Internet (diritto internazionale)

Chapter · October 2014

CITATIONS
0

READS
372

1 author:

Gianpaolo M. Ruotolo
Università degli studi di Foggia
79 PUBLICATIONS **7** CITATIONS

SEE PROFILE

ENCICLOPEDIA DEL DIRITTO

ESTRATTO

ANNALI VII

Gianpaolo Maria Ruotolo

INTERNET (DIRITTO INTERNAZIONALE)

pubblicazione fuori commercio

GIUFFRÈ

INTERNET (diritto internazionale)

1. *Premesse terminologiche e tecniche utili all'individuazione dell'oggetto dell'indagine.* — Il corretto inquadramento della disciplina giuridica di *Internet* presuppone la piena comprensione delle caratteristiche tecniche della Rete, sulle quali la dottrina giuridica ha spesso poco opportunamente sorvolato, dal momento che esse ne influenzano in maniera determinante le modalità di funzionamento e, quindi, di regolamentazione.

Con l'espressione *Internet* (contrazione di "*interconnected networks*", ovvero "reti interconnesse"), cui fanno da omologo *web* (1) e Rete ma anche, in maniera più evocativa, cyberspazio (2), si fa riferimento a un sistema complesso di apparecchi in origine coincidenti coi soli *computer*, ma negli ultimi tempi anche di diverso tipo come televisioni, *smartphone* o *consolle* per videogiochi, distribuiti in maniera disomogenea sulla superficie del pianeta (3), i quali comunicano tra loro mediante un segnale elettrico trasmesso da mezzi differenti come i cavi originariamente posati per le comunicazioni telefoniche, le fibre ottiche, o anche via etere. Con le medesime espressioni (*Internet*, Rete, *web*) si fa anche riferimento all'insieme di dati complessivamente conservati su tutte le macchine connesse mediante la Rete: tra le due accezioni, quindi, esiste una sorta di rapporto contenuto/contenitore: al fine di evitare fraintendimenti, cercheremo di rendere palese, nel corso della nostra esposizione, l'accezione che stiamo via via utilizzando, con l'avvertenza che oggetto della nostra analisi sarà essenzialmente la disciplina giuridica di diritto internazionale della Rete come infrastruttura.

È altresì il caso di premettere che la Rete ha avuto una crescita esponenziale, passando dalle quattro macchine connesse tra loro nel dicembre 1969, quando il suo nome era ancora ARPANet, acronimo di *Advanced Research Project Agency Net* del Dipartimento della Difesa statunitense, agli oltre cinquecento milioni (4) del 1998, ai due miliardi attuali, per attenersi alle stime dell'*International Telecommunications Union* (ITU), l'Agenzia specializzata delle Nazioni Unite competente in materia e che, come vedremo, mira a giocare un ruolo di primo piano nell'amministrazione internazionale della Rete.

La stessa denominazione data al sistema ("*interconnetted networks*"), poi, ne rende palese il

(1) Tale espressione non va confusa con « *world wide web* » (www), che identifica invece un particolare servizio offerto per il tramite della Rete e che consente di consultare un insieme vastissimo di contenuti (multimediali e non) a tutti o a una parte selezionata degli utenti connessi.

(2) Quest'ultima espressione è stata utilizzata per la prima volta, nell'accezione ormai diffusa di spazio digitale "navigabile" nel quale le persone interagiscono attraverso informazioni, dallo scrittore statunitense William Gibson, fondatore della corrente *cyberpunk*, nel romanzo *Neuromancer*, del 1984: « *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts* [...]. *A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non space of the mind, clusters and constellations of data. Like city lights, receding* »: GIBSON, *Neuromancer*, New York, 1984, 51.

(3) Limitazioni di accesso alle tecnologie dell'informazione possono essere causate dall'arretratezza delle infrastrutture, dalle condizioni economiche delle persone, dal loro scarso livello di alfabetizzazione (non solo) informatica o, ancora, dalle particolarità geomorfologiche di un determinato territorio, dando così luogo al cosiddetto *digital divide*, il quale può sussistere non solo tra Stati diversi, ma anche all'interno del medesimo Paese; cfr., da ult., ALI, *The Power of Social Media in Developing Nations: New Tools for Closing the Global Digital Divide and Beyond*, in *Harvard Human Rights Journal*, 2011, 185 ss.

(4) 541.677.360, secondo i dati dell'*Internet Systems Consortium*, www.isc.org.

modo di operare: la Rete, infatti, utilizzando un insieme di protocolli di comunicazione complessivamente detto *suite* di protocolli TCP/IP (*Transmission Control Protocol/Internet Protocol*) collega tra loro innumerevoli sottoreti, come quelle presenti in un ufficio o in un'abitazione; essa, pertanto, è suddivisa in sezioni che comunicano attraverso apparecchiature dedicate all'indirizzamento dei dati; nessuna sottorete è in grado di controllare tutta la Rete, né, d'altro canto, la rottura o il blocco di una o più sottoreti comporta la perdita di funzionalità del meccanismo complessivo di trasmissione dei dati.

Quanto ai protocolli, essi rappresentano il linguaggio comune che consente a macchine anche molto diverse di comunicare tra loro e costituiscono quindi il presupposto dell'architettura di rete "aperta", grazie alla quale tutte le sottoreti connesse possono comunicare tra loro indipendentemente da *hardware* e *software* utilizzati. Tali protocolli, peraltro, in un sistema complesso e ramificato quale quello che si sta descrivendo, hanno anche la funzione di dettare le regole per il cosiddetto "instradamento" dei dati, le quali consentono che le informazioni giungano correttamente al destinatario desiderato senza disperdersi dopo aver viaggiato attraverso una molteplicità di macchine e aver percorso migliaia di chilometri (5). A tali fini i dati da trasmettere sono suddivisi dalla macchina mittente in gruppi elementari, detti pacchetti, che viaggiano autonomamente nella Rete, e che saranno ricomposti alla fine del loro viaggio dalla macchina di destinazione (tale tecnica è detta *packet switching*). La Rete, quindi, si limita a trasmettere i dati senza effettuare su di essi alcuna elaborazione, che viene effettuata dalle macchine di partenza e di arrivo: questo meccanismo, detto *end-to-end* (e2e), consente alla Rete di essere molto "leggera" e quindi facilmente adattabile alle nuove esigenze a differenza di quanto avviene, ad esempio, nelle reti telefoniche di tipo classico, in cui gli apparecchi connessi non compiono alcuna operazione sui dati trasmessi, che viene effettuata invece proprio dalla rete stessa (è per questo motivo che aggiungere nuove funzioni a una rete telefonica — si pensi, ad esempio, al servizio di cosiddetta identificazione del chiamante, implementato sulle reti di telefonia fissa solo decine di anni dopo la loro attivazione — risulta molto più complesso e costoso di quanto non avvenga su *Internet*, essendo necessaria, nel primo caso, una modifica di tutta la rete anziché degli apparecchi).

Ogni singolo pacchetto di dati inviato via *web*, poi, reca con sé una sequenza di informazioni con la funzione di garantire la corretta ricostruzione dell'intero messaggio (la procedura di attribuzione di detta sequenza, che viene effettuata dalla macchina mittente, è detta incapsulamento): è come se, per inviare una lettera, il mittente la scomponesse in molte parti da spedire autonomamente al destinatario in buste numerate, lasciando a quest'ultimo il compito di "rimontare" il messaggio originario. Ancora, il sistema del *packet switching* è concepito in maniera tale da consentire di individuare l'eventuale perdita di una parte dei dati che compongono il messaggio: ogni *computer* che invia un'informazione ottiene infatti, al momento della ricezione, una sorta di ricevuta di consegna (*acknowledgement*) che consente la ritrasmissione dei dati eventualmente persi, cioè di quei pacchetti in relazione ai quali il *computer* mittente non ha ottenuto la conferma di ricezione; ogni pacchetto di informazioni, infine, è corredato da un codice di controllo (detto *checksum*), calcolato dal *computer* sorgente e che viene verificato dalla macchina di destinazione per assicurare l'integrità del pacchetto stesso (6).

Internet, quindi, nell'accezione che ci interessa, è un'infrastruttura — sulla quale transitano dati che possono poi assumere forme e contenuti differenti, come *file* audio, video, gli ipertesti del *world wide web* o un messaggio di posta elettro-

(5) La struttura di *Internet*, con una buona approssimazione, può essere descritta come un sistema con una miriade di ramificazioni, in cui ogni nodo è collegato a molti altri: una sua rappresentazione grafica, una sorta di mappa geografica del cyberspazio, detta *Peacock Map* per la sua somiglianza alla coda di un pavone, è stata elaborata, fino al 1998, da H. Burch e B. Cheswich ed è resa pubblica al sito www.cheswick.com. Interessante chiarire come la mappatura della Rete sia stata, sulle prime, effettuata manualmente utilizzando oltre centomila volte il comando *traceroute* ("*tracert*"), comunemente presente nei sistemi operativi ad interfaccia testuale, e che consente di ricavare il percorso seguito dai pacchetti di dati sulle reti informatiche, ovvero l'indirizzo IP di ogni *router* attraversato per raggiungere il destinatario. Da ultimo un gruppo di ricerca dell'Università del Michigan ha reso noto di essere riuscito a mappare, utilizzando un solo *computer* e *ZMap*, un programma *open source*, l'intera Rete IPv4 in soli 45 minuti, riuscendo finanche a mappare gli effetti dell'uragano Sandy, abbattutosi nel 2012 sulla costa orientale degli Stati Uniti: nell'area colpita infatti c'è stato un calo del trenta per cento di apparecchi connessi; cfr. DURUMERIC, WUSTROW e HALDERMAN, *ZMap: Fast Internet-wide Scanning and Its Security Applications*, in *Proceedings of the 22nd USENIX Security Symposium* (Washington D.C., 14-16 agosto 2013), in www.usenix.org, 605 ss. Uno strumento così potente e alla portata di tutti, tuttavia, apre alla dimensione amatoriale anche azioni malevole su ampia scala.

(6) Per un'analisi dettagliata dei meccanismi di funzionamento dei protocolli v. SIYAN e PARKER, *TC/IP Unleashed*, Indianapolis (Indiana), 2002.

nica — priva di organizzazione gerarchica (7): al suo interno, infatti, non esiste alcun punto, né "centrale" né di "vertice", dal quale si diramano tutti i percorsi, né è possibile individuare una macchina alla quale tutte le altre devono essere collegate per comunicare tra loro; le singole sottoreti, invero, sono connesse tra loro in numerosi punti. È grazie a questa architettura che la Rete può sopravvivere al collasso di alcuni suoi rami, dal momento che a ogni pacchetto di informazioni viene offerta una molteplicità di strade da seguire per raggiungere una determinata destinazione: sono queste caratteristiche strutturali a rendere la Rete difficilmente assoggettabile a forme di *governance* generale verticalizzata, sia per quanto riguarda i suoi aspetti tecnici (tranne per alcune eccezioni di cui si dirà appresso: v. *infra*, § 3) sia per quanto concerne le politiche di accesso e uso.

È poi il caso di chiarire l'accezione che, nel contesto di cui ci stiamo occupando, daremo al termine *governance* (8): a tal fine riteniamo di recepire la definizione adottata dal *Working Group on Internet Governance* istituito nell'ambito del *World Summit on the Information Society* (WSIS) delle Nazioni Unite di cui diremo appresso (v. *infra*, § 4), secondo la quale essa è il prodotto dello sviluppo e dell'applicazione, da parte di soggetti pubblici (Stati, organizzazioni internazionali) e privati (imprese, organizzazioni non governative, individui) di norme, principi, procedure e programmi condivisi che disciplinano l'utilizzazione e promuovono lo sviluppo della Rete (9). Useremo dunque un'accezione che, seppure molto ampia, fa esclusivo riferimento alle regole che disciplinano il funzionamento e l'utilizzazione della Rete in quanto mezzo, ad esclusione, quindi, delle norme adottate nelle sedi più disparate per disciplinare le attività umane che vi si svolgono (come, ad esempio, gli scambi commerciali).

2. *La disciplina giuridica di* Internet *e il diritto internazionale: modelli ricostruttivi e limitazioni di accesso alla Rete.* — Le caratteristiche tecniche di cui abbiamo appena detto, in uno con la natura ontologicamente transnazionale della Rete, ne hanno resa oltremodo difficoltosa una compiuta ed efficace regolamentazione unilaterale da parte degli Stati; la dottrina, già dagli anni Novanta del secolo scorso, ha così iniziato a investigare i problemi connessi alla disciplina giuridica di *Internet*, facendo emergere nel tempo diversi approcci ricostruttivi, riconducibili essenzialmente a tre autonomi modelli di cui è opportuno dare, seppur succintamente, conto (10).

Un primo approccio, affermatosi soprattutto agli albori della diffusione "globale" di *Internet*, ne enfatizzava le peculiarità sostenendone, per questo, la non regolabilità per il tramite delle tradizionali categorie giuridiche e, più in generale, del diritto (11): l'assenza di frontiere fisiche nel cyberspazio avrebbe infatti impedito l'individuazione del diritto (statale) applicabile alle fattispecie *on-line*, il giudice competente a dirimere le relative controversie e, in ogni caso, implicato rischi di *spillover* (12): sottoporre *Internet* al dominio del diritto statale, secondo questo orientamento, avrebbe potuto implicare il conflitto tra differenti regolamentazioni del medesimo fenomeno, in numero potenzialmente coincidente con quello dei legislatori statali, tra loro incompatibili. Pertanto si suggeriva di adottare per la Rete meccanismi di disciplina per così dire autonomi (13), le cui regole fossero cioè il prodotto di un procedimento normativo gestito dagli stessi utenti, che avrebbe dato luogo a un *tertium genus* di diritto, né statale né internazionale, che si suggeriva di denominare *cyber-law* (14). Tutto l'approccio ap-

(7) Cfr. CRAGO, *Fundamental Rights on the Infobahn: Regulating the Delivery of Internet Related Services Within the European Union*, in *Hastings International & Comparative Law Review*, 1997, 467 ss.

(8) V. anche DONATI, *Internet (diritto costituzionale)*, in questo Annale, 532 ss.

(9) Cfr. il *Report of the Working Group on Internet Governance* del giugno 2005, in www.wgig.org.

(10) Per un'analisi della rilevanza complessiva del diritto rispetto al fenomeno in esame cfr. GOLDSMITH e WU, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, 2006; KULESZA, *International Internet Law*, New York, 2012.

(11) Per un'esposizione dell'orientamento citato cfr., per tutti, JOHNSON e POST, *Law and Borders. The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, 1367; POST, *In Search of Jefferson's Moose*, Oxford, 2009, *passim*.

