RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0060
Articolo sottoposto a peer review

La Governance di Internet oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale

Angelo Alù

Il saggio identifica le principali questioni che il futuro ecosistema digitale pone, descrivendo il fenomeno della frammentazione di Internet come uno degli aspetti più complessi e problematici che emergono nell'attuale scenario geopolitico, ove si manifesta la tendenza degli Stati all'elaborazione di politiche "tecnonazionalistiche" volte alla costruzione di una Rete autonoma e indipendente, tecnologicamente difforme dall'originaria architettura distribuita e interoperabile su cui si basa il tradizionale modello operativo dell'Internet globale. Proliferano, infatti, nel panorama globale svariati interventi regolatori che impongono l'uso massivo di strumenti di sorveglianza generale per assicurare il controllo centralizzato della Rete, come obiettivo strategico prioritario di supremazia tecnologica stabilito a presidio delle infrastrutture critiche degli Stati, per evitare il rischio di possibili attacchi esterni in grado di destabilizzarne l'ordinamento interno. Rispetto alla progressiva balcanizzazione della Rete, si sta al contempo rafforzando, come imprevista variabile del mutato ecosistema di Internet, il potere – economico e politico – delle "Big Tech" nella veste di nuovi "players" dominanti che potrebbero dare vita ad un'inedita governance digitale oltre gli Stati.

Internet Governance – Frammentazione di Internet – Big-Tech – Splinternet – Sovranità digitale

1. Introduzione: verso nuovi modelli di governance digitale

L'attuale ecosistema di Internet sembra manifestare una significativa metamorfosi dell'originario modello di governance digitale risalente alla sua iniziale configurazione delineata dalla cd. "Agenda di Tunisi"[1], che edifica un modello partecipativo funzionale a salvaguardare, nella definizione delle politiche dedicate alla gestione di Internet, il primato del settore pubblico, sul presupposto che debbano essere gli organi democraticamente legittimati nel circuito politico-istituzionale ad assumere le scelte finali sia pure all'esito di un costante dialogo di cooperazione multilaterale ispirato al criterio "multistakeholder"[2].

Rispetto alla prima fase di sviluppo embrionale della Rete[3], nell'ambito del percorso evolutivo dell'ecosistema digitale, si è progressivamente determinato, in un clima di crescenti tensioni tra le superpotenze a livello globale[4], uno speculare processo di "balcanizzazione" di Internet[5] che ha accentuato l'interesse degli Stati a intensificare le politiche di controllo per la gestione della Rete[6] anche nel tentativo di ridefinire i tratti della sua tradizionale architettura tecnica[7] al fine di raggiungere la supremazia tecnologica, economica ed industriale[8] e, al contempo, giustificare

A. Alù è dottore di ricerca in Giurisprudenza e consigliere della Internet Society Italia.
Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

l'estensione di pervasivi poteri di sorveglianza[9] che realizzano forme di "autoritarismo digitale"[10], senza spesso fornire adeguate protezioni contro gli abusi[11].

Alla luce di un contesto regolatorio sempre più divisivo e differenziato, emergono epocali cambiamenti tecnologici dalle rilevanti implicazioni non solo economiche ma anche politiche destinate a trasformare la società nel suo complesso[12].

In tale mutato scenario si manifestano i tratti peculiari di un'inedita governance digitale, in grado di formalizzare, mediante una ridefinizione dei rapporti di forza nei tradizionali assetti di equilibrio dei poteri, il primato – anche politico – delle imprese "high-tech" nella veste di nuovi "players" dominanti che, a fronte della progressiva frammentazione delle regolamentazioni nazionali su Internet, potrebbero infatti generare un nuovo – e attualmente indecifrabile – ecosistema tecnologico al di fuori degli ordinari circuiti decisionali di legittimazione democratica politico-istituzionale[13].

2. L'impatto delle politiche statali sulla frammentazione della Rete

Dalla sua originaria genesi risalente al primordiale progetto Arpanet, Internet si è rapidamente diffusa su scala globale – anche grazie alla creazione del cd. Web ("World Wide Web")[14] – determinando un incremento esponenziale degli utenti della Rete[15] che costituisce il "network of networks"[16] cui tutti possono accedere per reperire informazioni e diffondere informazioni fruibili in tutto il mondo.

