati in Russia: in quell'occasione la NATO, pur non definendo "cyber-attacks as a *clear* military action", non ha negato la possibilità di una reazione cinetica, e si è limitata ad escludere l'applicazione *automatica* agli attacchi in parola delle disposizioni sulla legittima difesa collettiva contenute nel Trattato NATO[89]. È probabile, però, che nel caso di specie la reazione "morbida" sia stata suggerita dal tipo di attacchi subiti dall'Estonia, che in nessun modo avevano messo a repentaglio vite umane o infrastrutture critiche situate sul suo territorio.

Quello di cui ci stiamo occupando, come è evidente, rappresenta un

---

[86] Cfr. Department of Defense, *Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, Section 934 15th nov 2011, nonché il rapporto depositato il 3 luglio 2012 da R. Tehan del Servizio di ricerca del Congresso statunitense intitolato *Cybersecurity: Authoritative Reports and Resources*, reso pubblico sul sito dell'organizzazione non governativa *Federation of American Scientists* (FAS) all'indirizzo www.fas.org. I corsivi sono aggiunti.

[87] È il nome di una serie di leggi federali degli Stati Uniti che specificano il budget e le spese annuali del Dipartimento della Difesa. Il primo NDAA è stato approvato nel 1961.

[88] Un elenco di tali disposizioni è stato compilato in un file Excel scaricabile all'indirizzo thirdway.imgix.net/downloads/the-militarization-of-cyberspace-cyber-related-provisions-in-the-national-defense-authorization-act/Cyber-Related-NDAA-Provisions.xlsx. Al riguardo si veda anche M. Garcia, *The Militarization of Cyberspace: Cyber-Related Provisions in the National Defense Authorization Act* in T*hirdWay*, 30 marzo 2021, reperibile online, il quale evidenzia come "across 13 categories, three of the top four were aimed at the Department of Defense's(DoD) core cyber missions, such as changing organizational processes and structures, protecting DoD assets, and *engaging with foreign partners while deterring nation-state adversaries*".

[89] "Collective self-defence, will not *automatically* be extended to the attacked Country".

settore dell'ordinamento internazionale ancora oggi fluido, in cui il comportamento degli Stati non è univocamente orientato, e posizioni che pure possono apparire come significative espressioni di unilateralismo, in particolare statunitense o occidentale, non possono essere ignorate, anche in considerazione del fatto che appare quasi inevitabile che la prassi in materia sia promanante, in massima parte, dai Paesi maggiormente sviluppati nel settore delle tecnologie dell'informazione e delle telecomunicazioni.

Va tuttavia detto che, al momento in cui scriviamo, non si hanno notizie di reazioni armate, attraverso strumenti cinetici, avverso attacchi informatici; tuttavia, ad oggi, ci pare di poter dire che nessun attacco del secondo tipo, anche quando molto aggressivo, abbia mai superato la soglia che abbiamo individuato come necessaria a legittimare una reazione del primo tipo.

11. *(Segue)*: d) l'obbligo di uso pacifico: il terrorismo informatico

Ancora più complesso, poi, è riuscire a giungere ad una definizione univoca di *cyber terrorismo*. La letteratura che si è occupata della questione, nell'assenza di una definizione generalmente accettata del fenomeno anche "tradizionale", ha spesso ritenuto tale la commissione di crimini informatici ordinari, ma con l'intenzione specifica di instillare la paura in una popolazione bersaglio[90].

L'analisi della prassi consente di individuare almeno due distinte definizioni di *cyber terrorismo* degne di particolare attenzione, una promanante dal *Federal Bureau of Investigation* (FBI) statunitense, l'altra stilata dalla NATO.

Per l'FBI, tra i primi enti statali ad occuparsi della questione, sarebbe terrrorismo informatico ogni "premeditated, politically motivated attack *against information, computer systems, computer programs, and data* which results in violence *against non-combatant targets by sub-national groups or clandestine agents*"[91]: secondo questa lettura, quindi, perché vi sia un attacco informatico di tipo terroristico, oltre alla matrice politica, è necessario che lo stesso 1) sia posto in essere da gruppi sub-nazionali o agenti clandestini (e non, quindi, come ovvio, dall'esercito regolare di un Paese), 2) abbia luogo *nei confronti di sistemi informatici*, programmi per computer e dati, e 3) produca danni contro obiettivi *non militari*.

Di avviso parzialmente diverso appare la NATO, per la quale sarebbe

[90] Cfr. R. Garrett, Clarke, *Cyberterrorism: A New Challenge for International Law*, in A. Bianchi (Ed.), *Enforcing International Law Norms Against Terrorism*, Oxford-Portland, 2004, 465 ss.; Y. Shiryaev, *Cyberterrorism in the Context of Contemporary International Law*, in *San Diego International Law Journal*, 2012, 139 ss.; H.A. Harrison *Dinnis, The Threat of Cyber Terrorism and What International Law Should (Try To) Do about It*, in *Georgia Journal of International Affairs*, 2018, p, 43 ss.

[91] La definizione è contenuta in un *brief* elaborato nel 1997 per l'*FBI Laboratory* col titolo *Cyberterrorism – Fact or Fancy?*, pubblicato online.

cyber terrorismo ogni "cyber attack *using or exploiting computer or communication networks* to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal"[92]: secondo questa definizione, quindi, rientrano nella categoria in esame tutti gli attacchi informatici per un obiettivo ideologico, posti in essere 1) *utilizzando o sfruttando reti di computer o di comunicazione*, 2) col fine di causare distruzione o interruzione di operatività di entità sufficientemente rilevante da generare paura o intimidire la società bersaglio.

Le due definizioni, che hanno in comune tra loro l'elemento soggettivo dell'intento politico/ideologico dell'azione, differiscono sotto il profilo oggettivo per il fatto che, mentre nella prospettiva statunitense le strutture informatiche devono essere il *bersaglio* dell'attacco coi descritti caratteri, per l'Alleanza atlantica sarebbe ascrivibile al *cyber terrorismo* solo un attacco sferrato *utilizzando* computer e reti di telecomunicazioni come mezzo.

Peraltro, mentre la definizione del *Federal Bureau* prende ulteriormente posizione in merito ai profili soggettivi del comportamento in esame, e vi fa rientrare esclusivamente le operazioni poste in essere da individui o gruppi di individui per così dire indipendenti, o, al massimo "sponsorizzati" da Stati (i "sub-national groups" del testo), lasciando quindi fuori il c.d. terrorismo *di* Stato, l'elaborazione della NATO, sul punto, resta più sfumata.