(12) L'uso dell'espressione *spillover* in questa accezione è di JOHNSON e POST, *op. cit.*, 1374. Sul problema cfr. anche SEGURA SERRANO, *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, 2006, 191 ss.

(13) In merito basti citare la ormai celeberrima Dichiarazione di indipendenza del cyberspazio (Davos, 8 febbraio 1996) 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. BARLOW, *A Cyberspace Independence Declaration*, San Francisco, 1996. La Dichiarazione è integralmente pubblicata in projects.eff.org/~barlow/Declaration-Final.html.

(14) Si pensi, ad esempio, al caso della cosiddetta *netiquette*, 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*, che

pena illustrato, oltre a concepire *Internet* come uno spazio quasi ontologicamente « a-giuridico » (15), costruiva quindi le regole ivi applicabili, in quanto generate spontaneamente dagli utenti, alla stregua della *lex mercatoria* (16), sistema di norme elaborate dalla comunità che se ne deve servire e che, in quanto regole, per così dire, transazionali delle relazioni economiche, sono state lette come il primo caso di « diritto globale senza Stato » (17).

Un secondo orientamento, più conservativo e che ha di recente assunto consistenza maggioritaria, ritiene *Internet*, un mero mezzo di comunicazione seppure di portata incommensurabile, giuridicamente regolabile (18): la natura transnazionale della Rete renderebbe però necessaria l'armonizzazione dei vari ordinamenti statali per mezzo di norme di diritto internazionale, attraverso cui creare un quadro giuridico comune, in particolare con riguardo ad alcuni aspetti tecnici generali, nel quale i vari legislatori nazionali possano poi muoversi con l'adozione di normative di dettaglio (19). Secondo questo approccio sarebbero anche da ridimensionare i timori di *spillover* di cui si diceva, i quali non costituirebbero un problema peculiare di *Internet* quanto piuttosto il naturale portato di tutte le fattispecie caratterizzate da elementi di estraneità, gestibili attraverso le norme di conflitto, uniformi o comuni. Una compiuta regolamentazione giuridica dei vari aspetti di *Internet* (gestione delle infrastrutture "sottostanti", disciplina dei contenuti del *web*, regolamentazione dei comportamenti umani che hanno luogo nel cyberspazio) non può prescindere, per essere veramente efficace e onnicomprensiva, dall'uso contemporaneo di strumenti di diritto internazionale pubblico e norme di diritto internazionale privato: mentre i primi, infatti, sono idonei a disciplinare il regime di gestione della Rete come infrastruttura, le seconde sono invece di aiuto nell'individuazione, mediante il coordinamento dei vari ordinamenti nazionali, della giurisdizione nazionale competente a dirimere una determinata controversia relativa ad una fattispecie che ha luogo *on-line* e il diritto applicabile alla stessa (20).

Per un terzo modello ricostruttivo, a suo modo intermedio tra i due già illustrati, sarebbe invece impossibile anche solo tentare di decidere aprioristicamente in merito alla natura "regolabile" o "non regolabile" di *Internet*, la quale sarebbe priva di proprie caratteristiche strutturali immodificabili, che verrebbero invece contingentemente determinate dall'insieme di apparecchiature (*hardware*) che la compongono e, soprattutto, dal *software* (il "codice" informatico) che ne consente e disciplina l'uso. Secondo questa visione, insomma, il cyberspazio sarebbe compiutamente disciplinabile proprio per il tramite del suo codice informatico, il quale, però, dovrebbe a sua volta essere regolato, per quanto concerne i valori che lo devono informare, da norme giuridiche uniformi (21). La correttezza di questo approccio che,

è ormai di generale condivisione da parte degli utenti della Rete e implica, in caso di ripetute violazioni, la possibile 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 formalmente il rispetto agli utenti loro clienti.

(15) L'espressione è di GIGANTE, *Blackhole in Cyberspace: the Legal Void in the Internet*, in *The John Mashall Journal of Computer and Information Law*, 1997, 413 ss., il quale parla di « vuoto giuridico ».

(16) GALGANO, *Lex mercatoria*, in questa *Enciclopedia*, Aggiornamento, V, 2001, 721 ss.

(17) Cfr. TEUBNER, *Breaking Frames: Economic Globalisation and the Emergence of* Lex Mercatoria, in *European Journal of Social Theory*, 2002, 199 ss. Una ricostruzione siffatta, però, pare sollevare più dubbi di quanti non ne risolva, dal momento che pone, senza affrontarlo compiutamente, il difficile problema dell'esistenza di un terzo *genus* di norme giuridiche oltre al diritto internazionale e al diritto interno, problema che occupa da tempo la dogmatica giuridica proprio con riguardo alla *lex mercatoria.* Sul punto v. DRAETTA, *Internet e commercio elettronico nel diritto internazionale dei privati*, Milano, 2001, 19 ss.

(18) Per una illustrazione di tale approccio cfr., per tutti, GOLDSMITH, *Internet and the Abiding Significance of Territorial Sovereignty*, in *Indiana Journal of Global Legal Studies*, 1998, 475 ss.

(19) GOLDSMITH, *Against Cyberanarchy*, in *University of Chicago Law Review*, 1998, 1240 ss.; TRACHTMAN, *Cyberspace, Sovereignty, Jurisdiction and Modernism*, in *Indiana Journal of Global Legal Studies*, 1998, 568 ss.; MODY, *National Cyberspace Regulation: Unbounding the Concept of Jurisdiction*, in *Stanford Journal of International Law*, 2001, 382 ss.

(20) Sul rapporto tra diritto internazionale pubblico e diritto internazionale privato nel contesto in esame cfr. 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.; SCHULTZ, *Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, in *Eur. journ. intern. Law*, 2008, 799 ss.; 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 in www.svantesson.org. Per un'analisi della disciplina internazionalprivatistica della Rete v. BARIATTI, *Internet*: III) *Diritto internazionale privato e processuale*, in *Enc. giur.*, Aggiornamento, 2001.

(21) Cfr. 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*

consapevole delle difficoltà di disciplinare efficacemente la Rete per il tramite di mezzi esclusivamente giuridici, accresce la rilevanza, anche sotto il profilo regolatorio, del dato tecnico, pare da ultimo confermata dalle enormi difficoltà di controllo e repressione incontrate dai meccanismi giuridici "tradizionali" nei confronti del cosiddetto *deep web*, la (gran) parte di *Internet* che non è indicizzata dai motori di ricerca e che, ad oggi, rappresenta l'ultima frontiera della criminalità organizzata.

L'analisi della prassi conferma come gli strumenti di diritto interno, da soli, siano inidonei a disciplinare efficacemente l'uso di questa peculiare infrastruttura: si pensi, ad esempio, a come le pur importanti restrizioni all'accesso a *Internet* adottate da alcuni Paesi del Nord Africa e del Medio Oriente non siano riuscite ad impedire le comunicazioni dei cittadini di questi Paesi, attuate in particolare per il tramite dei *social network*, che hanno in qualche modo accelerato le rivoluzioni della cosiddetta "onda verde" del 2011 (22). Proprio l'inidoneità degli ordinamenti nazionali a regolare unilateralmente le questioni che ci occupano ha costituito la premessa della Dichiarazione di principi *Building the Information Society: A Global Challenge In The New Millennium*, adottata a Ginevra il 12 dicembre 2003 nell'ambito del *World Summit on the Information Society* (Wsis) promosso dalle Nazioni Unite, e di cui diremo *infra*, § 5, dove si riconosce alla *governance* di *Internet* una natura "multilivello", la quale implica necessariamente il coinvolgimento di una pluralità di attori, sia di rilevanza pubblicistica, come Stati e organizzazioni internazionali, sia di tipo privatistico, come operatori economici, organizzazioni non governative e la cosiddetta società civile (23).

L'ordinamento internazionale appare quindi chiamato a governare su base globale la Rete o quanto meno a fissare alcuni principi generali che (de)limitino la *domestic jurisdiction* degli Stati in materia: a tal fine, esso, come vedremo subito *infra*, § 3, si avvale in massima parte di norme di diritto internazionale generale e di diritto pattizio preesistenti alla Rete e che erano originariamente volte a disciplinare fattispecie da questa differenti; disposizioni specificamente applicabili alla Rete sono poi contenute in strumenti non vincolanti adottati da numerose organizzazioni internazionali.

3. *Inesistenza di norme di diritto internazionale generale specificamente applicabili ad* Internet*: la gestione unilaterale del sistema* Dns *da parte degli Stati Uniti.* — Allo stato attuale di sviluppo dell'ordinamento internazionale non è possibile individuare norme di diritto consuetudinario che limitino la sovranità statale relativamente alla gestione di *Internet*. A tale riguardo si può esaminare la prassi e i meccanismi giuridici che regolano il sistema dei nomi di dominio (*Domain Name System* - Dns): sebbene sia certamente limitativo far coincidere *in toto* il governo di *Internet* con la sola gestione di tale sistema, esso ne rappresenta però un elemento nevralgico, in quanto solo il suo corretto funzionamento assicura l'esistenza stessa della Rete come è oggi intesa.

Come abbiamo già detto, *Internet* non è sottoposta ad alcuna forma di *governance* verticalizzata né per quanto riguarda i suoi aspetti tecnici né in merito alle politiche di accesso e uso: l'unica eccezione degna di nota è relativa proprio all'assegnazione delle coordinate che consentono l'individuazione univoca di ogni dispositivo collegato e cioè all'assegnazione dell'indirizzo Ip e del nome di dominio (*domain name*) eventualmente ad esso associato (24).

L'indirizzo Ip (*Internet Protocol address*), in particolare, è un numero che identifica univocamente un dispositivo collegato alla Rete: nella versione Ipv4, quella attualmente più in uso, esso viene descritto mediante quattro numeri in base decimale, separati da un punto; gli indirizzi assegnati in base a questo protocollo sono ormai praticamente esauriti (al fenomeno si fa riferimento con l'espressione *Ipcalypse* o anche *Arpageddon*); per questo motivo è stata approntata una versione successiva del protocollo, la cosiddetta Ipv6, la quale consente di assegnare un numero maggiore di indirizzi Ip: ad ogni modo quanto appena detto ci consente di qualificare sin d'ora la Rete, almeno sotto alcuni aspetti, come una risorsa esauribile.

---

law). The challenge for our generation is to reconcile these two forces ».

(22) 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* », 16 maggio 2011, doc. A/HRC/17/27, in www.ohchr.org. Cfr. *infra*, § 8.

(23) World Summit on the Information Society, *Declaration of Principles*, WSIS-03/GENEVA/DOC/4-E, 12 dicembre 2003, Article 49, in www.itu.int.

(24) La conversione di un nome di dominio in indirizzo Ip è detta risoluzione, mentre la conversione di un indirizzo Ip in nome di dominio è detta risoluzione inversa. Come vedremo, entrambe vengono realizzate mediante l'accesso ad un *database* che contiene le associazioni nome di dominio/indirizzo Ip.

Un nome di dominio, ciò che digitiamo quando intendiamo consultare un sito *web*, è invece costituito da una serie di caratteri (stringa alfanumerica) separati da punti: ogni stringa rappresenta un livello, per così dire, gerarchico del nome; al primo livello, che è rappresentato dalla prima parte del nome di dominio letto partendo da destra, che individua il *genus* di dominio, seguono livelli via via più specifici. I domini di primo livello, poi, sono suddivisi in due grandi gruppi: quelli generici e quelli nazionali. I domini generici di primo livello (*generic Top Level Domains*, gTLDs), costituiti da un suffisso di tre o più lettere, sono quelli che, almeno in teoria, possono essere utilizzati da particolari categorie di organizzazioni (25) indipendentemente dalla loro localizzazione geografica, (sebbene, per ragioni meramente storiche, tre di essi, « .gov », « .mil » e « .edu », siano ancora oggi riservati rispettivamente al governo, all'esercito e agli enti educativi statunitensi) (26); i domini di primo livello nazionali fanno invece riferimento ad indirizzi che puntano a entità/operatori/servizi che sono localizzati in un determinato Stato o in una sua dipendenza territoriale e sono costituiti da due o tre lettere (si pensi all'estensione « .it » utilizzata per l'Italia).

La procedura di assegnazione dei nomi di dominio è gestita in via esclusiva da un'organizzazione statunitense di diritto privato senza scopo di lucro, la *Internet Corporation for Assigned Names and Numbers* (ICANN), istituita nel 1988 alla luce delle norme statali californiane, la quale amministra direttamente i gTLDs e, indirettamente, tutti gli altri (27). Tale organizzazione ha delegato alcuni dei suoi compiti, in particolare quello dell'assegnazione degli indirizzi IP, a un ente ad essa preesistente, la *Internet Numbers Assigned Authority* (IANA) (28), che è oggi amministrata direttamente dalla stessa ICANN, la quale si occupa invece in prima persona dei gTLDs, degli indirizzi IP, dei parametri di protocollo e del coordinamento della stabilità del *root server system* tutto.

Comprendere il modo di operare del DNS equivale a comprendere i meccanismi di base del funzionamento della Rete e, di conseguenza, le strategie attraverso le quali tali meccanismi possono essere alterati per il tramite di un intervento "normativo".

La Rete, infatti, non identifica i suoi "nodi" mediante i nomi di dominio, che hanno solo la funzione di essere più facilmente comprensibili dagli esseri umani, bensì mediante gli indirizzi numerici IP: il compito di trasformare un nome di dominio digitato da un utente in un indirizzo IP comprensibile per la Rete è quindi svolto, in ultima istanza, da soli tredici *root server* (*server* "radice") mediante un *root database* che ha la funzione di far conoscere alle macchine connesse che lo consultano l'indirizzo IP corrispondente al nome di dominio digitato. In realtà, dal momento che la maggior parte delle informazioni contenute nei *root server* cambia piuttosto di rado, essa viene memorizzata nella memoria di *server* DNS di gerarchia inferiore, ai quali si rivolgono in prima battuta i *computer* connessi; la richiesta viene infine girata ai *root server* se quelli "intermedi" non riescono a individuare l'indirizzo numerico corrispondente al nome digitato.

Sebbene di tali *server*, e quindi del *root database*, esistano oltre centotrenta "copie" localizzate su altrettanti *computer* fisici disseminati su tutto il pianeta — realizzate mediante un sistema di indirizzamento detto *anycast*, che consente di assegnare il medesimo indirizzo IP a più macchine fisiche —, tali *server* sono gestiti in maniera esclusiva dal Governo statunitense attraverso la *National Telecommunications and Information Administration* (NTIA) del *Department of Commerce*, la quale detiene il potere esclusivo di autorizzare o imporre unilateralmente le modifiche al contenuto del suddetto *database* (29).