L'espansione planetaria di Internet rende particolarmente controversa la regolamentazione della sua gestione tecnico-operativa, consentendo di comprendere il crescente interesse dei governi nazionali nei confronti di un'infrastruttura strategica, la cui concreta implementazione incide non solo sull'architettura logica della Rete, ma altresì sulle visioni politiche di controllo delle risorse digitali per assicurare l'erogazione dei servizi di telecomunicazione, l'esercizio dei diritti fondamentali degli individui e la tenuta degli standard democratici degli ordinamenti nazionali[17].

In tale prospettiva, si è intensificato il dibattito internazionale in ordine alla necessaria ridefinizione della governance digitale[18], per assicurare l'effettiva compartecipazione decisionale di tutti gli attori interessati al processo gestionale della Rete[19].

Già in occasione della rinegoziazione delle ITRs[20], è emerso un ostile contrasto, che sembra evocare l'inizio di un'inedita "digital cold war"[21], tra la visione decentralizzata di Internet (contraria a qualsivoglia regolamentazione frammentata della Rete in grado di limitarne la libertà) e la visione "statalista" (favorevole al riconoscimento di un maggiore potere degli Stati per assicurare, in nome di preminenti esigenze di sicurezza nazionale, una paritaria gestione nella funzione di controllo dell'infrastruttura tecnica di Internet)[22].

Alla luce delle divergenze esistenti sulla governance digitale nelle relazioni geopolitiche globali[23], si sta edificando, nell'ambito di una cornice regolatoria diversificata a livello nazionale, la costruzione di un'Internet alternativa (cd. "Splinternet"[24]) tecnologicamente difforme dall'originaria architettura distribuita e interoperabile della Rete.

In contrapposizione al tradizionale modello "aperto" di Internet, fondato sul primato tecnologico degli Stati Uniti d'America – che hanno (indirettamente) assunto a lungo, come unica superpotenza mondiale, il ruolo chiave di gestore principale della Rete attraverso l'attività dell'ICANN (*Internet Corporation for Assigned Names and Numbers*)[25] –, alcuni Stati stanno frammentando Internet, creando reti nazionali indipendenti dall'egemonia americana per evitare il rischio di ingerenze in grado di compromettere la sicurezza interna[26].

L'esigenza di proteggere lo spazio virtuale della Rete entro i propri confini nazionali viene invocata per rafforzare il ruolo degli Stati nazionali nell'ecosistema della Rete[27], anche mediante l'emanazione di leggi *ad hoc* volte alla creazione di un'Internet autonoma e sovrana[28] che consente di attuare forme pervasive di controllo sul flusso di informazioni veicolate online a presidio della cybersicurezza domestica[29].

La frammentazione di Internet, giustificata dalla necessità di ridurre la dipendenza esterna da organizzazioni straniere per rendere meno vulnerabili, mediante l'adozione di efficaci misure difensive, le infrastrutture nazionali critiche a fronte di possibili attacchi informatici in grado di pregiudicare gli interessi vitali di un Paese, realizza quindi un ingente controllo dei dati, anche intercettando le comunicazioni online – spesso con il supporto degli operatori telematici – per perseguire, sul versante interno, finalità di sorveglianza massiva con l'intento di contrastare e censurare gli avversari oppositori dei regimi politici in carica[30].

In tale scenario, la Russia, ad esempio, ha testato (nell'ambito di un ambizioso programma di implementazione dell'economia digitale[31]), la propria rete nazionale cd. "Runet"[32], come sistema alternativo di connessione Internet scollegato dal resto del mondo, che rappresenta il punto di inizio di una strategia di indipendenza tecnologica[33] in grado di bloccare l'accesso a servizi digitali stranieri, con indirette potenziali e insidiose ripercussioni per la libertà degli

utenti a causa di generalizzati effetti repressivi che potrebbero prodursi nell'ambiente virtuale mediante strumenti di "filtro" utilizzati per la selezione del flusso informativo veicolato online[34].

Internet risulta, pertanto, sottoposta a strategie massive di sorveglianza generale motivate dall'esigenza di assicurare la tutela della sicurezza nazionale, anche a costo di limitare le voci di dissenso esistenti, ove non allineate alla "narrazione" ufficiale della comunicazione istituzionale, consentendo il rafforzamento di regimi autocratici in grado di utilizzare massive tecnologie di manipolazione virtuale che trovano terreno fertile nel cyberspazio[35].