Nell'assenza di prassi significativa specificamente relativa al *cyber terrorismo*[93], per tentarne una definizione generale alla luce dell'ordinamento internazionale contemporaneo, visti i punti di contatto tra le due fattispecie, crediamo sia opportuno prendere le mosse dalla prassi relativa al terrorismo tradizionale: in quest'ultimo contesto, in particolare nella prassi ultimi anni, si è assistito a importanti sviluppi i quali, pur nella perdurante assenza di una definizione generalmente condivisa fra tutti i membri della Comunità internazionale, consentono di far rientrare nel terrorismo ogni attività riconducibile a privati o gruppi di privati che non rispondono ad alcuno Stato, nel senso che non agiscono per conto di esso o con la sua protezione, i quali pongano in essere atti di indiscriminata violenza diretti sia contro obiettivi civili sia contro obiettivi militari/governativi. Per rientrare nella categoria è altresì necessario che il comportamento materiale così individuato sia caratterizzato anche dall'elemento psicologico del fine di destabilizzazione dell'ordine mondiale, così come inteso dalla generalità degli Stati.

Sono quindi esclusi da una siffatta definizione tanto il terrorismo *di* Stato, che va ricondotto alla violazione di altri, più generali, obblighi di diritto internazionale e segnatamente del divieto generalizzato dell'uso della forza quanto, per motivi sostanzialmente analoghi, quello sponsorizzato da

[92] La definizione risulta riportata da un ufficiale dell'Alleanza, Everard, nel suo scritto *NATO and cyberterrorism*, nella pubblicazione ufficiale *Responses to cyber terrorism* editata dal Centre of Excellence Defence Against Terrorism della NATO e pubblicata ad Ankara nel 2007.

[93] L. Jarvis, S. Macdonald, L. Nouri, T*he Cyberterrorism Threat: Findings from a Survey of Researchers*, in *Studies in Conflict and Terrorism*, 2014, 1 68 ss.

Stati[94].

Su queste basi ci pare di poter affermare che una definizione di *cyber terrorismo* che sia sostanzialmente compatibile con quella di terrorismo "generico" come emersa dalla prassi recente potrebbe trarre il suo elemento oggettivo dal testo adottato in ambito NATO, dal momento che lo stesso consente di ricomprendere tutte le attività nocive poste in essere *mediante* strumenti informatici, indipendentemente dal loro *target*.

Ciò consente di unificare in un'unica categoria di comportamenti materiali *cyber terrorismo* e *cyber guerra*, che si distinguerebbero tra loro, quindi, sulla base della natura dell'aggressore (organizzazione di individui nel primo caso, di Stato nel secondo).

12. La *governance* del sistema dei nomi di dominio e di ICANN come indice di una tendenza all'informalizzazione dell'ordinamento internazionale

Sin dagli albori della diffusione di Internet, la gestione del sistema dei nomi di dominio (*Domain Name System*, DNS), il quale consente agli utenti di identificare i siti web digitando nomi facili da memorizzare (i nomi di dominio, appunto), invece dei rispettivi indirizzi numerici di rete (gli indirizzi IP), e rappresenta quindi l'indispensabile "elenco telefonico" della Rete, fondamentale per il funzionamento e, addirittura, per l'esistenza stessa del Web, era sempre stata svolta unilateralmente dagli Stati Uniti fino alla sua cessione, avvenuta nel 2016.

Il Governo degli Stati Uniti, va detto, concepiva *ab origine* il suo ruolo in maniera temporanea: se si legge lo *Statement of Policy on the Management of Internet Names and Addresses* adottato il 10 giugno 1998 dal Dipartimento del commercio statunitense vi si trova difatti, già allora, l'impegno ad una transizione che consentisse al settore privato di avere un ruolo dominante nella gestione del DNS[95]. È anche il caso di ricordare come numerose dichiarazioni rilasciate nel tempo dagli USA abbiano ripetutamente riconosciuto l'intenzione degli stessi di preservare la sicurezza e la stabilità del sistema dei nomi di dominio e, di conseguenza, l'impegno a non porre in

[94] U. Draetta, *The Internet and Terrorist Activities*, in A. Bianchi (Ed.), *Enforcing International Law Norms Against Terrorism*, Oxford-Portland, 2004, 453 ss., per il quale "it seems that the notion of cyber terrorism is insufficiently defined and addressed in the international conventional law, with the exception of the regional integration at the EU level, where such a notion seems to be emerging with sufficiently precise contours. As to terrorist acts carried out through the internet, international legal instruments dealing with cybercrimes do not yet contain specific provisions for terrorism, as they do for child pornography, infringement of intellectual rights, racism and xenophobia. There is here a definite need for improvement", 464.

[95] Reperibile sul sito della NTIA, all'indirizzo www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses. Come si vede dal testo citato, l'intenzione originaria era, quindi, di cedere il governo del sistema DNS al settore "privato". Vedremo più avanti se questo sia sul punto di avvenire e in che forma.

essere misure che potessero avere effetti negativi sulla sua efficienza[96].

Sebbene la prassi non avesse registrato molte proteste formali promananti da altri Stati, alla legittimazione dell'autorità esclusiva del Governo statunitense sul sistema dei nomi di dominio[97] – e ciò anche se, è bene chiarirlo, i server sui quali i relativi dati sono conservati, siano disseminati su tutta la superficie del pianeta, e quindi anche *al di fuori* del territorio nazionale statunitense[98] – già nel 2003, il WSIS delle Nazioni Unite, indetto dall'Assemblea generale con la risoluzione 56/183 del 21 dicembre 2001[99], aveva discusso e studiato i possibili meccanismi idonei a garantire un più ampio coinvolgimento internazionale nella *governance* di Internet e in particolare nella gestione del sistema dei nomi di dominio. Lo studio era stato condotto dal *Working Group on Internet Governance* (WGIG), un gruppo di lavoro a composizione "mista"[100] il cui compito, assegnatogli dal WSIS, era proprio "to investigate and make proposals for action, as appropriate, on the governance of Internet". Il lavoro del WGIG si concludeva con un rapporto che riconosceva che *nessun* Governo avrebbe dovuto rivestire un ruolo preminente nella *governance* di Internet e sollecitava, quindi, una maggiore internazionalizzazione della stessa, proponendo finanche l'istituzione di un nuovo organismo consultivo "globale", l'*Internet Governance Forum* (IGF), al quale è assegnato il compito di discutere le politiche pubbliche legate agli elementi chiave della *governance* di Internet al fine di promuoverne la sostenibilità e di mantenere aperto il dibattito tra tutti gli attori (statali, intergovernativi e privati) che se ne occupano, anche al fine di facilitare lo scambio di informazioni e delle *best practices* in materia[101]. L'IGF, ancora, promuove *ex ante* e valuta *ex post*, in modo continuativo, l'implementazione da parte degli Stati dei principi adottati nel corso del WSIS nei processi di *governance* e affronta le questioni relative alle risorse critiche della Rete, come gli indirizzi IP, nonché cerca di

[96] U.S. Principles on the Internet's Domain Name and Addressing System, in www.ntia.doc.gov.

[97] Unica eccezione degna di rilievo era quella promanante dal Governo brasiliano, da noi ricostruita in *Internet-ional Law – Profili di diritto internazionale pubblico della Rete*, Bari, 2012, 55, in part. *sub* nota 19.