La fattispecie appena descritta rientra tra le forme di applicazione extraterritoriale della potestà di governo: come noto, ciò accade quando una

(25) Si pensi al dominio « .com », che teoricamente sarebbe riservato alle sole organizzazioni di tipo commerciale.

(26) Gli Stati Uniti sono il Paese sul cui territorio *Internet* è in origine nata, come un progetto di ricerca del Dipartimento della difesa; anche per questo essi rivendicano diritti esclusivi di gestione della Rete. Cfr. RYAN, *Storia di Internet. Il futuro digitale*, Torino, 2011.

(27) In letteratura v., da ult., CAROTTI, *L'ICANN e la governance di Internet*, in *Riv. trim. dir. pubbl.*, 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 www. iilj.org; DELBIANCO e COX, *ICANN Intenet Governance: Is It Working?*, in *Global Business & Development Law Journal*, 2008, 27 ss.

(28) La IANA è l'organismo che ha responsabilità nell'assegnazione degli indirizzi IP, la quale però viene delegata ad enti regionali denominati *Regional Internet Registries* col compito di assegnare gli indirizzi per una specifica zona del mondo. La IANA nasce come organo consultivo della *Internet Society* (ISOC), organizzazione *non-profit* fondata nel 1992, con l'obiettivo di fornire una struttura organizzata che supportasse la definizione degli *standard* sulla Rete. Cfr. www.iana.org.

(29) Specificamente sulla gestione del *root file* del sistema DNS v. MUELLER, *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge-London, 2002.

norma statale viene utilizzata per disciplinare comportamenti localizzati al di fuori dei confini dello Stato che la ha adottata. È ormai pacifico che un'applicazione siffatta sia consentita non solo con riguardo a norme di diritto "privato", ma anche di diritto pubblico (30). La dottrina ha distinto tra la « mera applicazione extraterritoriale del diritto interno » — cioè l'esercizio all'estero del potere normativo di uno Stato, che sarebbe potenzialmente consentito tranne ove sia dimostrata l'esistenza di specifici divieti posti dal diritto internazionale generale — e l'esercizio del potere coercitivo o di governo in senso stretto, che trova invece un limite nel principio consuetudinario di non ingerenza, il quale potrebbe, a sua volta, essere legittimamente derogato solo in presenza di specifiche previsioni consuetudinarie o pattizie o di autorizzazioni del sovrano territoriale (31).

Quindi il potere in esame, data per certa l'assenza di trattati internazionali che disciplinano la gestione dei *root server*, dovrebbe trovare titolo in una norma di diritto internazionale generale dal contenuto permissivo o, in sua assenza, in autorizzazioni (esplicite o implicite) da parte degli Stati sul cui territorio sono situati i *server*.

Ebbene, la prassi, che si limita ad alcuni *statement* emanati dal Governo USA e, a quanto ci consta, a un solo caso di contestazione dell'esercizio del potere statunitense di gestione dei *server*, promanante dal Brasile (32), non è idonea a suggerire l'esistenza di norme di diritto internazionale generale.

Infatti, sebbene gli Stati Uniti, parlando di un proprio « *historic role* » (33) nella gestione del *file* di *root zone*, facciano riferimento ad una sorta di tradizione di esercizio del relativo potere, e quindi quanto meno all'elemento materiale di una consuetudine, non emerge alcuna convinzione USA di agire nel rispetto di obblighi giuridicamente vincolanti; d'altro canto, a parte le difficoltà di ricostruzione della prassi in materia, talmente scarna e unilaterale da essere inidonea a fornire anche solo un principio di prova in merito all'esistenza di una consuetudine, appare difficile che il diritto internazionale generale possa contenere norme dal contenuto così dettagliato.

Discorso analogo sembra potersi svolgere con riferimento a qualunque norma di diritto internazionale generale applicabile "esclusivamente" ad *Internet*, non tanto per il breve lasso di tempo intercorso dalla sua diffusione su base globale, che può datare, al massimo, agli ultimi due/tre anni del secolo scorso, quanto, come si è appena detto, proprio per il contenuto che norme siffatte dovrebbero avere, eccessivamente complesso per poter essere oggetto di una consuetudine internazionale (34).

In assenza di norme di diritto internazionale che attribuiscano agli Stati Uniti la legittimazione a porre in essere, al di fuori del proprio territorio nazionale, azioni che hanno 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 possono trovare titolo legittimante esclusivamente nell'acquiescenza da parte degli Stati di allocazione territoriale dei *server* (35).

---

(30) Picone, *L'applicazione extraterritoriale delle regole sulla concorrenza e il diritto internazionale*, in *Il fenomeno delle concentrazioni di imprese nel diritto interno e internazionale* (Atti del Convegno, Napoli, 29 aprile 1988), Padova, 1989, 81 ss., in particolare 84 ss.

(31) Cfr. Picone, *op. cit.*, 86 e nt. 6.

(32) Il delegato del Brasile, nel corso della riunione del terzo *Preparatory Committee* (cosiddetto Prepcom III), tenutasi il 20 settembre 2005, della seconda fase del Wsis, sostenne apertamente la carenza di legittimazione del Governo USA ad autorizzare unilateralmente le modifiche al *root database*. Per il testo integrale della mozione brasiliana v. Ruotolo, *Internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012, 55.

(33) Gli *U.S. Principles on the Internet's Domain Name and Addressing System*, del 30 giugno 2005, in www.ntia.doc.gov, prevedono che « *the United States Government intends to preserve the security and stability of the Internet's Domain Name and Addressing System (DNS).* [...] *As such, the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its* historic role *in authorizing changes or modifications to the authoritative root zone file* ».

(34) Esplicito, al riguardo, Fidler, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, in 7 *American Society of International Law Insights*, 2013, n. 6, 1 ss., il quale afferma che « *Internet developed and spread* [...] *without generating rules of international law* ». Né, d'altro canto, ci paiono giungere a conclusioni differenti quegli autori che pure sostengono l'esistenza di norme consuetudinarie applicabili ad alcuni specifici settori di attività sul *web* (in particolare le transazioni elettroniche), dal momento che tali norme, nella stessa costruzione di coloro che se ne occupano, non vengono mai proposte come norme consuetudinarie di diritto internazionale, quanto, piuttosto, come norme spontaneamente prodotte dalla comunità degli utenti di *Internet*: cfr. Chik, *Customary Internet-ional law*: *Creating a body of customary law for cyberspace*, in *Computer Law & Security Review*, 2010, 3 ss.; Polanski, *Customary Law of the Internet. In the Search for a Supranational Cyberspace Law*, Berlin, 2007.

(35) Sulla possibilità che il mero silenzio di uno Stato possa avere importanti effetti giuridici in termini di riconoscimento di una data situazione di fatto o di diritto v. Villani, *Riconoscimento (diritto internazionale)*, in questa *Enciclopedia*, XL, 1989, 634 ss., il quale sottolinea come gli

Peraltro il Governo statunitense ha in più occasioni riconosciuto l'esistenza di interessi legittimi degli altri Stati nella gestione dei loro nomi di dominio nazionali e si è di conseguenza impegnato a collaborare con tutti gli altri membri della Comunità internazionale al fine di assicurare il rispetto della comune esigenza fondamentale di garantire stabilità e sicurezza del sistema DNS (36): appare evidente come lo Stato responsabile della gestione del *root file* riconosca quindi non solo la *domestic jurisdiction* degli altri Stati — anche se con esclusivo riferimento ai domini nazionali di primo livello — ma anche l'esistenza di un interesse comune a tutti gli Stati alla permanenza della funzionalità della Rete.

Allo stato attuale, quindi, non si possono rintracciare norme di diritto internazionale generale specificamente volte a limitare la *domestic jurisdiction* degli Stati nelle materie che ci occupano e, d'altro canto, l'acquiescenza degli Stati sul cui territorio insistono i *root server* all'esercizio extraterritoriale della potestà di governo statunitense si incontra con il riconoscimento, da parte di questi ultimi, dell'esistenza di un interesse comune alla permanenza della funzionalità della Rete.

Infine rileviamo che, alla luce dei recenti studi in materia di *global administrative law*, l'esercizio extraterritoriale della potestà di governo statunitense potrebbe anche essere interpretato come una delle modalità di estrinsecazione dell'"amministrazione globale", appunto: ciò si verificherebbe dal momento che l'ente governativo statunitense si troverebbe ad agire come organo materiale del cosiddetto spazio amministrativo globale e quindi ad essere titolare del legittimo potere di adottare decisioni su questioni di interesse "comune" a tutti i membri della Comunità internazionale (37).

4. *Norme di diritto internazionale pattizio specificamente applicabili ad* Internet*: il fallimento della Convenzione generale del* World Summit on Information Society *(WSIS) delle Nazioni Unite, la Convenzione sul* Cybercrime *del Consiglio d'Europa e le* International Telecommunications Regulations *(ITRS) dell'*ITU *dopo la revisione del 2012.* — Il diritto internazionale pattizio possiede caratteristiche tali per essere, almeno potenzialmente, uno degli strumenti elettivi per la disciplina di *Internet*. E difatti la firma di una Convenzione generale sulla *governance* del *web* era uno degli obiettivi del *World Summit on the Information Society* (WSIS) indetto dall'Assemblea generale delle Nazioni Unite con la risoluzione del 21 dicembre 2001, n. A/RES/56/183 e che aveva luogo in seno all'*International Telecommunications Union* (ITU) in due momenti distinti, a Ginevra dal 10 al 12 dicembre 2003 e, successivamente, a Tunisi dal 16 al 18 novembre 2005.

L'obiettivo della prima fase, conclusasi con l'adozione di una Dichiarazione di principi e di un Piano d'azione sul prosieguo dei lavori, era solo di raggiungere una qualche forma di *consensus* tra gli Stati partecipanti ai lavori in merito all'opportunità di dotarsi di regole comuni di disciplina della società dell'informazione; la seconda fase, che aveva invece lo scopo, ben più ambizioso, di promuovere un accordo quadro relativo alla *governance* di *Internet*, era però segnata dal sostanziale fallimento e si concludeva così con l'adozione di un atto di impegno politico, il *Tunis Commitment* — 18 novembre 2005 (38) —, e dell'*Agenda* di Tunisi per la società dell'informazione, di cui diremo nel paragrafo successivo.

Tuttavia un testo normativo "generale" sulla *governance* di *Internet* avrebbe anche potuto essere foriero di criticità: l'idea stessa di una verticalizzazione del controllo della Rete nelle mani degli Stati o di organizzazioni da questi create, infatti, sarebbe potuta risultare strutturalmente incompatibile con le logiche che fino ad oggi hanno permesso alla Rete di proliferare, come quella *end-to-end* di cui abbiamo detto *supra*, § 1.

Sul negoziato per la Convenzione generale quindi ha gravato il timore che l'irrigidimento delle regole di gestione del *web* avrebbe potuto costituire un limite per i suoi sviluppi futuri, specie tecnologici, anche in considerazione del fatto che la Rete, come si è detto, non è una singola entità, ma un insieme di altre reti, attrezzature,

---

Stati che intendono negare che il loro silenzio possa essere interpretato in tal senso sono soliti esprimere una formale protesta.

Nel caso in esame, a parte il Brasile, peraltro, non si hanno tracce di alcuna protesta da parte degli Stati di allocazione dei *server* all'esercizio del potere statunitense di gestione del DNS.

(36) *U.S. Principles on the Internet's Domain Name and Addressing System*, cit. (v. *supra*, nt. 33).

(37) Cfr. in generale CASINI, *Diritto amministrativo globale*, in *Dizionario di diritto pubblico* a cura di CASSESE, III, Milano, 2006, 1944 ss.; CASSESE, *Il diritto amministrativo globale: una introduzione*, in *Riv. trim. dir. pubbl.*, 2005, 331 ss.; CHESTERMAN, *Globalisation and Public Law: a Global Administrative Law?*, in *Sanctions, Accountability and Governance in a Globalised World* a cura di FARRALL e RUBENSTEIN, Cambridge, 2009, 75 ss.; *Symposium on "Global Governance and Global Administrative Law in the International Legal Order"* a cura di KRISCH e KINGSBURY, in *European Journal of International Law*, 2006, 1 ss.

(38) Doc. WSIS-05/TUNIS/DOC/7-E, reperibile in www.itu.int.

software, applicazioni e tecnologie di proprietà, gestite e utilizzate da una moltitudine di utenti pubblici, privati e istituzionali.

L'unico trattato che contiene norme generali sulla Rete in quanto infrastruttura è quindi la Convenzione del Consiglio d'Europa sulla cybercriminalità (Budapest, 23 novembre 2001): si tratta infatti di un testo che, al di là delle norme materiali e processuali che contiene, tenta, per la prima volta nel contesto internazionale, l'armonizzazione giuridica di categorie e fattispecie generali che hanno come esclusivo riferimento la Rete.

Peraltro la Convenzione, nel suo preambolo, mediante il rinvio alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (firmata a Roma il 4 novembre 1950), al Patto internazionale sui diritti civili e politici (adottato a New York il 16 dicembre 1966 ed entrato in vigore il 23 marzo 1976) e a ogni altro strumento internazionale applicabile, solleva una questione sulla quale avremo modo di tornare (v. *infra*, § 8): la necessità di cercare un soddisfacente livello di bilanciamento tra misure statali restrittive dell'accesso ad *Internet* perché repressive di condotte caratterizzate da un qualche disvalore, da un lato, e il rispetto dei diritti fondamentali, dall'altro.

Il Trattato in esame, che mira a fornire un quadro normativo comune alla luce del quale i Paesi membri possano procedere all'armonizzazione del diritto penale nazionale e dei codici di rito in materia di reati commessi via *Internet*, è suddiviso in quattro capitoli (terminologia, misure da prendere a livello nazionale, cooperazione internazionale, clausole finali): in particolare, il primo consta del solo art. 1 che, in ossequio alla logica per la quale il modo più efficace di regolamentare la Rete potrebbe consistere nella previsione di regole giuridiche che ne informino gli aspetti tecnici, contiene la definizione di concetti basilari quali « *computer system* », « *computer data* », « *service provider* » e « *traffic data* ».

L'art. 1 lett. *a* ricomprende quindi nella definizione di « *computer system* » ogni dispositivo (« *device* ») o gruppo di dispositivi tra loro connessi che, in esecuzione di un programma, processino dati informatici: va detto che il termine « *device* » è di portata semantica amplissima e non limitata a soli oggetti fisici, ben potendo ricomprendere anche programmi informatici; ad ogni modo una sua definizione è ricavabile dall'art. 6 (« *Misuse of devices* ») della stessa Convenzione che, per l'appunto, ricomprende i « *computer programs* » tra i « *devices* » che possono essere utilizzati per gli scopi vietati dalla Convenzione: per comprendere la rilevanza di tale previsione si pensi al caso dei *malware*, espressione con la quale si fa generalmente riferimento a qualsiasi *software* creato con il solo scopo di causare danni più o meno gravi ad un *computer* o un sistema informatico su cui viene eseguito e tra i quali rientrano i più famosi *virus*.