Anche le politiche tecnologiche del governo cinese alimentano ulteriormente la frammentazione della Rete[36] mediante il controllo centralizzato di Internet[37] che, pur sfruttando i vantaggi offerti dall'innovazione[38], richiede l'implementazione di specifici standard operativi funzionali a salvaguardare la sovranità digitale di Pechino[39], senza rendere le tecnologie volano di cambiamenti politici suscettibili di destabilizzare il sistema di potere vigente[40].

In particolare, l'infrastruttura cinese si basa su un'architettura digitale "separata e ideologicamente distinta"[41] dall'Internet globale che, in applicazione di un vasto e articolato insieme di leggi e regolamenti dettagliati[42], prevede svariati strumenti di censura[43] con funzioni di supervisione, blocco e monitoraggio del flusso comunicativo veicolato nell'ambiente digitale, grazie al sempre più sofisticato perfezionamento tecnico del cd. "Great Firewall"[44].

3. La sovranità digitale come nuova prospettiva europea del governo di Internet

Mentre ancora il dibattito internazionale si trova in una fase embrionale di ridefinizione teorica del governo digitale alla ricerca di soluzioni efficaci in grado di assicurare l'adeguamento dell'attuale ecosistema di Internet rispetto alle complesse sfide regolatorie[45] che l'innovazione pone, nel frattempo si assiste alla rapida implementazione di svariati progetti tecnologici, la cui configurazione applicativa espone al rischio di pervasivi strumenti di controllo automatizzato in grado di realizzare sofisticate forme di sorveglianza massiva per finalità generali di sicurezza[46], mediante inedite strategie di intelligence da "cyberwar"[47] legate all'utilizzo di tecnologie emergenti che consentono anche l'identificazione biometrica degli individui e il tracciamento computerizzato delle identità personali[48].

Nell'ambito dell'ecosistema digitale dell'Unione europea si registra un progressivo potenziamento delle azioni di cibersicurezza per combattere il crimine informatico, rafforzando le misure difensive a presidio delle infrastrutture critiche in presenza di uno scenario evolutivo sempre più insidioso, caratterizzato da un incremento esponenziale di inediti pericoli configurabili nell'ambiente virtuale, ove circola un flusso quotidiano di decine di quintilioni di byte di dati processati da miliardi di dispositivi IoT (che potrebbero raggiungere la quota di 125 miliardi entro il 2030[49]). Risulta, pertanto, necessario, in via prioritaria, predisporre una governance digitale autonoma e sovrana, stimolando le capacità strategiche e di cooperazione[50] dell'UE[51], per realizzare un cyberspazio aperto e sicuro, «come quinto dominio della guerra[52], fondamentale per le operazioni militari»[53].

Alla stato attuale sussiste un generale quadro di vulnerabilità riscontrabile negli Stati europei che impedisce il raggiungimento di adeguati standard di sicurezza[54], pur in presenza di un'economia digitalizzata sempre più interconnessa, sebbene esposta a possibili attacchi esterni ostili a causa di un diffuso deficit infrastrutturale aggravato da condizioni radicate di ritardo tecnologico[55] in stato di (cyber)"dipendenza neocoloniale"[56].

In tale prospettiva, l'Europa aspira a conquistare la cd. sovranità digitale[57], come obiettivo strategico di integrazione sovranazionale volto a realizzare un indispensabile riposizionamento geopolitico della propria centralità nella ridefinizione dei rapporti di forza esistenti su scala globale[58] rispetto alle dinamiche conflittuali della predominante competizione tecnologica dualistica USA-Cina, non solo per farsi trovare proficuamente pronta a cogliere le opportunità offerte dal progresso tecnologico (nell'ottica di favorire la crescita del mercato digitale e stimolare la competitività produttiva sulla spinta di ingenti investimenti e generali riforme dei settori maggiormente trainati dall'innovazione[59]), ma altresì, in chiave preventiva, per evitare di subire cd. "minacce ibride"[60] a causa di attacchi informatici, interventi di cyberspionaggio[61], campagne massive di disinformazione, azioni di disturbo e strategie di manipolazione sistemica dell'opinione pubblica in grado di destabilizzare la società nel suo complesso[62], mettendo a rischio la tenuta degli ordinamenti democratici[63].