[98] Una mappa dei *root server* è consultabile all'indirizzo public-root.com/root-server-locations.htm.

[99] Cfr. General assembly, doc. A/RES/56/183 del 21 dicembre 2001, reperibile sul sito www.un.org.

[100] Usiamo l'espressione "mista" con riferimento a gruppi la cui composizione contempla la partecipazione di rappresentanti di Stati e di organizzazioni internazionali "classiche", cioè intergovernative, accanto a organizzazioni non governative (ONG) e soggetti privati. Nella letteratura anglofona, come già visto, è invalso l'uso del termine "multistakeholder".

[101] Il 13 dicembre 2015 l'Assemblea Generale delle Nazioni Unite ha approvato un documento "on the overall review of the implementation of the outcomes of the World Summit on the Information Society" con il quale, tra le altre cose, è stato esteso per altri 10 anni il mandato dell'Internet Governance Forum (IGF); il documento A/70/L.33 è reperibile all'indirizzo unbisnet.un.org.

individuare soluzioni per i problemi legati all'abuso di Internet[102].

Il WSIS proponeva così quattro distinti modelli regolatori per la Rete, due dei quali contemplavano la creazione di organismi collegati alle Nazioni Unite. È il caso di segnalare come, secondo tre dei quattro modelli proposti, la *Internet Corporation for Assigned Names and Numbers* (ICANN), della quale ci occuperemo più diffusamente *infra*[103] – l'organizzazione statunitense di diritto privato senza scopo di lucro, istituita nel 1988 alla luce delle norme statali californiane, che materialmente gestisce i meccanismi di funzionamento della Rete – avrebbe dovuto essere soppiantata del tutto, o comunque avrebbe dovuto render conto a un organismo intergovernativo.

Le conclusioni di questo rapporto avrebbero dovuto costituire il punto di partenza della seconda fase del *Summit*, svoltasi a Tunisi nel 2005, che però fece registrare il blocco del negoziato sull'internazionalizzazione della *governance* del Web, quando i delegati statunitensi, come richiesto loro dal Congresso, si opposero fermamente al trasferimento del controllo dell'amministrazione del sistema di nomi di dominio a qualunque organismo internazionale.

A partire dal 2010 la questione del ruolo degli Stati nella gestione di Internet tornava prepotentemente all'attenzione della comunità internazionale dal momento che molti Paesi, fra cui curiosamente gli stessi Stati Uniti e l'Unione europea, spingevano per un accrescimento del ruolo dei Governi nazionali in seno ad ICANN (cosa che peraltro, come già accennato, è avvenuta), mentre altri, come il Brasile, il Sudafrica e l'India cercavano di rinverdire le proposte di istituzione di un ente internazionale di

[102] Ad oggi l'IGF si è riunito quindici volte: dal 30 ottobre al 2 novembre 2006 ad Atene in Grecia, dal 12 al 15 novembre 2007 a Rio de Janeiro in Brasile, dal 3 al 6 dicembre 2008 a Hyderabad in India, dal 15 al 18 novembre 2009 a Sharm El Sheik in Egitto, dal 14 al 17 settembre 2010 a Vilnius in Lituania, dal 27 al 30 settembre 2011 a Nairobi in Kenya, dal 6 al 9 novembre 2012 a Baku in Azerbaijan, dal 22 al 25 ottobre 2013 a Bali in Indonesia, dal 2 al 5 settembre 2014 a Istanbul in Turchia, dal 10 al 13 novembre 2015 in Brasile, dal 6 al 9 dicembre 2016 a Jalisco in Messico, dal 18 al 21 dicembre 2017 a Ginevra in Svizzera, dal 12 al 14 novembre 2018 a Parigi, presso l'UNESCO, dal 25 al 29 novembre 2019 a Berlino. L'edizione 2020, a causa della pandemia da COVID-19 si è tenuta online. Per una ricostruzione dell'attività delle organizzazioni internazionali in materia di Internet *governance*, anche per ulteriori indicazioni bibliografiche, ci permettiamo di rinviare a G.M. Ruotolo, *Internet (diritto internazionale)*, cit., 545 ss. Sul tema v. anche E. Pavan, *Frames and Connections in the Governance of Global Communications: A Network Study of the Internet Governance Forum*, in *Journal of International Communication*, Lexington, 2013; T. Natoli, *Il ruolo delle organizzazioni internazionali nella gestione delle reti digitali globali*, in F. Marcelli, Marsocci, M. Pietrangelo (a cura di), *La rete Internet come spazio di partecipazione politica. Una prospettiva giuridica*, Napoli, 2015, 101 ss.

[103] In letteratura si vedano *ex multis*, B. Carotti, *L'ICANN e la governance di Internet*, in *Rivista trimestrale di diritto pubblico*, 2007, 681 ss.; Id., *ICANN and Global Administrative Law*, reperibile sul sito del progetto di ricerca relativo al *Global Administrative Law (GAL)* dell'*Institute for International Law and Justice*, New York University, all'indirizzo iilj.org/GAL; S. Delbianco, B. Cox, *ICANN Internet Governance: Is It Working?*, in *Global Business & Development Law Journal*, 2008, 27 ss.

DPCE online
ISSN: 2037-6677

regolamentazione all'interno del sistema delle Nazioni Unite, idoneo ad assorbire gli organismi già esistenti (ICANN *in primis*), e ancora, un terzo gruppo di Stati, fra cui Russia e Cina, sosteneva l'esistenza di *consensus* internazionale sulla cui base adottare un International Code of Conduct for Information Security, da adottare in seno alle Nazioni Unite, nella forma di una risoluzione dell'Assemblea generale[104]. È interessante notare come la versione rivista di tale Codice, proposta all'Assemblea generale nel gennaio 2015, ribadisce che "all States must play *the same role* in, and carry *equal responsibility for*, *international governance of the Internet*, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet"[105].

In effetti, già nel 2013 le principali organizzazioni responsabili della gestione tecnica di Internet – ICANN, IETF, Internet Society (ISoc)[106] – riunite a Montevideo, avevano fatto proprio questo approccio adottando lo *Statement on the Future of Internet Cooperation*, che auspicava un'accelerazione della globalizzazione di ICANN e delle funzioni di IANA (*Internet Assigned Numbers Authority*, l'organismo che concretamente gestisce il DNS) verso un modello in cui tutte le parti interessate, ivi compresi i Governi, partecipassero in condizioni di parità[107].

Malgrado tutti questi tentativi, fino al 2016 – quando il procedimento di cessione delle funzioni di IANA a favore di ICANN si è perfezionato finalmente – gli USA hanno continuato a gestire unilateralmente il sistema DNS[108] e ciò ha sollevato, sotto il profilo giuridico-internazionalistico, una serie di problemi relativi alla legittima titolarità di quel potere, dal momento che, come dicevamo, i server sui quali il medesimo potere si esercita sono allocati anche al di fuori del territorio statunitense.