La categoria dei « *computer data* » è poi definita dalla successiva lett. *b* dell'art. 1, come ogni fatto, informazione o concetto che assuma una forma idonea ad essere processata da un *computer*; anche quest'ultima categoria è ritenuta comprensiva dei programmi, complessi di comandi che istruiscono un *computer* a svolgere una determinata operazione.

Passando ai profili soggettivi la successiva lett. *c* definisce poi il « *service provider* » come qualsiasi soggetto pubblico o privato che metta a disposizione dei suoi utenti gli strumenti necessari a comunicare per il tramite di un sistema informatico, nonché qualunque altro soggetto che esegua, per conto del primo o dei suoi utenti, attività di trattamento o archiviazione di dati informatici.

La lett. *d*, infine, provvede a definire un concetto particolarmente importante per la gestione della Rete, quello di « *traffic data* », quei dati informatici intrinsecamente relativi al solo traffico, per il cui tramite è possibile individuare l'origine, la destinazione, il percorso, le dimensioni e la durata di una comunicazione informatica, nonché il momento in cui essa è avvenuta.

Queste norme definitorie rappresentano il perno del sistema della Convenzione e uno degli snodi principali della disciplina internazionalistica della Rete: esse, infatti, provvedono a fissare, in maniera vincolante e, soprattutto, condivisa, profili tecnici generali in un contesto complesso e fluido quale quello in esame, in cui si è lamentata spesso proprio l'assenza di definizioni. Peraltro queste disposizioni, rappresentando le uniche norme comuni di definizione di categorie veramente basilari per il funzionamento della Rete, potrebbero riverberare i propri effetti anche al di fuori del sistema della Convenzione contribuendo così, assieme agli elementi di *soft law* che esamineremo nel paragrafo che segue, a creare un quadro giuridico di diritto internazionale sulla *governance* della Rete.

I successivi tre capitoli della Convenzione contengono, poi, rispettivamente, una serie di previsioni volte a imporre agli Stati membri l'inserimento, nei propri ordinamenti nazionali, di specifiche norme di diritto penale sostanziale (capitolo

II, sez. I: art. da 2 a 13) — tra le quali i reati di accesso senza legittimazione ai sistemi informatici, di attentato all'integrità di dati e sistemi, di falsificazione e frode, nonché i reati collegati alla pornografia minorile e alla violazione di diritti di proprietà intellettuale — e norme di natura processuale relative al perseguimento dei reati così introdotti (capitolo II, sez. II: art. da 14 a 22) (39), e al rafforzamento degli strumenti di cooperazione internazionale in materia (capitolo III: art. da 23 a 35). Chiudono il testo della Convenzione le disposizioni finali relative a firma, ratifica, entrata in vigore, modalità di adesione, ambito territoriale di applicazione e strumenti di soluzione delle controversie sull'applicazione e l'interpretazione della Convezione medesima (capitolo IV: art. da 36 a 48).

Il quadro del diritto internazionale pattizio concepito per *Internet* è completato dalle *International Telecommunication Regulations* (ITRs) dell'ITU, un trattato internazionale firmato il 9 dicembre 1988 a Melbourne, entrato in vigore il 1° luglio 1990, e sottoposto a revisione nel corso della *World Conference on International Telecommunications* 2012 (WCIT-12) svoltasi a Dubai dal 3 al 14 dicembre 2012 e conclusasi con l'adozione dei *Final Acts*.

Le ITRs, sebbene originariamente concepite in un contesto precedente alla diffusione massiccia di *Internet*, hanno comunque costituito il principale strumento internazionale di regolamentazione dell'interconnessione tra le diverse reti nazionali di telecomunicazioni, rendendo così possibile quella precondizione indispensabile per la nascita e lo sviluppo di *Internet* che è l'esistenza di una rete "globale" di telecomunicazioni: i meccanismi normativi previsti dalle ITRs hanno infatti predisposto per gli operatori di telecomunicazioni un quadro di riferimento globale idoneo a garantirne l'interoperabilità.

Le ITRs del 1988 erano fondate sul principio « *sending network pays* » (« chi trasmette paga »), in base al quale il gestore della rete nazionale che affida determinati dati ad un'altra rete per la loro consegna al destinatario è tenuto a pagare un *fee* (il quale può essere corrisposto *una tantum* oppure in relazione allo specifico traffico), principio che non è mai stato applicato sul *web*, in cui non sono previsti costi di interlacciamento tra i vari operatori di telecomunicazioni.

L'estensione di tale principio a *Internet* era uno dei nodi principali del negoziato del 2012, chiusosi senza il raggiungimento del *consensus* a causa dello scontro irrisolto tra la *lobby* degli operatori di telecomunicazioni, proprietari delle infrastrutture sulle quali viaggiano i dati, che spingeva perché i centoquarantaquattro governi riuniti a Dubai estendessero anche al *web* il principio in parola, e le imprese di *Internet*, soprattutto le cosiddette *over-the-top* (Google, Microsoft, Facebook, ecc.), che vi si opponevano strenuamente.

Oggetto più ambizioso della WCIT-12 era però il tentativo di revisione complessiva della *governance* del *web* come da noi illustrata: in particolare Cina e Russia, assieme a molti Paesi del Medio Oriente, avrebbero voluto affidarne la gestione a un'organizzazione internazionale di stampo classico come le Nazioni Unite o un suo Istituto specializzato, al fine di aumentarvi la rilevanza dei Governi. Tale posizione, frutto di una dichiarata diffidenza verso l'ICANN, cui questi Paesi contestano da tempo un approccio eccessivamente filo-occidentale, surrettiziamente cercava però anche di introdurre norme idonee a conferire agli Stati maggiori poteri di controllo sulla Rete, fino ad oggi, come abbiamo visto, difficilmente praticabile.

Il testo delle ITRs 2012 uscito dal negoziato (40), che è stato firmato solo da ottantanove Paesi sui centoquarantaquattro partecipanti, risulta di impatto minore rispetto a quello proposto (41), pur accrescendo comunque il ruolo dei governi nazionali nella *governance* della Rete riconoscendo loro un ruolo paritario per assicurarne stabilità, sicurezza, continuità e futuro sviluppo (42): le ITRs 2012, infatti, all'art. 7 (« *Unsolicited bulk electronic communications* »), attribuiscono agli Stati il potere di adottare misure di contrasto alle comunicazioni elettroniche non richieste, le quali, oltre che un legittimo strumento di lotta al cosiddetto *spamming*, potrebbero costituire anche un potenziale titolo di censura di contenuti *on-line* eventualmente sgraditi al potere politico in carica.

5. *Gli atti di* soft law *adottati dalle organizzazioni internazionali: la Dichiarazione di Ginevra del*

(39) Per un'analisi di alcune di queste norme v. RUOTOLO, Hey! You! Get Off My Cloud! *Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Arch. pen.*, 2013, 785.

(40) *Final Acts of the World Conference on International Telecommunications*, Dubai, 14 dicembre 2012, reperibile in www.itu.int. In dottrina v. ODDENINO, *Diritti individuali, sicurezza informatica e accesso alla conoscenza in rete: la revisione delle International Telecommunication Regulations dell'ITU*, in *Dir. umani e dir. intern.*, 2013, 532 ss.

(41) Per un'analisi delle proposte emerse nel corso del negoziato v. RUOTOLO, *op. cit.*, 109 ss.

(42) Cfr. FIDLER, *op. cit.*, 4.

*2003, l'Impegno e l'Agenda di Tunisi del 2005. L'*Internet Governance Forum *(IGF). Gli atti adottati dal Consiglio economico e sociale e dall'Assemblea generale delle Nazioni Unite.* — Abbiamo già accennato a come numerosi atti non vincolanti siano stati emanati da parte di varie organizzazioni internazionali con riguardo agli aspetti più disparati della gestione di *Internet*, dalla sua *governance* vera e propria, oggetto di numerose risoluzioni adottate soprattutto nell'ambito delle Nazioni Unite, ad aspetti più di dettaglio o relativi a settori e comportamenti specifici, sui quali ci limiteremo ad alcuni cenni.

In un settore come quello in esame è, infatti, comprensibile che previsioni normative "flessibili", quali quelle che stiamo per esaminare, siano state utilizzate più di frequente rispetto a strumenti vincolanti, non tanto perché meno invasive delle prerogative sovrane degli Stati quanto, piuttosto, perché ritenute idonee ad avviare processi di produzione normativa che consentono, dopo le prime applicazioni, rapide modifiche della disciplina già suggerita; per altro verso le procedure adottate per la redazione di strumenti siffatti contemplano di frequente il coinvolgimento di attori diversi dagli Stati, i quali, in una visione, per così dire, classica, sarebbero invece gli unici legittimati a prendere parte a pieno titolo sia alla fase ascendente — di adozione — che a quella discendente — di applicazione — di norme di diritto internazionale vincolante.

Con riguardo alla *governance* del *web* si assiste così al diffuso uso di strumenti di *soft law* per la fissazione, da un lato, di principi generali di tipo materiale e, dall'altro, di norme di contenuto procedimentale volte a disciplinare le modalità di discussione dei detti principi e ad individuare i soggetti legittimati a prendere parte al dibattito (43).

In particolare la già citata Dichiarazione *Building the Information Society: A Global Challenge In The New Millennium* del 2003 (44) contiene un elenco dei principi cui, secondo i centosettantacinque Paesi partecipanti al *Summit*, la *governance* di *Internet* dovrebbe ispirarsi: vi si dice che essa, in particolare, dovrebbe rispettare l'approccio multilaterale e garantire la trasparenza, nel rispetto del principio democratico e dei diritti fondamentali, al fine di consentire l'accesso diffuso alle informazioni e alla conoscenza del maggior numero possibile di persone; nel contempo gli Stati sono esortati a prevedere meccanismi che impediscano la commissione di comportamenti pericolosi per gli utenti e a garantire la sicurezza e la stabilità del *web*.

Anche il *Tunis Commitment* (45), adottato il 18 novembre 2005 a conclusione della seconda fase del *Summit*, afferma l'impegno dei partecipanti (i quali, significativamente, nel preambolo dell'atto, si definiscono « *representatives of the peoples of the world* ») a costruire una società dell'informazione incentrata sulla persona, inclusiva e orientata allo sviluppo, nel rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale, in particolare delle norme che tutelano i diritti fondamentali, di cui l'Impegno ribadisce universalità, indivisibilità, interdipendenza e interrelazione: il *Tunis Commitment* esplicita così la correlazione tra una corretta amministrazione della società dell'informazione, e quindi del *web*, e il diritto allo sviluppo, riconoscendo, al § 10, come l'accesso all'informazione e la creazione e condivisione della conoscenza contribuiscano in maniera significativa al rafforzamento dello sviluppo economico, sociale e culturale, e possano rappresentare un ulteriore strumento per il raggiungimento degli obiettivi di sviluppo concordati internazionalmente.

Pure l'*Agenda* di Tunisi (46), adottata contestualmente al *Commitment*, prevede che la gestione della Rete debba essere concordata, all'interno dell'*Internet Governance Forum* (IGF) che viene a tal fine istituito, in un contesto di "cooperazione rafforzata" e debba essere soggetta a costanti revisioni periodiche, così da tenere sempre in considerazione gli inarrestabili mutamenti, tecnici e di contenuto, ai quali la Rete stessa va, per sua natura, soggetta.

Agli atti in parola, poi, deve aggiungersi la risoluzione approvata nel 2006 dal Consiglio economico e sociale delle Nazioni Unite (ECOSOC) che fissa i criteri secondo i quali monitorare il *follow-up* del WSIS: il Consiglio investe del compito di sorvegliare l'implementazione dei risultati del WSIS la *Commission on Science and Technology for Development* (CSTD) dell'ITU (47), che è invitata a

(43) Atti siffatti, che rientrano nel cosiddetto *soft law*, peraltro sono dotati di caratteristiche differenti e, di conseguenza, sono idonei a produrre effetti giuridici diversi: si pensi, a mero titolo di esempio, alle differenze intercorrenti tra le raccomandazioni, idonee a produrre il noto effetto di liceità, e le norme programmatiche, che sono utilizzabili come parametro di legittimità delle disposizioni che le attuano.

(44) Doc. WSIS-03/GENEVA/DOC/4-E, cit.

(45) Doc. WSIS-05/TUNIS/DOC/7-E, cit.

(46) *Tunis Agenda for the Information Society*, 18 novembre 2005, doc. WSIS-05/TUNIS/DOC/6(Rev. 1)-E, reperibile in www.itu.int.

(47) Risoluzione 28 luglio 2006, n. 2006/46, *Follow-up*

tenere in considerazione le esigenze dello sviluppo e a rispettare l'approccio *multistakeholder* della Rete (48).

Anche l'Assemblea generale è intervenuta nel dibattito adottando a partire dal 2002 una serie di risoluzioni relative agli « Sviluppi nel campo dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale », in cui si afferma ripetutamente la centralità delle tecnologie dell'informazione, le quali « *affect the interests of the entire international community* » (49). Nel corso della 64ª e della 65ª sessione, l'Assemblea generale ha poi adottato una coppia di risoluzioni dal medesimo titolo — « Tecnologie dell'informazione e della comunicazione per lo sviluppo » (50) — in cui, dopo aver significativamente ribadito l'indissolubile collegamento esistente tra tecnologie e scienze dell'informazione e diritto allo sviluppo e riaffermato la perdurante centralità degli Stati nei processi di gestione di *Internet*, ha altresì sottolineato l'importanza del coinvolgimento dei soggetti non statali nei vari *fora* negoziali.

In maniera non dissimile da quanto già affermato in sede WSIS, il procedimento per la redazione delle norme di gestione del *web*, nella visione dell'Assemblea generale, è quindi di natura complessa e composita, e, per questo, suddiviso in due distinti momenti, tra loro complementari: il primo, di ampio coinvolgimento sotto il profilo soggettivo, è volto ad acquisire le opinioni e gli interessi finanche di enti tradizionalmente estranei al novero dei soggetti di diritto internazionale, quali organizzazioni non governative, società multinazionali, comunità accademiche e così via; il secondo, di tipo più classico e che per la sua natura non può che coinvolgere esclusivamente Stati ed organizzazioni internazionali, si sostanzia in un negoziato intergovernativo, volto in primo luogo a precisare la portata del principio cooperativo mediante l'assunzione di obblighi di informazione e consultazione.