Pur essendo ancora significativo il "gap" tecnologico rispetto alle superpotenze globali, l'Unione europea, grazie ad un recente incisivo approccio regolatorio[64] interventista e proattivo, sta consolidando un quadro giuridico sempre più vigoroso e sviluppato in grado di modellare la governance di Internet, la cui configurazione potrebbe imporsi nella concreta prassi in ragione del rilevante valore economico del mercato digitale europeo, con l'effetto catalizza-

tore di indurre il tessuto imprenditoriale "high-tech" su scala planetaria ad adeguarsi spontaneamente alle relative prescrizioni per poter instaurare vantaggiosi rapporti commerciali forieri di un ingente introito di profitti generati dal settore ICT[65].

4. Scenari inediti e aspetti critici: una governance digitale oltre gli Stati?

La governance di Internet[66] è stata formalizzata in sede internazionale con l'istituzione dell'Internet Governance Forum (IGF)[67] che opera, con un mandato quinquennale soggetto a revisione periodica[68], come *forum* multilaterale, aperto, inclusivo e collaborativo chiamato ad esprimersi sui temi legati all'ecosistema della Rete mediante la semplice formulazione di mere raccomandazioni senza però adottare decisioni vincolanti, pur garantendo la formale paritaria rappresentatività di tutte le parti interessate (Stati, istituzioni accademiche, settore privato e società civile) coinvolte nell'ambito dei lavori realizzati da gruppi consultivi che si riuniscono durante ogni consueto *meeting* annuale[69].

Sebbene siano stati promossi anche forum nazionali per stimolare ulteriormente la cooperazione su vasta scala secondo un maggiore diffuso livello di interazione e integrazione tra gli attori interessati al processo di definizione delle politiche sulla Rete[70], nella concreta prassi la partecipazione dei governi è progressivamente diminuita poiché l'IGF rappresenta in ogni caso un organismo informale privo di poteri cogenti, rendendo quindi l'incidenza dei relativi lavori conclusivi generalmente tenue e marginale in termini di azioni concrete tangibili sull'ecosistema digitale[71].

In tale prospettiva, l'attuale (ancora per poco?) modello di governance risulta progressivamente eroso dall'avvento di un inedito ecosistema digitale fondato sulla concentrazione di potere in capo alle autorità nazionali per isolare Internet, in reti sempre più disconnesse, entro i propri confini territoriali, unitamente al crescente dominio – economico e politico – delle imprese "high-tech"[72].

In un mutato scenario di contesa geopolitica, sembra pertanto delinearsi una progressiva perdita di centralità dell'IGF[73], al pari di qualsivoglia ulteriore iniziativa internazionale di cooperazione multilaterale[74].

Anche sulla spinta di esigenze di regolamentazione a "geometria variabile" volte al rafforzamento della "sovranità digitale"[75], in un crescente clima di tensioni tra le superpotenze globali (destinate verosimilmente a culminare in una possibile "alleanza tecnologica anti-cinese"[76]), emerge, infatti, la configurazione "tripolare"[77] di Internet che, lungi dal privilegiare forme di multilateralismo partecipativo, risulta scomponibile in distinti poli di influenza nella definizione delle regole applicabili all'ambiente digitale, dando vita ad un processo di balcanizzazione destinato a sfociare nella frammentazione di un variegato quadro giuridico sull'ecosistema della Rete, in cui i singoli Stati cercano sempre più spesso di imporre i propri specifici orientamenti politici "particolari" per definire le caratteristiche di un nuovo cyberspazio dalle caratteristiche di funzionamento del tutto diverse rispetto alla sua originaria conformazione libertaria[78].

Invero, lo sforzo competitivo dei governi nazionali per affermare la propria autorità su Internet si sta intensificando in parallelo al crescente potere dei "Colossi del web" che potrebbero rappresentare un'ulteriore variabile – ancora non del tutto decifrabile – per la nascita di un nuovo ordine "tecno-politico" globale.

Le aziende tecnologiche stanno, infatti, assumendo le inedite sembianze di dominanti "digital decision makers" per la definizione delle nuove "regole del gioco" da imporre a livello planetario – in una logica presumibilmente non neutrale e discriminatoria[79] – nell'ambito della progressiva frammentazione di Internet alimentata dai recenti interventi settoriali adottati dai singoli Stati che, piuttosto che rafforzare le garanzie di tutela dei diritti configurabili in Rete, approfittano dei pericoli di propaganda estremista, odio, disinformazione, attacchi informatici e illeciti di varia natura sempre più diffusi online[80] per rivendicare, spesso anche con la complicità degli stessi intermediari telematici fornitori dei servizi digitali[81], l'acquisizione di pervasivi poteri di controllo e repressione come decisa inversione di rotta rispetto all'originaria configurazione del governo della Rete esistente su scala globale[82].