Per quanto concerne l'individuazione del titolo giuridico dell'esercizio del potere in parola, sono stati proposti essenzialmente due distinti modelli ricostruttivi: il primo, caratterizzato dall'uso di istituiti più "tradizionali" del diritto internazionale, il secondo che invece si rifà a modelli mutuati dal *global*

---

[104] Doc. A/66/359.

[105] United Nations General Assembly, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General," January 13, 2015, 5, reperibile all'indirizzo regmedia.co.uk/2015/02/04/un-internet-security-13jan15.pdf. Corsivi nostri.

[106] Internet Society (ISoc) è un'organizzazione internazionale non governativa – fondata nel 1992 da Vinton Cerf, Robert Kahn, Jon Postel e altri pionieri della Rete – senza fini di lucro, dedita a favorire lo sviluppo libero, equo, universale e stabile di Internet e a promuoverne gli usi benefici per l'intera umanità.

[107] Lo *Statement* è pubblicato su www.icann.org/news/announcement-2013-10-07-en.

[108] Cfr. N. Krisch, *International Law in Times of Hegemony: Unequal Power and the Shaping of the International Legal Order*, in *European Journal of International Law*, 2005, 369 ss., in part. 406.

administrative law[109].

Seguendo il modello ricostruttivo per così dire classico, il detto potere, esplicandosi su oggetti collocati in aree geografiche sottratte alla sovranità USA, andava letto come una forma di esercizio extraterritoriale del potere coercitivo o di governo in senso stretto[110] il quale trova un limite territoriale nel principio consuetudinario di non ingerenza[111], principio che, a sua volta, può essere legittimamente derogato solo in presenza di specifiche previsioni consuetudinarie o pattizie (e in questo caso le relative norme avrebbero contenuto *permissivo*) o di autorizzazioni (esplicite od implicite) del sovrano territoriale, cioè, nel caso di specie, da parte degli Stati sul cui territorio sono

[109] Come noto, il *global administrative law* è un modello ricostruttivo frutto dell'elaborazione dottrinale di un gruppo di studiosi statunitensi degli inizi di questo secolo. In letteratura si vedano L. Boisson de Chazournes, *Changing Roles of International Organizations: Global Administrative Law and the Interplay of Legitimacies*, in *International Organizations Law Review*, 2009, 655 ss.; S. Chesterman, *Globalisation and Public Law: a Global Administrative Law?*, in J. Farrall, K. Rubenstein (Eds), *Sanctions, Accountability and Governance in a Globalised World*, Cambridge University Press, Cambridge, 2009, 75 ss.; M. D'Alberti, *Administrative Law and the Public Regulation of Markets in a Global Age*, in S.Rose-Ackerman, P.L. Lindseth (Eds), *Comparative Administrative Law*, Cheltenham, 2010, 63 ss.; D. C. Esty, *Good Governance at the Supranational Scale: Globalizing Administrative Law*, in *Yale Law Journal*, 2006, 1490 ss.; C. Harol, *Accountability as a Value in Global Governance and for Global Administrative Law*, in A. Gordon (Ed.), *Values in Global Administrative Law*, Oxford, 2011, 173 ss.; B. Kingsbury, L. Casini, *Global Administrative Law Dimensions of International Organizations Law*, in *International Organizations Law Review*, 2009, 319 ss.; B. Kingsbury, *The Concept of "Law" in Global Administrative Law*, in *European Journal of International Law*, 2009, 23 ss.; B. Kingsbury, N. Kirsch, R.B. Stewart, *The Emergence of Global Administrative Law*, in *New York University Public Law and Legal Theory Working Papers*, 2005; N. Krisch, B. Kingsbury (Eds), *Symposium on "Global Governance and Global Administrative Law in the International Legal Order"*, in *European Journal of International Law*, 2006, 1 ss. Per la letteratura italiana si vedano, per tutti, S. Cassese, *Il diritto amministrativo globale: una introduzione*, in *Rivista trimestrale di diritto pubblico*, 2005, 331 ss.; Id., *Administrative Law without the State? The Challenge of Global Regulation* in *New York University Journal of International Law and Politics*, 2005, 663 ss.; L. Casini, *Diritto amministrativo globale*, in S. Cassese (Ed.), *Dizionario di diritto pubblico*, Milano, 2006.

[110] V. G. Handl, *Extra-territoriality and Transnational Legal Authority*, in G. Handl, J. Zekoll, Zumbansen (Eds), *Beyond Territoriality. Transnational Legal Authority in an Age of Globalization*, 2012, 1 ss., nonché T. Baudet, *The Significance of Borders. Why Representative Government and the Rule of Law Require Nation States*, 2012. Per una ricostruzione della categoria v. Picone, *L'applicazione extraterritoriale delle regole sulla concorrenza e il diritto internazionale* in F. Capotorti, F. Di Sabato, A. Patroni Griffi, Picone, L.C. Ubertazzi, *Il fenomeno delle concentrazioni di imprese nel diritto interno e internazionale*, Padova, 1989, 84 ss.

[111] Il principio, la cui disamina è impossibile in questa sede, è pacificamente riconosciuto come parte del diritto internazionale generale ed è in genere concepito come "a corollary of every State's right to sovereignty, territorial integrity and political independence"; così *Oppenheim's International Law*, 428. La dichiarazione dell'Assemblea generalde delle Nazioni Unite sulle relazioni amichevoli tra Stati (res. 2625(XXV), 1970) contiene un'intera sezione sul principio in parola "concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter"; la medesima Assemblea generale, peraltro, aveva già in precedenza adottato una Dichiarazione "on the Inadmissibility of Intervention and Interference in the Domestic Affairs of States (res. 2131 (XX) 1965).

DPCE online
ISSN: 2037-6677

situati i server. Nell'impossibilità di individuare norme di diritto internazionale, generale o pattizio, che attribuissero agli Stati Uniti la legittimazione a porre in essere, al di fuori del proprio territorio nazionale, azioni che avessero l'effetto di modificare il *root file* del DNS, nonché nell'impossibilità di rintracciare dichiarazioni esplicite di autorizzazione a tali modifiche da parte degli Stati sul cui territorio sono localizzati i relativi server, azioni siffatte potevano trovare legittimazione nell'acquiescenza a tale attività da parte degli Stati di allocazione territoriale dei server. Per quanto concerne, poi, le modalità di esercizio di tale potere, il Governo federale USA, riconoscendo l'esistenza in capo agli altri Stati di un interesse particolarmente rilevante in materia, si era da sempre impegnato a collaborare con gli altri Stati nell'obiettivo di preservare l'esigenza fondamentale di assicurare stabilità e sicurezza al sistema DNS[112], ammettendo esplicitamente, l'esistenza di un interesse *comune* a tutti gli Stati alla permanenza della funzionalità della Rete, in quanto bene di rilevanza "globale". Insomma, lo stesso Stato che esercitava il potere esclusivo di governo del sistema DNS, al contempo, riconosceva l'esistenza di una necessità di assicurarne il funzionamento e che tale necessità era in qualche modo riconducibile a *interessi fondamentali* della comunità internazionale[113].