Gli strumenti esaminati, nel loro complesso, ci confermano l'esistenza dell'interesse di tutti gli attori di *Internet* — ivi compresi i soggetti di diritto internazionale — a una gestione comune della stessa, conseguenza ineludibile della sua natura indivisibile: a questi elementi complessivamente intesi è possibile attribuire una forma normativa che coincide col principio procedurale di cooperazione contenuto nell'*Agenda* di Tunisi; tutte le caratteristiche della Rete sin qui individuate ci consentono di individuare, come vedremo immediatamente, un regime normativo di diritto internazionale per la sua *governance*.

6. *L'applicazione a* Internet *di norme di diritto internazionale generale a essa preesistenti: il* web *come patrimonio comune dell'umanità e il relativo regime.* — Le caratteristiche generali di *Internet* che abbiamo individuato (indivisibilità, esauribilità, interesse comune degli Stati al suo efficace funzionamento) rievocano quelle possedute da altri beni il cui pieno sfruttamento, al pari della Rete, presuppone da parte degli Stati il possesso di elevate competenze tecnologiche.

Beni con caratteristiche siffatte sono stati spesso ritenuti patrimonio comune dell'umanità (51).

Come noto, definire un bene patrimonio comune dell'umanità è un'operazione che, lungi dall'essere meramente descrittiva, ha valenza normativa, nel senso che a tale oggetto, in conseguenza della qualificazione fattane, sarà applicabile il relativo regime di diritto internazionale; la categoria in parola, già nota al diritto internazionale classico, vide una riattualizzazione in occasione della Terza conferenza delle Nazioni Unite sul diritto del mare, aperta nel 1973 e conclusasi a Montego Bay il 10 dicembre 1982, e venne inserita dapprima nella risoluzione dell'Assemblea generale del 17 dicembre 1970, n. A/RES/2749 (XXV) (52) — secondo la quale l'Area dei fondi marini e degli oceani e il loro sottosuolo, che si trovano oltre i

to the World Summit on the Information Society and review of the Commission on Science and Technology for Development, in www.un.org.

(48) La Commissione è invitata a « *ensure the meaningful and effective participation, including by providing assistance on a voluntary basis, of all stakeholders from developing countries, including nongovernmental organizations, small and medium-sized enterprises, industry associations and development actors* », § 16 della risoluzione, cit.

(49) Cfr. risoluzioni 22 novembre 2002, n. A/RES/57/53; 8 dicembre 2003, n. A/RES/58/32; 3 dicembre 2004, n. A/RES/59/61; 8 dicembre 2005, n. A/RES/60/45; e 6 dicembre 2006, n. A/RES/61/54.

(50) Risoluzioni 21 dicembre 2009, n. A/RES/64/187 (documento reso pubblico il 9 febbraio 2010) e 20 dicembre 2010, n. A/RES/65/141.

(51) Sulla categoria v. KISS, *La notion de patrimoine commun de l'humanité,* in *Recueil des Cours de l'Académie de droit international de la Haye*, CLXXV, 1982, 99 ss., nonché BASLAR, *The Concept of the Common Heritage of Mankind in International Law*, The Hague, 1998; WOLFRUM, *The Principle of Common Heritage of Mankind*, in *Z. aus. öff. R.VR.*, 1983, 312 ss. e, da ult., SCISO, *Appunti di diritto internazionale dell'economia*, Torino, 2012, 33 ss.

(52) Dichiarazione sui principi che disciplinano i fondi marini e il loro sottosuolo di là dei confini delle giurisdizioni nazionali, in www.un.org.

limiti delle giurisdizioni nazionali, così come le loro risorse, sono patrimonio comune dell'umanità e, pertanto, la loro esplorazione e il loro sfruttamento vanno condotti a beneficio di tutta l'umanità — e successivamente nella Parte XI della Convenzione delle Nazioni Unite sul diritto del mare del 10 dicembre 1982, relativa proprio alla detta Area (53). Un concetto analogo, anche se dai confini ancora sfumati, era già apparso nel Trattato sull'Antartide, firmato a Washington il 1° dicembre 1959 (54), e in una Dichiarazione dell'Assemblea generale delle Nazioni Unite relativa ai principi giuridici governanti le attività degli Stati nell'esplorazione e nell'uso dello spazio esterno, adottata il 13 dicembre 1963, la quale fa riferimento agli « interessi comuni dell'umanità » nell'esplorazione del cosmo e indica che « ogni Stato ha assoluta libertà di movimento, e nessuno può dichiarare la propria sovranità su parti di esso » (55), nonché, ancora, nel successivo Trattato del 27 gennaio 1967 relativo alle attività degli Stati nell'esplorazione e utilizzazione dello spazio (56).

Pure il Trattato relativo alle attività degli Stati sulla Luna e gli altri corpi celesti del 1979 (57) all'art. 11 provvede a definire patrimonio comune dell'umanità la Luna e le sue risorse naturali. Ulteriori e più recenti applicazioni del concetto sono poi contenute nella Convenzione UNESCO del 16 novembre 1972 sui beni culturali e nazionali di eccezionale valore (58) nonché nella Dichiarazione universale sul genoma umano adottata, ancora dall'UNESCO, l'11 novembre 1997 (59), secondo la quale esso non può essere oggetto di appropriazione da parte di Stati o di privati.

Quest'ultima dichiarazione, in particolare, evidenzia l'estrema duttilità della categoria, utilizzabile per la tutela di beni tra loro anche molto diversi per caratteristiche e funzioni: la categoria di bene patrimonio comune dell'umanità appare essersi quindi progressivamente ampliata, specie in conseguenza del progresso tecnologico, passando così a ricomprendere oggetti anche molto distanti da quelli per i quali il regime era originariamente applicabile (60).

Gli elementi comuni a tutte le norme che disciplinano l'uso di beni rientranti nella categoria in esame tracciano un regime di diritto internazionale generale volto a limitare la libertà di sfruttamento degli Stati mediante quattro distinte restrizioni: *a*) il divieto di estensione della sovranità nazionale ai beni ritenuti patrimonio comune e, in particolare, quello della loro appropriazione unilaterale da parte di singoli Stati (principio di non appropriazione); *b*) l'obbligo di assoggettamento dei beni in questione a un regime internazionale di cooperazione per quanto concerne la loro gestione; *c*) il divieto della loro utilizzazione, anche per interessi generali, con modalità tali da arrecare pregiudizio irreparabile 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 dei principi contenuti nella Carta delle Nazioni Unite relativi al mantenimento della pace e della sicurezza internazionale.

Internet possiede i caratteri per rientrare nella famiglia dei beni cui è applicabile il regime normativo appena descritto (61): la Rete, infatti, rappresenta una risorsa indivisibile, dal momento che mantiene la sua capacità di mezzo di comunicazione di incommensurabile potenza tale solo se non viene frammentata in una serie di sottoreti, ad esempio di portata nazionale, tra loro non comu-

(53) La Convenzione è reperibile in www.un.org. In dottrina v. *The International Legal Regime of Areas beyond National Jurisdiction* a cura di ELFERINK e MOLENAAR, Leiden, 2010; SCOVAZZI, *Fondi marini e patrimonio comune dell'umanità*, in *Riv. dir. intern.*, 1984, 249 ss.; TREVES, *Fondi marini internazionali*, in questa *Enciclopedia*, Aggiornamento, II, 1998, 347 ss.; VILLANI, *Il regime di sfruttamento dei fondi marini*, in *Prospettive del diritto del mare all'alba del XXI secolo* (Istituto Italo-latino americano), Roma, 1999, 149 ss., in particolare 162.

(54) Il Trattato è entrato in vigore nel 1961; il Segretariato del Trattato ha un suo sito *web* sul quale è possibile reperire il testo del Trattato medesimo e la relativa prassi: www.ats.aq.

(55) La Dichiarazione è reperibile in www.un.org.

(56) Il Trattato è reperibile in www.unoosa.org.

(57) Il Trattato, reperibile in www.unoosa.org, è stato adottato dall'Assemblea Generale con la risoluzione 5 dicembre 1979, n. A/RES/34/68, ed è entrato in vigore nel luglio 1984, quando ha raggiunto il numero minimo di ratifiche richieste.

(58) La Convenzione è reperibile in www.en.unesco.org.

(59) La Dichiarazione è reperibile in www.unesco.org.

(60) KUPPUSWAMY, *The International Legal Governance of the Human Genome*, London, 2012. V. anche MARCHISIO, *Patrimonio comune dell'umanità (Dir. internaz.)*, in *Il Diritto. Enciclopedia giuridica del Sole 24 ore*, X, Milano, 2007, 728 ss; ID., *L'ONU. Il diritto delle Nazioni Unite*, Bologna, 2012, 83 ss.; SPECTAR, *The fruit of the human genome tree: cautionary tales about technology, investment, and the heritage of humankind*, in *Loyola of Los Angeles International & Comparative Law Review*, 2001, 1 ss.

(61) Su *Internet* come patrimonio comune dell'umanità cfr. SEGURA SERRANO, *Internet Regulation and the Role of International Law*, cit., 231 ss.; SPANG-HANSSEN, *Public International Computer Network Law Issues*, Copenhagen, 2006. V. anche MALCOLM, *The Space Law Analogy to Internet Governance*, in *Journal of Law, Information and Science*, 2007, 57 ss.

nicanti, ed esauribile (si pensi, ad esempio, alla questione della finitezza del numero degli indirizzi IP, di cui si è già detto *supra*, § 3): e in merito all'opportunità della loro conservazione, di interesse comune, abbiamo già individuato numerose prese di posizione, da parte di Stati e di svariate organizzazioni internazionali. La prassi fin qui esaminata, infatti, evidenzia la riconosciuta importanza globale del bene in questione e la consapevolezza dei membri della Comunità internazionale dell'esistenza di un interesse "collettivo" al mantenimento delle sue piene funzionalità; peraltro gli atti adottati in seno a svariate organizzazioni internazionali, come abbiamo visto nel paragrafo precedente, esplicitano l'esistenza di *consensus* in merito all'opportunità di fare in modo che il governo della Rete sia oggetto di condivisione da parte di tutti i soggetti interessati, pubblici e privati.

Esplicito sul punto è lo studio preparatorio predisposto dal Presidente del Gruppo di esperti dell'ITU (*International Telecommunication Union*) in vista del XII Congresso delle Nazioni Unite sulla prevenzione dei crimini e la giustizia penale svoltosi in Brasile dal 12 al 19 aprile 2010, che individua nel cyberspazio il quinto spazio comune, dopo la terra, il mare, l'aria e gli spazi extra-atmosferici (62).

A nostro parere il diritto internazionale generale, quindi, impone agli Stati di rispettare, con riguardo alla Rete, gli obblighi previsti per i beni patrimonio comune dell'umanità: più in dettaglio l'applicazione a *Internet* del principio di non appropriazione, come già avviene per gli altri spazi comuni quali l'alto mare o gli spazi extra-atmosferici, vieta ad ogni Stato di trattare la Rete — e quindi anche le parti di essa che, fisicamente, sono collocate in zone sottoposte alla sua sovranità — come se fosse sotto la sua esclusiva giurisdizione e, quindi, di porvi in essere comportamenti che impediscano del tutto o in parte agli altri Stati di utilizzarla o di limitare la loro discrezionalità in merito al suo uso. Questo, con particolare riguardo alla gestione del sistema DNS di cui abbiamo già detto *supra*, § 3, suggerisce l'esistenza di un divieto, in capo a tutti gli Stati, e quindi anche agli USA, lo Stato gestore del sistema, a porre in essere qualunque azione o comportamento idonei a mettere in pericolo l'efficienza del sistema DNS e, per il suo tramite, l'esistenza del *web* tutto.

L'obbligo di cooperazione — che, nel caso di specie, assume la triplice forma di un obbligo di informazione, consultazione e *de negotiando* — poi 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 il *consensus* in merito alle misure di disciplina e di uso del bene comune.

Il divieto di inquinamento va fatto oggetto, più degli altri, di un'interpretazione che consenta di tener conto delle peculiarità del fenomeno di *Internet*: se per inquinamento si intende l'irreversibile alterazione peggiorativa di un ambiente per il tramite di fattori patogeni, nel caso di *Internet* si deve pensare all'inquinamento "virtuale" dell'ambiente informatico, in particolare a quello posto in essere mediante *software* malevolo; il divieto in questione, peraltro, ci pare vada 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 l'obbligo gravante sugli stessi di porre in essere misure preventive e repressive per evitare che i medesimi strumenti siano disseminati in Rete da privati. Va anche chiarito che il divieto in parola non è applicabile a ogni comportamento statale che implichi la progettazione e/o consenta la diffusione via *web* di ogni strumento informatico malevolo, ma solo, e più limitatamente, di quelli dotati di offensività tale da mettere in pericolo o 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*).

7. (Segue): Internet *e il divieto dell'uso della forza.* — Discorso specifico, poi, deve essere condotto con riguardo alla possibilità che uno Stato utilizzi determinati strumenti informatici come mezzo di attacco armato ad altri Stati: l'uso di strumenti così congegnati, infatti, appare proibito dalle norme sul divieto della minaccia e l'uso della forza, le quali, applicate ad *Internet*, ne vietano l'uso come mezzo di attacco; il tema, peraltro, come vedremo più avanti, si interseca con quello delle possibili legittime reazioni statali nei confronti degli attacchi, nonché con quello del *cyber* terrorismo.

Con l'espressione *cyberwarfare* (o *cyber* guerra) si fa, infatti, ormai comunemente riferimento all'uso di strumenti informatici da parte di uno Stato con l'intento di ledere altri soggetti di diritto internazionale analogamente a quanto avviene nel caso di una guerra tradizionale, cioè col fine di

(62) *A Cyberspace Treaty - A United Nations Convention or Protocol on Cybersecurity and Cybercrime*, Background paper doc. A/CONF.213/IE/7, 23 marzo 2010.

causare « *injury or death to persons and damage or destruction to objects* » (63).