In altri termini, si potrebbe progressivamente affermare un'inedita governance digitale[83] declinabile anche oltre gli Stati, cedendo quindi il passo al definitivo primato dei cd. "Colossi del web"[84], fondato sull'uso pervasivo di sofisticati e invisibili sistemi algoritmici di tracciamento, profilazione[85] e manipolazione[86] dalle implicazioni ancora non del tutto note[87].

Note

[1] Cfr. *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6, 18 November 2005.

[2] Al riguardo, l'Agenda di Tunisi sottolinea che: «a) l'autorità politica per le questioni di politica pubblica relative a Internet è il diritto sovrano degli Stati [...]; b) il settore privato ha avuto e dovrebbe continuare ad avere un ruolo importante nello sviluppo di Internet, sia in campo tecnico che economi-

co; c) anche la società civile ha svolto un ruolo importante in materia di Internet, in particolare a livello di comunità, e dovrebbe continuare a svolgere tale ruolo; d) le organizzazioni intergovernative hanno avuto e dovrebbero continuare a svolgere un ruolo di facilitazione nel coordinamento delle questioni di politica pubblica legate a Internet; e) anche le organizzazioni internazionali hanno avuto e dovrebbero continuare a svolgere un ruolo importante nello sviluppo di standard tecnici relativi a Internet e politiche pertinenti»: cfr. *Tunis Agenda for the Information Society*, cit., p. 35.

[3]Lo sviluppo tecnologico di Internet risale alla creazione della rete Arpanet, come sistema affidabile di comunicazione distribuita, progettato per garantire la trasmissione di informazioni tra le unità periferiche in condizioni di stabilità e sicurezza grazie al perfezionamento di una struttura aperta e decentralizzata, basata sulla tecnologia "packet switching", implementata per evitare rischi di paralisi e blocchi causati da vulnerabilità e criticità in grado di determinare possibili danneggiamenti con la conseguente perdita dei dati memorizzati. Sul tema: A. Di Corinto, *Internet non è nata come progetto militare, mettetevelo in testa*, in L. Abba, A. Di Corinto (a cura di), "Il futuro trent'anni fa. Quando Internet è arrivata in Italia", Manni, 2017.

[4]Cfr. C. Hobbs (ed.), *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*, European Council on foreign relations, 30 July 2020; M. Leonard, J. Shapiro, *Strategic sovereignty: How Europe can regain the capacity to act*, European Council on foreign relations, 25 June 2019.

[5]Per un approfondimento sul tema si rinvia a M. Bey, *The Age of Splinternet: The Inevitable Fracturing of the Internet*, in "Worldview", 25 April 2019.

[6]Al riguardo, si rinvia alle osservazioni di L. Zorloni, *La Cina non ha rinunciato al suo progetto per cambiare i connotati di internet*, in "Wired.it", 11 dicembre 2021. In particolare, l'autore descrive la strategia della Cina volta a sostituire, con il nuovo protocollo "New IP", l'attuale standard di Internet, per superare il modello TCP/IP, al fine di risolvere i problemi della Rete globale e garantire l'efficiente sviluppo dei servizi digitali, senza al contempo frenare il processo evolutivo dell'innovazione. Si veda anche L. Zorloni, *La silenziosa battaglia della Cina per cambiare le regole di internet*, in "Wired.it", 9 dicembre 2020.

[7]L'architettura tecnica di Internet si basa sul funzionamento del cd. "Internet Protocol Suite" (regolato dalla RFC 791/1981), e consta di due protocolli primari di trasmissione: il TCP (*Transmission Control Protocol*), e l'IP (*Internet Protocol*), che assicurano l'intercomunicabilità univoca dei dati trasmessi da reti diverse.

[8]Si veda N. Attrill, A. Fritz, *China's cyber vision: How the Cyberspace Administration of China is building a new consensus on global internet governance*, Policy Brief Report No. 52/2021, International Cyber Police Centre, November 2021.

[9]Secondo le rilevazioni empiriche contenute nel Report *Freedom House 2021*. Sul tema si segnala L. Zorloni, *La Cina può disconnettersi dall'internet globale quando vuole*, in "Wired.it", 20 agosto 2019.