Anche il secondo modello ricostruttivo muoveva dalla considerazione dell'esistenza di un interesse *comune* e *basilare* degli Stati a individuare una modalità di governo di Internet che ne assicuri la perdurante funzionalità, ma interpretava l'esercizio della potestà di governo USA del sistema DNS come una delle forme in cui si estrinseca il diritto amministrativo globale, espressione con la quale, come noto, si fa riferimento, in linea molto generale, tanto all'esercizio da parte di amministrazioni pubbliche nazionali di poteri amministrativi a un livello che coinvolga non solo l'ordinamento e gli interessi dello Stato d'origine, ma anche ordinamenti e, ancora, interessi di Stati diversi, al fine di perseguire obiettivi comuni, quanto all'insorgenza di forme di diritto "amministrativo" (da intendersi nel senso di disciplina giuridica delle amministrazioni pubbliche e dei rapporti tra queste e i privati) di rilevanza transnazionale, in tutti quei casi in cui l'obbiettivo da raggiungere presenti caratteristiche tali da rendere necessaria l'utilizzazione

[112] U.*S. Principles on the Internet's Domain Name and Addressing System*, documento del 30 giugno 2005, in www.ntia.doc.gov.

[113] Quello degli interessi fondamentali della comunità internazionale, e delle modalità attraverso le quali garantire la loro tutela, è un tema su cui la dottrina internazionalistica si è ampiamente concentrata, muovendo da premesse teoriche spesso molto differenti tra loro e con esiti molteplici e differenziati. Per alcune differenti prospettive v. G. Gaja, *The Protection of General Interests in the International Community*, in *Collected Courses of the Hague Academy of International Law*, The Hague, 2013; M. Iovane, *La tutela dei valori fondamentali nel diritto internazionale*, Napoli, 2000; Picone, *Comunità internazionale e obblighi "*erga omnes" – *Studi critici di diritto internazionale*, Napoli, 2013; S. Villalpando, *The Legal Dimension of the International Community: How Community Interests Are Protected in International Law*, in *European Journal of International Law*, 2010, 387 ss.

di un meccanismo per così dire "misto", in cui su un sistema di regole di base previste dal diritto internazionale, si vada a innestare un meccanismo più strettamente amministrativo, ma comunque di rilevanza "globale", per l'appunto[114].

In particolare, nel caso di specie, ci si trovava in presenza di un caso di "amministrazione distribuita", posta cioè in essere da un determinato Stato (gli USA) legittimato a svolgere funzioni di rilevanza "globale", in forza di un interesse comune, riconosciuto.

La stessa ICANN, poi, è stata vista quale sorta di paradigma di un'altra forma di *global administration*, quella cui è stato dato il nome di *hybrid intergovernmental-private administration*[115]: essa, infatti, è stata istituita come un organismo puramente non governativo ma, col passare del tempo, in conseguenza delle rilevanti pressioni degli Stati, si è trovata a coinvolgere nella sua organizzazione, e in maniera sempre più penetrante, anche rappresentanti dei Governi nazionali, i quali sono, a partire dal 2002, titolari di rilevanti poteri, che esercitano in seno al Governmental Advisory Committee, in cui attualmente siedono i Governi in qualità di membri e le organizzazioni internazionali, anche come osservatori[116].

In quel contesto gli Stati – che sono vincolati sia da norme nazionali sia da obblighi derivanti dal diritto internazionale – operano di fianco ad attori privati, i quali non subiscono invece, quanto meno direttamente, i vincoli da ultimo elencati, e possono farsi portatori di interessi concorrenti con quelli amministrati dai primi.

Il riconoscimento dell'esistenza di un *interesse comune e fondamentale* degli Stati alla perdurante funzionalità della Rete rappresenta, quindi, uno dei presupposti che hanno indotto l'amministrazione USA a completare il procedimento di cessione del sistema DNS alla c.d. "global community"[117].

---

[114] Per una ricostruzione del fenomeno v. C. Moellers, *Ten Years of Global Administrative Law*, in *International Journal of Constitutional Law*, 2015, 469 ss.; R.B. Stewart, *The normative dimensions and performance of global administrative law*, in *International Journal of Constitutional Law*, 2015, 499 ss., nonché S. Cassese, *Administrative Law without the State? The Challenge of Global Regulation*, in *New York University Journal of International Law and Politics*, 2005, 663 ss.; B. Kingsbury, N. Krisch, R.B. Stuart, The *Emergence of Global Administrative Law*, in *New York University Public Law and Legal Theory Working Papers*, 10-1-2005.

[115] B. Kingsbury, N. Krisch, R.B. Stewart, *The Emergence Of Global Administrative Law*, in *Law & Contemporary Problems*, 2005, 2 i quali, oltre all'esempio di ICANN ("which established as a non-governmental body, but which has come to include government representatives who have gained considerable powers, often via service on ICANN's Governmental Advisory Committee, since the 2002 reforms") citano anche la "Codex Alimentarius Commission, which adopts standards on food safety through a decisional process that now includes significant participation by non-governmental actors as well as by government representatives, and produces standards that gain a quasi-mandatory effect via the SPS Agreement under WTO law".

[116] Sulle difficoltà di qualificare ICANN come un'organizzazione internazionale classica ci permettiamo di rinviare a G.M. Ruotolo, *Fragments of Fragments*, cit.

[117] L'espressione è utilizzata nel comunicato di NTIA da noi già citato *supra*, alla nota 1. Il 55mo Meeting di ICANN, che si svolgerà a Marrakech, in Marocco, dal 5 al 10 marzo 2016,

DPCE online
ISSN: 2037-6677

Con quest'ultima espressione si fa generalmente riferimento alla costellazione di tutti gli enti che pongono in essere attività di rilevanza internazionale, anche se privi della soggettività di diritto internazionale, e che quindi comprende, accanto a Stati e organizzazioni internazionali governative – i membri della comunità internazionale tradizionalmente intesa[118] – anche organizzazioni non governative, imprese multinazionali, e finanche individui[119].

Tali enti, per regolamentare i loro rapporti, utilizzano sempre più spesso, accanto a norme appartenenti alle fonti classiche dell'ordinamento internazionale, anche strumenti normativi, strutture organizzative e procedimenti decisionali "atipici", caratterizzati, in particolare, da un alto grado di *informalità*.

Tali strutture mirano a porre in essere forme di cooperazione transfrontaliera in contesti differenti da un'organizzazione internazionale (mediante, quindi, processi di natura informale) tra attori diversi – o comunque ulteriori – rispetto a quelli che tradizionalmente sono titolari delle relazioni internazionali/diplomatiche (tra soggetti, quindi, che solo parzialmente rientrano tra quelli formalmente classificati come soggetti di diritto internazionale) e che si basano, utilizzano e producono norme differenti da trattati internazionali o da altre fonti di diritto internazionale (e parimenti informale, quindi, è l'*output* normativo dei processi in parola).