Tra i comportamenti materiali che potrebbero rientrare nella definizione di *cyber* guerra possiamo annoverare il caso di un attacco informatico che riesca a bloccare il sistema dell'aviazione militare di un Paese, impedendone un intervento tempestivo, o che interrompa l'erogazione di corrente da parte delle centrali elettriche e di *backup* di un ospedale, causando così la perdita di vite umane. Purtroppo non si tratta di mere ipotesi di scuola, come dimostra la prassi recente relativa al caso del *malware* denominato *Conficker*, in grado di infettare, bloccandone molte funzioni, i sistemi operativi Microsoft: il sistema informatico della Marina militare francese ne fu colpito agli inizi del 2009 e l'infezione costrinse diversi aerei a restare a terra a causa delle difficoltà di caricare sui *computer* di bordo i piani di volo; anche il Ministero della difesa del Regno Unito riferì di infezioni ai propri sistemi, ed in particolare al *software* caricato sulle navi e sui sottomarini della Marina reale; problemi analoghi furono accusati anche dal *Bundeswehr*, la Difesa federale della Germania, che comunicò il 2 febbraio del 2009 una diffusa infezione ai propri *computer*. E attacchi, con conseguenti, anche se minori, crisi di funzionalità, furono riportati, nel Regno Unito, da un ospedale della città di Sheffield, dalla Municipalità e dalla polizia di Manchester e dalla *House of Commons* (64).

Ancora più interessante, poi, è il caso di *Stuxnet*, un *worm* capace di riprogrammare *computer* industriali prodotti dalla tedesca Siemens, isolato nel giugno del 2010, e che ha infettato i *computer* localizzati nell'impianto nucleare iraniano di Bushehr (65), col conseguente rischio di surriscaldamento della centrifuga e di un incidente nucleare di proporzioni devastanti.

Cerchiamo di comprendere se i comportamenti appena descritti, qualora fossero imputabili a degli Stati, possano rientrare tra quelli vietati dal diritto internazionale in quanto forme di minaccia o di uso della forza nelle relazioni internazionali.

Ricordiamo che, come noto, l'interpretazione maggioritaria dell'art. 2 § 4 della Carta delle Nazioni Unite, nonché della corrispondente norma di diritto internazionale generale, ritiene che il divieto della minaccia e dell'uso della forza ivi previsto sia relativo esclusivamente alla forza militare, rientrando altre forme di coercizione e segnatamente quelle non militari nell'ambito di applicazione del principio di non ingerenza (66).

Il divieto in questione potrebbe essere però oggetto di un'interpretazione evolutiva che includa anche i comportamenti appena descritti, o almeno alcuni di essi: la Corte internazionale di giustizia, nel noto caso delle « Attività militari e paramilitari in Nicaragua », ha fatto rientrare nel divieto stesso anche attività non 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 un altro Stato (67) e, soprattutto, nel parere del 1996 relativo alla « Legittimità della minaccia e dell'uso delle armi nucleari » ha chiarito come il sistema della Carta non contenga alcuna definizione o elencazione del concetto di « arma » rispetto al divieto dell'uso della forza (68).

Sulla base di questi elementi una parte della dottrina ha avanzato l'ipotesi di poter considerare almeno alcuni strumenti informatici alla stregua delle armi tradizionali e, di conseguenza, ritenere il loro uso vietato dal diritto internazionale, ap-

(63) Cfr. al riguardo la *Rule* 30 del "*Tallinn Manual*": *Tallinn Manual on the International Law Applicable to Cyber Warfare* a cura di Schmitt, Cambridge, 2013, 91, reperibile in www.ccdcoe.org. Il Manuale di Tallinn è un lungo rapporto stilato da un gruppo indipendente di esperti su invito del *Nato Cooperative Cyber Defence Centre of Excellence* di Tallinn, appunto, al fine di effettuare una codificazione in 95 *Rules* del diritto internazionale applicabile a queste nuove forme di guerra, con riguardo sia al *ius ad bellum*, le norme internazionali che disciplinano il ricorso alla "forza informatica" da parte degli Stati, sia al *ius in bello*, il diritto internazionale che regola la condotta degli Stati nei conflitti informatici.

(64) Markoff, *Worm Infects Millions of Computers Worldwide*, in *New York Times*, www.nytimes.com, 22 gennaio 2009.

(65) Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, reperibile in www.ssrn.org; Tappero Merlo, *Soggetti e ambiti della minaccia cibernetica: dal sistema-Paese alle proposte di* Cyber Governance*?*, in *Comun. intern.*, 2012, 25 ss.

(66) Gargiulo, *Uso della forza (diritto internazionale)*, in questa *Enciclopedia*, Annali, V, 2012, 1367 ss., in particolare 1384 ss. e la bibliografia ivi citata.

(67) I.C.J. 27 giugno 1986, Attività militari e paramilitari in Nicaragua (Nicaragua *v*. United States of America), in *I.C.J. Reports*, 1986, 14 ss., § 36. In dottrina v. Boothby, *Weapons and the Law of Armed Conflicts*, Oxford-New York, 2009; Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge, 2012, 65 ss. Discorso a parte andrebbe poi svolto per le armi di tipo tradizionale ma gestite a distanza per il tramite di strumenti informatici, i cosiddetti droni, su cui v. Herbach, *Into the Caves of Steel: Precaution, Cognition and Robotic Weapon Systems Under the International Law of Armed Conflict*, in *Amsterdam Law Forum*, 2012, 3 ss.; Thurner, *The Law that Applies to Autonomous Weapon Systems*, in *American Society of International Law Insights*, www.asil.org, gennaio 2013.

(68) I.C.J., *Advisory Opinion*, 8 luglio 1996, Legality of the Threat or Use of Nuclear Weapons, in *I.C.J. Reports*, 1996, 226 ss., § 52 (www.icj-cij.org).

puntando l'attenzione non già sulla modalità di realizzazione dell'attacco quanto sugli effetti da questo prodotti, i quali, per essere paragonabili a quelli di un attacco armato di stampo classico, con la conseguente estensione della relativa disciplina giuridica, devono essere idonei a causare la distruzione di beni e la perdita di vite umane (69).

Per questo non tutti gli attacchi informatici compiuti da uno Stato nei confronti di un altro, per quanto su larga scala, possono ritenersi *sic et simpliciter* vietati sulla base delle norme sull'uso della forza: al riguardo la dottrina ha 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 » (70).

Gli attacchi informatici che non raggiungono una tale soglia di aggressività ci pare siano comunque 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 non comportino 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 del 1970 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 » (71).

Questione altrettanto complessa e delicata, poi, è quella che riguarda la possibilità di una reazione in legittima difesa a un attacco informatico: l'ordinamento internazionale, come noto, distingue le violazioni *minoris generis* del divieto dell'uso della forza da quelle, particolarmente qualificate, che si sostanziano in un attacco armato (72) e consente solo in quest'ultimo caso, come chiarito dalla Corte internazionale di giustizia nel caso delle « Attività militari e paramilitari in Nicaragua » (73), una reazione armata in legittima difesa. L'attenzione, allora, va spostata sui mezzi che possono essere legittimamente utilizzati dallo Stato che reagisce a un attacco informatico, e, in particolare, se essi possano assumere esclusivamente la medesima forma dell'attacco subito, e cioè possano essere esclusivamente informatici, o possano anche sostanziarsi in misure belliche di tipo tradizionale (74).

La soluzione ci pare vada individuata alla luce del principio di proporzionalità, il quale consentirebbe di ritenere legittima anche una reazione armata tradizionale dello Stato che stia subendo un attacco informatico su larga scala che abbia prodotto danni paragonabili a quelli di un attacco militare classico; ovviamente la reazione deve essere comunque posta in essere nel rispetto del diritto internazionale cogente e del diritto internazionale umanitario (75).

In questo senso vanno alcuni elementi della prassi recente: il rapporto del 2011 sulla *cybersecurity* della Casa Bianca dichiara esplicitamente che gli Stati Uniti si ritengono autorizzati a reagire con l'uso della forza militare contro attacchi informatici particolarmente virulenti (76); secondo tale

(69) 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 Reserve Journal of International Law*, 1998, 567 ss.; 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. Sul punto v. anche Beard, *Law and War in the Virtual Era*, in *Am. journ. intern. Law*, 2009, 1 ss. e Harrison Dinniss, *lc. cit.*

(70) Ronzitti, *Introduzione al diritto internazionale*[4], Torino, 2013, 418.

(71) Risoluzione dell'Assemblea generale delle Nazioni Unite del 24 ottobre 1970, n. A/RES/2625 (XXV), in www.un.org.

(72) Nel medesimo senso anche I.C.J. 6 novembre 2003, relativa al caso Oil Platforms (Islamic Republic of Iran v. United States of America), in *I.C.J. Reports*, 2003, 161; 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.

(73) I.C.J. 27 giugno 1986, cit.

(74) Harrison Dinniss, *op. cit.*, 75 ss.

(75) Specificamente sul tema 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.; Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal of International Law*, 2011, 421 ss.

(76) Cfr. doc. *International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World*, maggio 2011, consultabile nel sito www.whitehouse.gov, dove si afferma che « *the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law, in order to defend our Nation, our allies,*

rapporto, la reazione potrebbe comportare sia l'uso di mezzi elettronici sia opzioni militari convenzionali. Anche la prassi che si è sviluppata in seno all'Organizzazione del Trattato dell'Atlantico del Nord (NATO) in occasione dei ripetuti attacchi subiti nel 2007 da numerosi siti governativi, di banche ed importanti imprese estoni, partiti da indirizzi IP situati in Russia, alcuni dei quali riconducibili direttamente al governo e ai servizi di sicurezza russi, si limita solo a escludere l'applicazione automatica agli attacchi informatici delle disposizioni sulla legittima difesa collettiva contenute nel Trattato NATO, ma non la possibilità di una reazione militare ad attacchi siffatti (77).

Passando ora al *cyber* terrorismo, la dottrina che se ne è occupata, nell'assenza di una definizione generalmente accettata del fenomeno, anche di stampo tradizionale, ha spesso ritenuto tale la commissione di « *ordinary computer crimes but with the added intention to instill fear among a target audience* » (78).

Nell'assenza di prassi significativa specificamente relativa al *cyber* terrorismo, per tentarne una definizione alla luce dell'ordinamento internazionale (79), riteniamo di dover prendere le mosse dal terrorismo tradizionale (80), visti gli indubbi punti di contatto tra le due fattispecie: in particolare nella prassi degli ultimi dieci anni, si è assistito a importanti sviluppi i quali, pur nella perdurante assenza di una definizione che sia generalmente condivisa da 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 né con la sua protezione, i quali pongano in essere atti di indiscriminata violenza diretti sia contro obiettivi civili sia contro obiettivi militari/governativi che cagionino la perdita di vite umane e/o la distruzione di beni materiali; per rientrare nella categoria è altresì necessario che il comportamento materiale così individuato sia caratterizzato da intenti di destabilizzazione. Sono quindi esclusi da una siffatta definizione sia il terrorismo di Stato, che va ricondotto alla violazione di altri obblighi di diritto internazionale e segnatamente del divieto generalizzato dell'uso della forza, sia, per motivi sostanzialmente analoghi, quello sponsorizzato da Stati.

Su queste basi ci pare di poter ritenere che una definizione di *cyber* terrorismo che sia contemporaneamente compatibile con quella di terrorismo "generico" e con quella di *cyberwarfare* dovrebbe essere tale da ricomprendere tutte le attività idonee a cagionare la perdita di vite umane e/o la distruzione di beni materiali, poste in essere da privati mediante strumenti informatici, indipendentemente dal loro *target* (civile o militare): ciò avrebbe anche l'indubbio vantaggio di far coincidere i comportamenti materiali che caratterizzano sia il *cyber* terrorismo sia la *cyber* guerra, che si distinguerebbero tra loro esclusivamente sulla base della natura dell'aggressore (organizzazione di individui nel primo caso, di Stato nel secondo) e dell'obiettivo che i loro autori si prefiggono (sovvertimento dell'ordine costituito nel primo, *debellatio* del nemico nel secondo).

8. *L'accesso a* Internet *come mezzo di tutela dei diritti fondamentali e come diritto fondamentale autonomo.* — L'accesso a *Internet* costituisce certamente un mezzo di attuazione di molti diritti fondamentali già garantiti a vario titolo dall'ordinamento internazionale, come il diritto a una libera espressione, i diritti di informazione e, come abbiamo già visto, il diritto allo sviluppo; d'altro canto, quello di accedere liberamente e senza limitazioni illegittime alla Rete potrebbe assumere i connotati di un autonomo diritto fondamentale di ultima generazione (81).

Con riguardo al primo profilo ricordiamo che

---

our partners, and our interests »; v. anche il rapporto del Servizio di ricerca del Congresso statunitense, del 3 luglio 2012, intitolato *Cybersecurity: Authoritative Reports and Resources*, reso pubblico sul sito dell'organizzazione non governativa *Federation of American Scientists* (FAS), www.fas.org.

(77) « *Collective self-defence, will not* automatically *be extended to the attacked Country* ».

(78) Cfr. GARRETT e CLARKE, *Cyberterrorism: A New Challenge for International Law*, in *Enforcing International Law Norms Against Terrorism* a cura di BIANCHI, Oxford-Portland (Oregon), 2004, 465 ss.

(79) DRAETTA, *The Internet and Terrorist Activities*, in *Enforcing International Law Norms Against Terrorism* a cura di BIANCHI, cit., 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 cyber crimes 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* » (ivi, 464).

(80) CHERUBINI, *Terrorismo (diritto internazionale)*, in questa *Enciclopedia*, Annali, V, 2012, 1213 ss.

(81) In generale sul tema v. PADOVANI, MUSIANI e PAVAN, *Diritti umani nell'età digitale: concetti in evoluzione e norme emergenti nel contesto trans-nazionale*, in *Pol. dir.*, fascicolo monografico su: *Diritti e sfera pubblica nell'era digitale*, 2010, 391 ss.

le *International Trade Regulations* dell'ITU, all'art. 3, prevedono esplicitamente il diritto di ogni utente connesso alla rete di telecomunicazioni di « inviare traffico », cioè di utilizzare la rete stessa per trasmettere informazioni; il diritto di accedere ai servizi internazionali di telecomunicazioni è riconosciuto anche nell'art. 33 (« *The Right of the Public to Use the International Telecommunication Service* ») della Costituzione ITU, la quale consente agli Stati di adottare limitazioni a tali servizi solo al fine di tutelare interessi di rilevanza superiore, come, ad esempio, la sicurezza nazionale.

Il diritto di utilizzare le reti internazionali di telecomunicazioni, quindi, costituisce una delle più efficaci forme di attuazione del diritto di formarsi un'opinione — consacrato, sul piano universale, dall'art. 19 comma 1 del Patto internazionale sui diritti civili e politici del 1966 (82) e, a livello regionale europeo, dall'art. 10 CEDU —, di esprimerla ed esprimersi, liberamente cercando, ricevendo e diffondendo attraverso qualsiasi mezzo informazioni e idee di ogni genere (art. 19 comma 2 del medesimo Patto, nonché, ancora, art. 10 CEDU) (83) o del diritto a partecipare alla vita culturale e godere dei benefici del progresso scientifico e delle sue applicazioni (art. 15 del Patto internazionale sui diritti economici, sociali e culturali del 16 dicembre 1966) (84).

Certamente, difatti, i diritti fondamentali appena elencati trovano applicazione anche sul *web*, come precisato dal Comitato per i diritti umani delle Nazioni Unite — organo che, come noto, ha il compito di monitorare l'esecuzione e il rispetto del Patto sui diritti civili e politici da parte dei suoi membri — in un *General comment* che chiarisce come il già citato art. 19 del Patto ONU II riguardi anche gli « *electronic and internet-based modes of expression* » (85).

L'Assemblea generale ha ribadito la rilevanza del *web* per il diritto allo sviluppo, ricordando che le tecnologie dell'informazione possono contribuire a favorire una crescita economica sostenibile ed inclusiva « *that will help to expedite the integration of all countries, especially developing countries, in particular the least developed countries, into the global economy* » (86); e, ricordiamo, proprio il diritto allo sviluppo era invocato nella Dichiarazione di Principi del WSIS addirittura come potenziale titolo di un diritto di accesso universale alle tecnologie dell'informazione (87), in particolare nell'ottica del raggiungimento degli obiettivi di sviluppo del millennio (*Millenium Development Goals*) di cui alla *Millenium Declaration* delle Nazioni Unite (88): quest'ultima auspica infatti che gli Stati, in cooperazione con il settore privato, rendano « *available the benefits of new technologies, especially information and communications* » e che a tal fine adottino tutte le misure per ottenere che, entro il 2015, vi sia quanto meno una connessione ad *Internet* ogni cento persone.

Anche il Consiglio per i diritti umani (89) ha sollecitato gli Stati ad adottare misure di promozione dell'accesso alle tecnologie di comunicazione, dal momento che tali tecnologie rappresentano mezzi di attuazione della libertà di espressione e di quella di cercare e ottenere informazioni (90); da ultimo, nel corso della sua ventesima sessione, il Consiglio ha adottato una risoluzione che afferma esplicitamente che « *the same rights that people have offline must also be protected online* » (91). E il Rapporto predisposto dal relatore speciale nominato dal medesimo Consiglio per i diritti umani col compito di promuovere e proteggere i diritti alla libertà di espressione e

(82) Come già ricordato, in vigore dal 23 marzo 1976.

(83) EVATT, *The International Covenant On Civil And Political Rights: Freedom Of Expression And State Security*, in *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information* a cura di COLIVER, HOFFMAN, FITZPATRICK e BOWEN, The Hague, 1999, 83 ss.

(84) Il Patto è entrato in vigore il 3 gennaio 1976. Cfr. PINESCHI, *Il Patto delle Nazioni Unite sui diritti civili e politici*, in *La tutela internazionale dei diritti umani. Norme, garanzie, prassi* a cura di PINESCHI, Milano, 2006, 78 ss.; ID., *Il Patto delle Nazioni Unite sui diritti economici, sociali e culturali*, ivi, 129 ss. Più specificamente, VATT, *The International Covenant on Civil and Political Rights: Freedom of Expression and State Security*, in *Secrecy and liberty*, cit., 83 ss.

(85) Cfr. Doc. CCPR/C/GC/34 del 12 settembre 2011, § 12.

(86) Risoluzione dell'Assemblea generale del 22 dicembre 2011, n. A/RES/66/184, su *Information and communications technologies for development*, reperibile in www.un.org.

(87) WSIS, Dichiarazione di principi, cit., A.8.

(88) Con tale risoluzione adottata l'8 settembre del 2000, n. A/RES/55/2, e reperibile all'indirizzo www.un.org, l'Assemblea generale ha esortato gli Stati membri dell'ONU a sradicare la povertà estrema e la fame, rendere universale l'istruzione primaria, promuovere la parità dei sessi e l'autonomia delle donne, ridurre la mortalità infantile, migliorare la salute materna, combattere l'HIV/AIDS, la malaria ed altre malattie, garantire la sostenibilità ambientale e sviluppare un partenariato mondiale per lo sviluppo.

(89) Sul Consiglio v. RODLEY, *UN Treaty Bodies and the Human Rights Council*, in *UN Human Rights Treaty Bodies: Law And Legitimacy* a cura di KELLER e ULFSTEIN, Cambridge, 2012, 320 ss.

(90) *Report of the Speech Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 16 maggio 2011, doc. A/HCR/17/27, § 9.

(91) Human rights Council, 20th regular session, risoluzione del 5 luglio 2012, doc. A/HRC/20/L.13, reperibile all'indirizzo www.ohchr.org.

opinione riconosce l'impatto « senza precedenti » della Rete sulle possibilità degli individui di esercitare i diritti fondamentali e, per questo, esprime preoccupazione per le molteplici misure adottate dagli Stati al fine di limitare il flusso di informazioni *on-line* (92).

Proprio in quest'ultimo senso la prassi recente registra significativi orientamenti giurisprudenziali: la Corte europea dei diritti dell'uomo, nella sentenza relativa all'affare « Yildirim » (93), ha difatti ritenuto incompatibili con l'art. 10 CEDU le misure adottate da un tribunale turco volte a impedire l'accesso all'intera piattaforma *Google Sites*, al fine di evitare la diffusione di informazioni, ritenute illegittime, pubblicate su uno solo dei *blog* di tale piattaforma. D'altro canto la Corte Suprema statunitense nel caso « Reno » aveva già giudicato incostituzionali, per violazione delle libertà di culto, parola e stampa di cui al quinto emendamento, le norme che prevedevano l'adozione di sanzioni nei confronti degli utenti che avevano utilizzato la Rete per diffondere contenuti moralmente sconvenienti (94).

Ci pare poi che la prassi recente di legislatori, organi giurisdizionali ed esecutivi di molti Paesi sia idonea ad indicare quanto meno un *trend* nel senso di ritenere l'accesso ad *Internet* come diritto umano autonomo *ex se*, e cioè indipendentemente dall'uso eventualmente fattone per esercitare altri diritti fondamentali. Si pensi a come, nel luglio 2010, il Governo finlandese abbia adottato un provvedimento che impone alle società che offrono servizi di telecomunicazioni di fare in modo che tutti i cittadini, anche quelli che vivono in località remote, abbiano a disposizione una connessione a banda larga (95), e a come lo Stato di Panama abbia ritenuto di dover estendere l'accesso dei cittadini alla Rete istituendo sul suo esiguo territorio nazionale ben duecentoquattordici punti pubblici di connessione (96).

Per quanto riguarda il legislatore italiano, ricordiamo che l'art. 1 comma 1 l. 9 gennaio 2004, n. 9 (cosiddetta legge Stanca), relativa all'accesso dei disabili alle tecnologie informatiche, riconosce a tutti i cittadini il diritto di accesso ad *Internet*, fondandolo sull'art. 3 della Costituzione e qualificandolo quindi come uno strumento di realizzazione del principio di eguaglianza sostanziale (97). Nel corso della XVI legislatura era finanche stato depositato in Senato un disegno di legge intitolato « Introduzione dell'articolo 21-*bis* della Costituzione recante il riconoscimento del diritto di accesso ad *Internet* » (98); il disegno di legge, poi decaduto, è stato ripreso da ben tre separati progetti di legge depositati alla Camera nella legislatura successiva (99).

Il diritto individuale alla partecipazione alla società dell'informazione e il conseguente dovere statale di promuoverne il progresso sono già previsti dalla Costituzione greca del 2001 (100) e da quella dell'Ecuador del 2008, che riconosce addirittura un diritto soggettivo perfetto alla connessione (101).

---

(92) *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression Frank La Rue*, 17 aprile 2013, doc. A/HRC/23/40.

(93) C. eur. dir. uomo, sez. II, 18 dicembre 2012, Ahmet Yildirim c. Turchia, n. 3111/10, in www.echr.coe.int.

(94) Reno *v.* American Civil Liberties Union, 521 U.S. 844, pubblicata in italiano, in una traduzione di ZENO-ZENCOVICH, in *Dir. inform.*, 1998, 64 ss., la quale dichiara incostituzionale il *Communications Decency Act*, titolo V del *Telecommunications Act* del 1996, 47, U.S.C. § 151 et seq. (Supp. V 2000); in dottrina v. LEETS, *Responses to Internet Hate Sites: Is Speech Too Free in Cyberspace?*, in *Communication Law and Policy*, 2001, 287 ss.

(95) MALKIN, *Finland enshrines "legal right" to broadband*, in *The Telegraph*, 1° luglio 2010.

(96) MILLER, *Measuring the Contribution of Infoplazas to Internet Penetration and Use in Panama*, in *The Massachusetts Institute of Technology Information Technologies and International Development*, 2005, 1 ss.

(97) Cfr. BORGIA, *Riflessioni sull'accesso ad Internet come diritto umano*, in *Comun. intern.*, 2010, 395 ss., in particolare nt. 51.

(98) In Atti parl. Sen., XVI legislatura, doc. n. 3487, in www.senato.it. Cfr. RODOTÀ, *Un articolo 21 bis per internet*, in archivi.articolo21.org/2183/notizia/un-articolo21bis-per-internet-.html.

(99) Proposta di legge costituzionale « Biffoni », in Atti parl. Cam., XVII legislatura, doc. n. 1244, 20 giugno 2013, « Introduzione dell'articolo 21-bis della Costituzione, in materia di riconoscimento del diritto universale di accesso alla rete internet »; proposta di legge costituzionale « De Lorenzis ad altri », in Atti parl. Cam., XVII legislatura, doc. n. 1058, 27 maggio 2013 « Introduzione dell'articolo 21-bis della Costituzione, in materia di riconoscimento del diritto di accesso alla rete internet »; proposta di legge costituzionale « Tentori », in Atti parl. Cam., XVII legislatura, doc. n. 850, 29 aprile 2013, « Introduzione dell'articolo 21-bis della Costituzione, in materia di riconoscimento del diritto di accesso alla rete internet », consultabili in www.camera.it.

(100) Il § 5A comma 2 della Costituzione greca prevede che « ognuno ha il diritto di partecipare alla società dell'informazione », precisando, allo scopo, che « lo Stato ha l'obbligo di agevolare l'accesso alle informazioni che circolano in forma elettronica, nonché la produzione, lo scambio e la diffusione di queste informazioni ».

(101) L'art. 16 prevede che « *todas las personas, en forma individual o colectiva, tienen derecho a:* [...] *2. El acceso universal a las tecnologías de información y comunicación. 3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas* ». Tale diritto soggettivo, peraltro, viene supportato da una serie di obblighi imposti

Riguardo alla prassi giurisprudenziale, ricordiamo che il Consiglio costituzionale francese ha ritenuto illegittime le misure di disconnessione dalla Rete decise dall'Esecutivo per sanzionare accertate violazioni dei diritti di proprietà intellettuale commesse da privati, in quanto non sottoposte preventivamente, ma solo *ex post*, al vaglio dell'autorità giudiziaria (102): il *Conseil* ha ritenuto di dover equiparare le limitazioni imposte alla libertà sulla Rete con quelle alla libertà personale, in una sorta di *habeas corpus electronicus* (103).

Ancora più in là si è spinta la Corte costituzionale del Costa Rica, che ha qualificato l'accesso a *Internet* come un diritto fondamentale degli individui (104), facendone discendere l'obbligo per l'Esecutivo di porre in essere tutte le misure necessarie a garantire che l'intera popolazione possa beneficiare delle nuove tecnologie dell'informazione (ricordiamo come il diritto a godere dei benefici del progresso scientifico e delle sue applicazioni sia riconosciuto dall'art. 15 del Patto sui diritti economici, sociali e culturali).

9. *La* governance *di* Internet *e l'Unione europea (cenni).* — L'Unione europea, muovendosi nel contesto normativo fissato dal diritto internazionale che abbiamo delineato, ha adottato numerosi strumenti di diritto derivato, sia vincolante sia non vincolante, volti a governare la Rete: l'approccio assunto dall'Unione appare più simile a quello di un legislatore interno che a quello delle altre organizzazioni internazionali, dal momento che le norme da essa adottate, in massima parte, non impongono agli Stati membri obblighi che riguardano specificamente la *governance* della Rete in quanto infrastruttura, limitandosi a disciplinare aspetti del mercato interno, e quindi di attività umane (in particolare poste in essere dai consumatori) che hanno luogo *on-line*, come il commercio elettronico (105), i diritti di proprietà intellettuale (106), il trattamento dei dati personali (107).

La dottrina ha cercato di cogliere la caratteristica fondamentale dell'approccio descritto affermando che l'Unione europea, la quale più che "regolamentare" la Rete intende "governarla", avrebbe a tal fine assunto, invece del consueto ruolo di "armonizzatore" degli ordinamenti nazionali, quello di « *policy maker* » (108): molto più semplicemente a noi pare che, sul punto, l'Unione abbia adottato logiche non molto distanti da quelle che avevano caratterizzato il funzionalismo economico, in cui, per il tramite di disposizioni relative ad aspetti economici dell'attività degli individui, le istituzioni comunitarie perseguivano anche obiettivi più latamente politici.

Ad ogni modo, già nel 2002, la Comunità europea al fine di disciplinare il settore delle telecomunicazioni si era dotata di cinque direttive (109), poi modificate e integrate da altre due

---

all'apparato statale al fine di garantirne l'effettività dall'art. 17, il quale prevede che « *el Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: 1. Garantizará la asignación, a través de métodos transparentes y en igualdad de condiciones, de las frecuencias del espectro radioeléctrico, para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelará que en su utilización prevalezca el interés colectivo. 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada. 3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias* ».

(102) Conseil constitutionnel 10 giugno 2009, n. 2009-580, in www.conseil-constitutionnel.fr, relativa alla costituzionalità della l. 12 giugno 2009, n. 2009-669, sulla diffusione e protezione delle creazioni in *Internet*. In dottrina v. Carotti, *L'accesso alla Rete e la tutela dei diritti fondamentali*, in *Giorn. dir. amm.*, 2010, 643 ss.; Simon, *Les adresses IP sont des données personnelles selon le Conseil constitutionnel*, in *Revue Lamy Droit de l'Immatériel*, 2009, 114 ss.; Verpeaux, *La liberté de communication avant tout. La censure de la loi Hadopi 1 par le Conseil constitutionnel*, in *Semaine juridique. Édition générale*, 2009, 46 ss.

(103) Per un approccio differente v. il provvedimento cit. *infra*, nt. 112, che attribuisce ampi poteri di sanzione all'Autorità indipendente italiana sulle comunicazioni.

(104) Corte Suprema de Justicia 30 giugno 2010, n. 12790, reperibile in www.pgr.go.cr.

(105) Direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, n. 2000/31/Ce, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico.