Finanche la nomenclatura utilizzata per definire tali strumenti, la quale fa di tutto per evitare le più tradizionali espressioni di "trattato", "accordo", "organizzazione internazionale" *et similia*, è un importante indice di questa informalizzazione.

Per fare qualche esempio, oltre all'ICANN, si possono citare, tra gli altri, l'*Intesa* di Wassenaar sui controlli all'esportazione di armi convenzionali (Wassenaar *Arrangement* on Export Controls for Conventional Arms and Dual-Use Goods and Technologies)[120], la *Conferenza*

avrà il compito di definire i dettagli della transizione; cfr. meetings.icann.org/en/marrakech55.

[118] Ma per l'analisi delle varie accezioni con le quali l'espressione "comunità internazionale" viene utilizzata oggi v. C. Focarelli, *op.cit.*, 88 ss.

[119] A. Iriye, *Global community: the role of international organizations in the making of the contemporary world*, Oakland, 2004, vi fa rientrare "all organizations—the state, business enterprises, international organizations, and nongovernmental associations" le quali, complessivamente, "form what Kofi Annan, secretary general of the United Nations, has called a "strategic partnership"", 209.

[120] Il Wassenar Arrangement, assieme al Nuclear Suppliers Group (NSG) for the control of nuclear related technology , all'Australia Group (AG) for control of chemical and biological technology that could be weaponized e al Missile Technology Control Regime for the control of rockets and other aerial vehicles capable of delivering weapons of mass destruction, rientra nei c.d. multilateral export control regimes (MECRs), "an international *body* that states use to organize their national export control system"; cfr. Stockholm International Peace Research Institute, *SIPRI Yearbook*: *Armaments, Disarmament and International Security*, 2015. Come si vede, anche in questo caso le definizioni aggirano la terminologia classica, parlando di

internazionale per l'armonizzazione dei requisiti tecnici per la registrazione dei farmaci ad uso umano (International *Conference* on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, ICH)[121], il *Sistema* di certificazione del *processo* di Kimberley sui diamanti (Kimberley Process Certification *Scheme*, KPCS)[122], l'*Iniziativa* di sicurezza contro la proliferazione delle armi di distruzione di massa (Proliferation Security *Initiative*, PSI)[123] l'International Competition *Network*[124], il Financial Stability *Board*[125], il Comitato di Basilea per la vigilanza bancaria

"international bodies", anzichè di "organizations".

[121] www.ich.org. L'ICH riunisce in un unico *forum* le autorità di regolamentazione e le industrie farmaceutiche per discutere gli aspetti scientifici e tecnici di registrazione dei farmaci. Istituita nel 1990, persegue l'armonizzazione internazionale dei requisiti di registrazione dei farmaci per uso umano. A.E. Ryan, *Protecting the Rights of Pediatric Research Subjects in the International Conference Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use*, in *Fordham International Law Journal*, 2000, 848 ss.

[122] www.kimberleyprocess.com. In dottrina si vedano J.M. Durnovich, *This land is my land: mending the Kimberley Process and promoting stability in Sub-Saharan Africa by reinforcing individual property rights*, in *North Carolina Journal of International Law and Commercial Regulation*, 2014, 885 ss. ; V. Grado, *Divieto di commercio di diamanti insanguinati e ordinamento dell'OMC*, in A. Ligustro, G. Sacerdoti (Eds), *Problemi e tendenze del diritto internazionale dell'economia* – Liber amicorum *in onore di Paolo Picone*, Napoli, 2011, 927 ss.

[123]Secondo il documento alla base della PSI, lo Statement of Interdiction Principles, "the Proliferation Security Initiative is a response to the growing challenge posed by the proliferation of weapons of mass destruction (WMD), their delivery systems, and related materials worldwide. The PSI builds on efforts by the international community to prevent proliferation of such items, including existing treaties and regimes"; cfr. www.psi-online.info. In pratica, l'iniziativa contempla la condivisione, tra i Paesi coinvolti, di informazioni di intelligence e il coordinamento delle forze armate al fine di interdire il transito di navi e aerei sospettati di trasportare armi di distruzione di massa o materiali idonei per la loro costruzione; cfr. A. Etzioni, *Tomorrow's Institution Today: The Promise of the Proliferation Security Initiative*, in *Foreign Affairs*, 2009, 7 ss.; National Institute for Public Policy, *The Proliferation Security Initiative: A Model for Future International Collaboration*, in *Comparative Strategy*, 2009, 395 ss.

[124] "The ICN is a specialized yet informal network of established and newer agencies, enriched by the participation of non-governmental advisors (representatives from business, consumer groups, academics, and the legal and economic professions), with the common aim of addressing practical antitrust enforcement and policy issues. By enhancing convergence and cooperation, the ICN promotes more efficient and effective antitrust enforcement worldwide to the benefit of consumers and businesses"; www.internationalcompetitionnetwork.org. J. Backhaus, *The international competition network at ten. Origins, accomplishments and aspirations*, in *European Journal of Law and Economics*, 2012, 413 ss.; H.M. Hollman, W.E. Kovacic, *The International Competition Network: its past, current and future role*, in *Minnesota Journal of International Law*, 2011, 274 ss.

[125] www.financialstabilityboard.org. Il FSB, creato nell'aprile del 2009 in occasione di una riunione del G20, rientra tra le iniziative volte a fronteggiare la crisi economica "globale" in atto ormai dal 2007 e ha preso il posto del Financial Stability Forum (FSF) che era stato creato quasi esattamente 10 anni prima in seguito alla Crisi finanziaria dell'Asia orientale del 1997, rispetto al quale un mandato ampliato, volto a promuovere la stabilità finanziaria internazionale. Il FSB rientra tra le c.d. "umbrella organizations" e tra i suoi membri comprende rappresentanti di altre strutture internazionali informali come il Comitato di Basilea e l'International Accounting Standards Board, i quali operano accanto ai regolatori nazionali, come le banche centrali e ai rappresentanti dei ministeri delle finanze nazionali e

DPCE online
ISSN: 2037-6677

(Basel *Committee* on Banking Supevision)[126].

Al riguardo la dottrina ha parlato di *informal international lawmaking*[127].

Le ragioni dell'insorgenza nella prassi di modelli siffatti sono molteplici[128], ma tutte originano dall'esistenza sempre più frequente di relazioni e interessi che trascendono i confini statali e i *soli* Stati come centri di imputazione di interessi[129] e che per questo non sono efficacemente gestibili dai soli operatori tradizionali del diritto internazionale (gli Stati, per l'appunto) mediante processi formali e per il tramite di regole da questi sviluppate in tali procedimenti, che comportano l'espressione del consenso statale (come avviene per i trattati, ma discorso analogo vale per gli atti adottati dalle organizzazioni internazionali, che, come noto, necessitano dell'approvazione dei competenti organi, composti di rappresentanti degli Stati).

Peraltro, come è stato efficacemente affermato, la disciplina giuridica delle nuove tecnologie è spesso resa particolarmente complessa, e

---

dei servizi di tesoreria. Cfr. M. Moschella, *Designing the Financial Stability Board: a theoretical investigation of mandate, discretion, and membership*, in *Journal of International Relations and Development*, 2013, 380 ss.; S. Gadinis, *The Financial Stability Board: the new politics of international financial regulation*, in *Texas International Law Journal*, 2013, 157 ss.; L. Catà Backer, *Private Actors and Public Governance Beyond the State: The Multinational Corporation, the Financial Stability Board, and the Global Governance Order*, in *Indiana Journal of Global Legal Studies*, 2011, 751 ss.

[126]Il Comitato di Basilea per la vigilanza bancaria fornisce un *forum* per la cooperazione internazionale in materia di vigilanza bancaria al fine di migliorare la comprensione delle questioni di vigilanza e la la qualità della vigilanza bancaria a livello mondiale; la consultazione pubblica è un elemento essenziale del processo di definizione delle norme del Comitato di Basilea. Attualmente i membri del Comitato provengono da Argentina, Australia, Belgio, Brasile, Canada, Cina, Unione Europea, Francia, Germania, Hong Kong, India, Indonesia, Italia, Giappone, Corea, Lussemburgo, Messico, Paesi Bassi, Russia, Arabia Saudita, Singapore, Sud Africa, Spagna, Svezia, Svizzera, Turchia, Regno Unito e Stati Uniti. In dottrina v. M. Peihani, *The Basel Committee on Banking Supervision: a post-crisis assessment of governance and accountability*, in *Canadian Foreign Policy Journal*, 2015, 146 ss; K.L Young, *Transnational regulatory capture?: an empirical examination of the transnational lobbying of the Basel Committee on Banking Supervision*, in *Review of international political economy*, 2012, 663 ss.

[127] J. Pauwelyn, R.A. Wessel, J. Wouters (Eds), *Informal International Lawmaking*, Oxford, 2012, 22 nonché J. Pauwelyn, R.A. Wessel, J. Wouters, *When Structures Become Shackles: Stagnation and Dynamics in International Lawmaking*, in *European Journal of International Law*, 2014, 733 ss che nel titolo rievoca proprio quell rapporto tra stutture e "ceppi" di cui all'*incipit* di Christopher Nolan, citato in apertura di questo articolo. Per un'ampia analisi di alcune recenti tendenze dell'ordinamento internazionale v. anche gli interessanti lavori recentemente raccolti in C. Rygaert, E.J. Molenaar, S.M.H. Nouwen (Eds), *What's Wrong With International Law?* Liber amicorum *A.H.A. Soons*, Leiden/Boston, 2015.

[128] Per un'accurata disamina cfr. J. Pawelyn, R.A.Wessel, J. Wouters, *When Structures Become Shackels: Stagnation and Dynamics in International Lawmaking*, in *European Journal of International Law*, 2014, 733 ss.

[129] A. D. Murray, *Conceptualising the Post-Regulatory (Cyber)state*, in R. Brownsword, K. Yeung (Eds), *Regulating Technologies. Legal Futures, Regulatory Frames and Technological Fixes*, Oxford/Portland, 2008, 287 ss.

difficilmente perseguibile per il tramite di strumenti tradizionali, dal fatto che "they move too quickly for regulatory comfort"[130].

Deve anche essere chiarito come le fonti in parola non siano neppure inquadrabili nella nota e comunque composita categoria del *soft law*[131], e questo per due ordini di ragioni: quest'ultima categoria, *in primis*, raccoglie norme comunque prodotte da soggetti "tradizionali" dell'ordinamento internazionale (Stati e organizzazioni internazionali) mediante processi decisionali "classici", che appaiono comunque rigidamente condizionati da forme di espressione del consenso degli Stati e, in secondo luogo e soprattutto, perché le regole "informali" di cui parliamo, spesso, sotto il profilo contenutistico, hanno ben poco di *soft*, nel senso di vago, non vincolante, non condiviso, dal momento che il loro mancato rispetto spesso implica la privazione della possibilità di utilizzare la risorsa da esse disciplinata.

In quest'ultimo senso proprio le fonti relative alla *governance* di Internet ci paiono paradigmatiche: si pensi all'ineluttabile necessità di rispettare le RFC (ne abbiamo parlato nel par. 1) o le regole previste per il sistema DNS per *tutti* coloro (Stati, organizzazioni internazionali, organizzazioni non governative, imprese, individui) che vogliano usufruire della Rete.

Peraltro, a scanso di equivoci, riteniamo opportuno chiarire che a noi pare che, anche con riferimento alle strutture "informali" in discorso, il consenso statale giochi ancora un ruolo determinante (ma, si badi, non esclusivo), ma che esso, in tali casi venga espresso con modalità e in contesti peculiari, che potrebbero modificarne forma e contenuto e che, insomma, le "novità" riguardino l'emersione di inediti modelli procedurali.

Quanto sin qui detto, a nostro giudizio, non implica però che si sia perfezionato il superamento della struttura post-westfaliana del diritto (e dell'ordinamento) internazionale: come è stato detto, infatti, "il global law non sostituisce il diritto internazionale, non incarna un diritto esclusivo di ogni altro, e non è un metaordinamento mondiale" [132]. Lo Stato resta ancora al centro di questo sistema – si pensi, ad esempio, al ruolo che il consenso USA ha giocato nel passaggio alla nuova *governance* del sistema DNS – e

[130] R. Brownsword, K. Yeung, *Regulating Technologies: Tools, Targets and Thematics*, in Id. (Eds), *Regulating Technologies*, cit., 5.

[131] Sul tema, anche per riferimenti, si vedano A. Boyle, *Soft law in International Law-making*, in M.D. Evans (ed.), Oxford, 2010, 411 ss. e, in una prospettiva differente, E. Mostacci, *La soft law nel sistema delle fonti: uno studio comparato*, Milano, 2008, *passim*.

[132] G. Palombella, *È possibile una legalità globale? Il* Rule of law *e la governance del mondo*, Bologna, 2013, 151. C. Focarelli, *Diritto internazionale*, cit., afferma chiaramente che "il diritto internazionale di oggi *tende* a regolare questa rete e questo flusso globale. Si tratta di una tendenza che non va sottovalutata in nome di esigenze formali perché il diritto internazionale, come il diritto in genere, è intrinsecamente in movimento e va colto nel movimento. (…) Il diritto internazionale è il diritto che regola strumentalmente la comunità degli Stati per regolare in ultima analisi la comunità individuale universale", 92-93.