(106) Direttiva del Parlamento europeo e del Consiglio 22 maggio 2001, n. 2001/29/Ce, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.

(107) Direttiva del Parlamento europeo e del Consiglio 12 luglio 2002, n. 2002/58/Ce, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

(108) Savin, *EU Internet Law*, Cheltenham, 2013, 10.

(109) Oltre alla direttiva n. 2002/58/Ce, cit., ne fanno parte le direttive del Parlamento europeo e del Consiglio 7 marzo 2002: n. 2002/21/Ce, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro); n. 2002/19/Ce, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime (direttiva accesso); n. 2002/20/Ce, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni); e n. 2002/22/Ce, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale).

direttive e da un regolamento (110): il complesso normativo che ne è scaturito, detto *Telecoms Package*, costituisce oggi il quadro di base del diritto dell'Unione relativo alle comunicazioni via *web*.

È il caso di sottolineare come la base giuridica utilizzata dalle istituzioni europee per adottare le misure relative a *Internet* sia, in massima parte, costituita dall'art. 114 TFUE, il quale, come noto, consente a Parlamento e Consiglio di porre in essere le misure relative al ravvicinamento delle disposizioni nazionali che hanno per oggetto l'instaurazione e il funzionamento del mercato interno, disciplinato dall'art. 26 TFUE.

Le misure così adottate, seppure relative a settori e aspetti specifici del mercato interno, sono però idonee a produrre un importante impatto sulla *governance* complessiva di *Internet*: ciò è dimostrato dalla giurisprudenza della Corte di giustizia, che, proprio con riguardo all'accesso a *Internet*, ha operato un bilanciamento tra vari diritti fondamentali inclusi nella Carta dei diritti fondamentali dell'Unione europea — quali la protezione dei dati personali (art. 8), la libertà di pensiero (art. 10), quella di espressione e informazione (art. 11), il diritto d'autore (art. 17 § 2) — garantendo prevalenza a tutte le forme di manifestazione del pensiero, di cui *Internet* è certamente mezzo di espressione (111): la Corte ha infatti affermato che gli organi giurisdizionali nazionali sono privi del potere di imporre a un fornitore di servizi *Internet* l'utilizzo di sistemi di filtraggio delle informazioni memorizzate sui suoi *server* dai suoi utenti, anche solo al fine di identificare i *file* contenenti opere protette da diritti di proprietà intellettuale, onde bloccare la messa a disposizione del pubblico di dette opere, lesiva del diritto d'autore, a meno che un potere siffatto non sia già esplicitamente previsto da disposizioni nazionali che ne specifichino preventivamente e in dettaglio limiti e condizioni di esercizio (112).

Per quanto concerne poi le relazioni esterne dell'Unione con altri Stati e organizzazioni internazionali, la Strategia sulla sicurezza informatica dell'Unione europea (113) esplicita l'intento del-

---

(110) Direttiva del Parlamento europeo e del Consiglio 25 novembre 2009, n. 2009/140/CE, recante modifica delle direttive n. 2002/21/CE, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, n. 2002/19/CE, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e n. 2002/20/CE, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica; e direttiva del Parlamento europeo e del Consiglio 25 novembre 2009, n. 2009/136/CE, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori. Nell'occasione è stato anche adottato il reg. CE del Parlamento europeo e del Consiglio 25 novembre 2009, n. 1211/2009, che istituisce l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC). In dottrina v. MASTROIANNI, *Servizi di media audiovisivi (diritto dell'Unione europea)*, in questa *Enciclopedia*, Annali, VI, 2013, 827 ss., nonché HORTEN, *The copyright enforcement enigma: internet politics and the "Telecoms Package"*, Basingstoke, 2012; OROFINO, *Il* Telecoms Package*: luci ed ombre di una riforma molto travagliata*, in *Riv. it. dir. pubbl. com.*, 2010, 513 ss.

(111) C. giust. UE 24 novembre 2011, causa C-70/10, Scarlet Extend c. Société belge des auteurs, compositeurs et éditeurs (SABAM), in *Racc. giur. C. giust.*, 2011, I-11959 ss.; C. giust. UE 16 febbraio 2012, causa C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV, in http://curia.europa.eu.

(112) Ci pare incompatibile con l'orientamento descritto nel testo lo « Schema di regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70 », predisposto dall'Autorità garante per le comunicazioni italiana e sottoposto a consultazione pubblica con delibera del 25 luglio 2013, n. 452/13/CONS, in www.agcom.it. La bozza di provvedimento, pur essendo dichiaratamente mossa dalla consapevolezza che « nell'applicazione della disciplina del diritto d'autore sulle reti di comunicazione elettronica è necessario operare il bilanciamento tra i diversi diritti in gioco, rispettando la libertà di espressione e di manifestazione del pensiero, il diritto alla privacy e l'accesso dei cittadini alla cultura e ad internet, alla luce di quanto sancito dall'ordinamento dell'Unione in materia di comunicazioni elettroniche, e tutelando il diritto d'autore e la remunerazione del titolare dei diritti », prevede però due possibili misure sanzionatorie adottabili dall'Autorità stessa, ossia la « rimozione selettiva » e la « disabilitazione dell'accesso ». In particolare, la prima dovrebbe essere « applicabile nei casi in cui il sito ospiti sia contenuti legali che contenuti illegali e non abbia quale finalità prevalente quello della pirateria informatica » e sarebbe « implementabile dai prestatori di servizi per i server collocati sul territorio nazionale, mentre, nel caso di server collocati all'estero, si tratta di una misura che non appare opportuno prevedere in quanto implicherebbe il ricorso a tecniche di filtraggio non compatibili con la recente giurisprudenza della Corte di giustizia dell'Unione europea »; la disabilitazione dell'accesso al contenuto illegale è invece realizzata mediante « il blocco dell'IP e/o della risoluzione DNS » e « appare la più idonea sia per le ipotesi di pirateria massiva, sia nel caso di siti con server situati all'estero. Tale misura potrebbe anche essere "aggirata" dal pubblico nazionale mediante l'accesso alle opere per altre vie (cd. *proxy* esteri). Essa ha tuttavia un effetto collaterale positivo, in quanto, accedendo attraverso il *proxy*, il sito non viene remunerato in base alla pubblicità parametrata seguendo il numero degli accessi, potendo così comportare un forte incentivo al consumo di prodotti "legali" ».

(113) Comunicazione congiunta della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, « Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aper-

l'Unione di operare in questo settore nel rispetto del principio di cooperazione, di cui abbiamo detto *supra*, § 6, al fine di tutelare i diritti fondamentali e di garantire la resilienza informatica (cioè la capacità di un sistema informatico di adattarsi alle condizioni d'uso e, soprattutto, di resistere all'usura e a eventuali attacchi in modo da continuare a offrire i suoi servizi), ridurre la criminalità informatica, sviluppare le capacità informatiche connesse alla politica di sicurezza e di difesa comune, sviluppare le risorse industriali e tecnologiche a tal fine impiegate. Per il raggiungimento di tali obiettivi, oltre al rafforzamento del ruolo e delle funzioni svolte dall'Agenzia europea per la sicurezza delle reti (ENISA), sono attualmente allo studio numerosi strumenti di diritto derivato al fine di incrementare il livello di cooperazione tra i Paesi membri nel quadro già istituito da una precedente decisione quadro relativa agli attacchi contro i sistemi di informazione (114), a sua volta largamente ispirata al modello della Convenzione sul *cybercrime* del Consiglio d'Europa di cui abbiamo detto *supra*, § 4.

Gianpaolo Maria Ruotolo

FONTI. — Nazioni Unite: *a*) Assemblea generale: risoluzioni 22 novembre 2002, n. A/RES/57/53, 8 dicembre 2003, n. A/RES/58/32, 3 dicembre 2004, n. A/RES/59/61, 8 dicembre 2005, n. A/RES/60/45 e 6 dicembre 2006, n. A/RES/61/54, tutte concernenti « *Developments in the field of information and telecommunications in the context of international security* »; risoluzioni 21 dicembre 2009, n. A/RES/64/187 (doc. reso pubblico il 9 febbraio 2010) e 20 dicembre 2010, n. A/RES/65/141, entrambe concernenti « *Information and communication technologies for development* »; *b*) Consiglio economico e sociale: risoluzione 28 luglio 2006, n. 2006/46, « *Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development* »; *c*) Consiglio dei diritti dell'uomo: risoluzione 29 giugno 2012, n. A/HRC/20/L.13, « *The promotion, protection and enjoyment of human rights on the Internet* »; *d*) *World Summit on Information Society* (WSIS): Dichiarazione di principi, Ginevra, 12 dicembre 2003, n. WSIS-03/GENEVA/DOC/4-E, « *Building the Information Society: A Global Challenge In The New Millennium* »; *Tunis Commitment*, Tunisi, 18 novembre 2005, doc. WSIS-05/TUNIS/DOC/7-E; *Tunis Agenda for the Information Society*, Tunisi, 18 novembre 2005, n. WSIS-05/TUNIS/DOC/6(Rev. 1)-E; *e*) *Internet Governance Forum*: 5 novembre 2012, Baku Declaration of the High Level Ministerial Meeting on « *Addressing The Challenges Of A Hyperconnected World* »; *International Telecommunications Union* (ITU): *Final Acts World Conference on International Telecommunications*, Dubai, 14 dicembre 2012.

Unione europea: direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, n. 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; direttiva del Parlamento europeo e del Consiglio 22 maggio 2001, n. 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; decisione del Parlamento europeo e del Consiglio 16 dicembre 2008, n. 1351/2008/CE, relativa a un programma comunitario pluriennale per la protezione dei bambini che usano Internet e altre tecnologie di comunicazione; Comunicazione congiunta della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, « Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro », 7 febbraio 2013, doc. JOIN(2013) 1 final.

LETTERATURA. — AMOROSO, *Cyber attacks: protecting national infrastructure*, Waltham (Massachusetts), 2013; AUDIT, *Droit international de l'internet*, in *Revue Lamy Droit de l'Immatériel*, 2010, 4 ss.; BALLARINO, *Internet nel mondo della legge*, Padova, 1996; BEARD, *Law and War in the Virtual Era*, in *Am. journ. intern. Law*, 2009, 1 ss.; BENEDEK, *Internet governance and the information society: global perspectives and European Dimensions*, Utrecht, 2008; CAMMAERTS, *Internet-mediated participation beyond the nation State*, Manchester, 2008; DENARDIS, *Protocol Politics. The Globalization of Internet Governance*, Cambridge-London, 2009; DRAETTA, *Internet et commerce électronique en droit international des affaires*, in *Recueil des Cours de l'Académie de droit international de la Haye*, CCCXIV, 2005, 9 ss.; FIDLER, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, in 7 *American Society of International Law Insights*, 2013, n. 6, 1 ss.; GERCKE, *The Slow Wake of a Global Approach Against Cybercrime: the Potential of the Council of Europe Convention on Cybercrime as International Model Law*, in *Computer Law Review International*, 2006, 145 ss.; GOLDSMITH e WU, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, 2006; *Governing the internet: freedom and regulation in the OSCE region* a cura di MÖLLER e AMOUROUX, Vienna, 2007; GUADAMUZ, *Networks, Complexity and Internet Regulation: Scale-Free Law*, Cheltenham, 2011; HARRISON DINNISS, *Cyber Warfare and the Laws of War*, Cambridge, 2012; HART, *Internet law: a field guide*, Arlington (Texas), 2008; HEVERLY, *Breaking the Internet: International Efforts to Play the Middle Against the Ends - A Way Forward*, in *Georgetown Journal of International Law*, 2011, 1083 ss.; 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.; JACOB, *La gouvernance de l'internet du point de vue du droit international public*, in *Anr. fr. dr. intern.*, 2010, 543 ss.; JORGENSEN, *Framing the Net - Internet and Human Rights*, Cheltenham, 2013; KULESZA, *International Internet Law*, New York, 2012; KURBALIJA, *An Introduction to Internet Governance*, Msida (Malta)-Genève, 2010; *Le droit international de l'internet (Actes du Colloque, Ministère de la Justice, Paris, 19-20 novembre 2001)* a cura di CHATILLON, Bruxelles, 2003; *Les dimensions internationales du droit du cyberspace* a cura di FUENTES-CAMACHO, Paris, 2000; LESSIG, *Code - Version 2.0*, Cambridge, 2006; MARSDEN, *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*, Cambridge, 2011; MATHIASON, *Internet governance: the new frontier of global institutions*, London, 2009; MORTH, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2 (4) of the U.N. Charter*, in *Case*

to e sicuro », 7 febbraio 2013, doc. JOIN(2013) 1 final, in www.europa.eu.

(114) Decisione quadro del Consiglio 24 febbraio 2005, n. 2005/222/GAI, la quale ha l'obbiettivo di armonizzare gli ordinamenti dei Paesi membri con riguardo ad alcune fattispecie penali rilevanti per la lotta coordinata alla criminalità informatica e la criminalità organizzata e il terrorismo che utilizzano gli strumenti informatici.

Western Reserve Journal of International Law, 1998, 567 ss.; Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge-London, 2002; Oddenino, *La* governance *di Internet fra autoregolazione, sovranità statale e diritto internazionale*, Torino, 2008; Perrit, *The Internet is Changing the Public International Legal System*, in *Kentucky Law Journal*, 2000, 885 ss.; Polanski, *Customary Law of the Internet. In the Search for a Supranational Cyberspace Law*, Berlin, 2007; Post, *In Search of Jefferson's Moose*, Oxford, 2009; *Research Handbook on Governance of the Internet* a cura di Brown, Cheltenham, 2013; Rijgesberg, *The state of interdependence: globalization, Internet and constitutional governance. The modern State and transnational interdependence*, The Hague, 2010; Rogers, *The Internet and International Law*, in *Kentucky Law Journal,* 2000, 803 ss.; Ruotolo, *Internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012; Ryan D., Dion, Tikk e Ryan J., *International Cyberlaw: A Normative Approach*, in *Georgetown Journal of International Law*, 2011, 1161 ss.; Savin, *EU Internet Law*, Cheltenham, 2013; Schultz, *Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, in *Eur. journ. intern. Law*, 2008, 799 ss.; Segura Serrano, *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, 2006, 1374; Spang-Hanssen, *Public International Computer Network Law Issues*, Copenhagen, 2006; *Tallinn Manual on the International Law Applicable to Cyber Warfare* a cura di Schmitt, Cambridge, 2013; *The Oxford Handbook of Internet Studies* a cura di Dutton, Oxford, 2013; Ventre, *Cyberattaque et cyberdéfense*, Paris, 2011; Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal of International Law*, 2011, 421 ss.


F D
d
F D
d
F D
d