DPCE online
ISSN: 2037-6677

continua a detenere il monopolio della forza (si pensi alla cyber guerra); il sistema attuale, insomma, non è (almeno non ancora) caratterizzato dall'emersione di nuovi soggetti dell'ordinamento internazionale, ma, per ora, dall'emersione di nuovi procedimenti normativi.

Due delle critiche mosse dalla dottrina alle forme di regolamentazione internazionale di cui stiamo parlando è che esse sarebbero prive delle *garanzie* tipiche delle norme giuridiche[133] e che le strutture miste che le gestiscono sarebbero caratterizzate da un difetto di *accountability*.

Con riguardo alla prima critica è stato replicato che, grazie alla partecipazione di numerosi attori differenti con alte competenze specialistiche, le norme internazionali così elaborate, sarebbero supportate addirittura da un *consensus* più ampio di quelle tradizionali, sia *ex ante*, in fase di sviluppo della norma, sia *ex post*, quando la norma viene accettata in quanto "funzionante"[134].

Per quanto, poi, concerne le critiche relative al difetto di *accountability*, ci pare che esse vadano ridimensionate, per varie ragioni, non ultima la difficile inquadrabilità in termini giuridici internazionalistici della categoria stessa: si tratta di un tema molto complesso e che non può essere esaminato compiutamente in questa sede, ma qui ci preme ricordare almeno come tale espressione sia spesso utilizzata nella letteratura internazionalistica[135] per fare riferimento, in maniera peraltro spesso indistinta, a varie forme di controllo dell'autorità pubblica; spesso ONG e multinazionali sono chiamate ad essere "accountable" per le loro attività nel campo, ad esempio, dei diritti umani, e tuttavia, una pretesa siffatta pare riflettere più che altro l'esigenza di attribuire a questi attori una qualche forma di responsabilità succedanea di quella di diritto internazionale, attualmente da escludersi[136].

---

[133] J. Klabbers, *The Idea(s) of International Law*, in S. Muller, S. Zouridis, M. Frishman, L. Kistemaker (Eds), *The Law of the Future and the Future of Law*, Oslo, 2011, 79.

[134] N. Krisch, *The Decay of Consent: International Law in An Age Of Global Public Goods*, in *American Journal of International Law*, 2014, 1 ss. studia il mutato ruolo del consenso in relazione ai beni pubblici globali. Si vedano anche, seppure su basi teoriche differenti e in una prospettiva maggiormente di diritto interno, G.P. Calliess, Zumbansen, *Rough Consensus and Running Code: A Theory of Transnational Private Law*, Oxford, 2010.

[135] Per qualche esempio si vedano R. Collins, N. White, *Moving Beyond the Autonomy-Accountability Dichotomy: Reflections on Institutional Independence in the International Legal Order*, in *International Organizations Law Review*, 2010, 1 ss.; A. Reinsch, *Securing the Accountability of International Organizations*, in *Global Governance*, 2001, 131 ss.

[136] Cfr. il "Final Report of the International Committee on the Accountability of International Organizations" adottato dall'International Law Association nel 2004. Nel documento si stabilisce chiaramente che l'*accountability* è connessa all'autorità ed al potere di un'organizzazione internazionale. Specificamente sull'applicazione della categoria della *accountability* ad Internet, e, in particolare, all'ICANN v. C.N.J. De Vey Mestdagh, R.W. Rijgersberg, *Rethinking Accountability in Cyberspace: A New Perspective on ICANN*, in *International Review of Law, Computers & Technology*, 2007, 27 ss.; T.M. Lenard, L.J. White, *Improving ICANN's governance and accountability: a policy proposal*, in *Information economics and policy*, 2011, 189 ss.; J.G. Koppell, *Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"*, in *Public Administration Review*, 2005, 94 ss.; R.H. Weber,

Insomma, la disciplina di diritto internazionale di Internet pare esser costruita attraverso la *concorrenza* di modelli regolatori di diritto internazionale di tipo classico, come il regime del patrimonio comune di cui abbiamo detto, in particolare per quanto concerne le limitazioni imposte agli Stati, e modelli regolatori informali i quali invece servono ad ampliare il novero dei soggetti che partecipano alla *governance* di Internet oltre la sfera dei soggetti dell'ordinamento internazionale in senso stretto, come Stati e organizzazioni internazionali governative.

Questi ultimi – ai quali è da aggiungersi l'istituzione, da ultimo, del Comitato per il controllo (*Oversight Board*), l'organo di controllo della legittimità delle informazioni pubblicate su o censurate da Facebook[137] – inserendosi nel trend più ampio di cui abbiamo detto, contribuiscono al consolidamento dell'informalizzazione dell'ordinamento internazionale e, in particolare, delle sue fonti e di alcuni dei suoi procedimenti di produzione[138].

Gianpaolo Maria Ruotolo
Dipartimento di Giurisprudenza
Università di Foggia
gianpaolo.ruotolo@unifg.it

R.S. Gunnarson, *A Constitutional Solution for Internet Governance*, in *Columbia Science & Technology Law Review*, 2013, 1 ss.; J. Weinberg, *ICANN and the Problem of Legitimacy*, in *Duke Law Journal*, 2000, 187 ss.

[137] Sul punto rinviamo a L. Gradoni, *Constitutional Review via Facebook's Oversight Board. How platform governance had its Marbury v Madison*, e O. Pollicino, G. De Gregorio, *Shedding Light on the Darkness of Content Moderation. The First Decisions of the Facebook Oversight Board* entrambi in *Verfassungsblog*, 2021, nonché a L. Helfer, M. K. Land, *Is the Facebook Oversight Board an International Human Rights Tribunal?*, in *Lawfare*, 13 maggio 2021, tutti reperibili online, nonché a G.M. Ruotolo, *Scritti*, cit., 265 ss.

[138] "One area that illustrates this is the internet sector. Thick stakeholder consensus is visible, for example, in the so-called Internet Governance Forum, established with a view to better understanding issues related to internet governance and to promoting dialogue among stakeholders in an open and inclusive manner. The IGF allows for many groups to participate in meetings: governments, the private sector, civil society, intergovernmental and other international organizations. In the 2010 meeting (in Vilnius), 1,451 people participated (a total of around 2,000 people were present). The breakdown of participants shows that all the major stakeholder groups were represented almost equally, with 21 per cent of participants coming from civil society, 23 per cent from the private sector, 24 per cent comprising government representatives, and 22 per cent made up of technical and academic communities. Institutionalization took place on the basis of the creation of a *de facto* secretariat, the Multi-stakeholder Advisory Group (MAG)"; cfr. R.A. Wessel, *Regulating Technological Innovation through Informal International Law: The Exercise of International Public Authority by Transnational Actors*, in M.A. Heldeweg, E. Kica (Eds), *Regulating Technological Innovation: A Multidisciplinary Approach*, Basingstoke, 2011, 77, il quale riconosce altresì esplicitamente l'esistenza di una "intense cooperation between State and non-State actors, in the regulation of the Internet".