[10]Cfr. R. Kemeny, *Brazil is sliding into techno-authoritarianism*, in "MIT Technology Review", 19 August 2020.

[11]Prolifera la frammentazione sempre più conflittuale e illiberale della Rete in sistemi autoreferenziali localizzati entro i confini statali, regolati da legge nazionali e separati dall'ecosistema globale di Internet, con il rischio di generare l'utilizzazione massiva di svariati sistemi di "filtri" dei contenuti controllati online per finalità politiche di censura e sorveglianza su vasta scala. Si vedano: J.C. Wong, *Revealed: the Facebook loophole that lets world leaders deceive and harass their citizens*, in "The Guardian", 12 April 2021; G. Porro, *Putin incassa il primo sì per isolare internet in Russia*, in "Wired.it", 12 aprile 2019.

[12]Sul versante imprenditoriale si assiste alla promozione, in via sperimentale, di numerose iniziative formative per sviluppare le competenze digitali richieste dal mercato del lavoro e incrementare le opportunità professionali legate al settore ICT, con l'intento di fornire soluzioni di alta specializzazione nei settori più altamente remunerativi (come, ad esempio, i cd. "Google Career Certificates"), unitamente all'inedita definizione di politiche di "cyber-welfare state" redistributive della ricchezza, mediante l'erogazione di un reddito universale di base come sussidio pagato agli individui, indipendentemente dal fatto che lavorino o meno, nell'ottica di compensare gli svantaggi derivanti da una possibile contrazione della forza lavoro provocata dalla cd. "automazione dei processi robotici". Sul tema: J. Sadowski, *Why Silicon Valley is embracing universal basic income*, in "The Guardian", 22 June 2016.

[13]Alla crescita continua di ricavi generati dall'utilizzo massivo di un'elevata varietà di applicazioni, piattaforme di e-commerce, servizi di messaggistica e social network offerti in regime di strapotere tecnologico a istituzioni pubbliche, imprese, operatori privati e utenti cittadini, si aggiunge l'ulteriore massiva acquisizione, da parte dei "Colossi del web", di un consistente patrimonio di dati personali, da cui discende un enorme potere gestito da imprese private che sono in grado di influenzare, anche indirettamente, le scelte dell'opinione pubblica sul dibattito politico e la libertà di autodeterminazione individuale. Sia consentito rinviare ad A. Alù, *Stati contro le big tech: siamo allo scontro finale? La linea dura di Ue, Usa e Cina*, in "Agendadigitale.eu", 13 maggio 2021.

[14]Il Web è stato sviluppato da Tim Berners-Lee, insieme a Robert Calliau, nel 1991 presso il CERN di Ginevra, come innovativo servizio di organizzazione dei contenuti disponibili online, basato sul linguaggio "html" (*Hypertext markup language*) che consente agli utenti di reperire facilmente le informazioni ricercate mediante collegamenti ipertestuali (cd. "link"), con l'intento di promuovere, come "mission" valoriale sottesa alla realizzazione del progetto, la diffusione di una Rete universale, libera e accessibile. Per un approfondimento, T. Berners-Lee, *L'architettura del nuovo web*, Feltrinelli, 2001.

[15]Secondo il Report "Global Digital 2020", a fronte di poco meno di 8 miliardi di persone, sono 4,66 miliardi gli utenti che accedono ad Internet, come quota che rappresenta il 59,5% di penetrazione globale (con un incremento del 7,3% rispetto al precedente anno), mentre risultano attivi 4,20 miliardi di utenti delle piattaforme sociali, registrando una penetrazione dei social pari al 53% della popolazione mondiale (con un incremento del 13% rispetto al 2020). Circa 5,22 miliardi di persone utilizzano telefoni cellulari, pari al 66,6% della popolazione globale. L'utente medio di Internet trascorre online 6 ore e 43 minuti ogni giorno (corrispondenti a più di 100 giorni di connessione l'anno), di cui circa 2 ore e 30 minuti nei social network (cfr. Report *Digital 2021 – Global Overview Report*, in "We are Social", in collaborazione con Hootsuite).

[16]Cfr. Corte Federale degli Stati Uniti – Distretto Orientale della Pennsylvania, sentenza 11 giugno 1996, caso *American Civil Liberties Union e American Library Association v. Stati Uniti d'America*.

[17]Su tali aspetti si rinvia a L. Abba, A. Alù, *Internet Governance Forum: l'evoluzione del modello multi-stakeholder tra criticità e prospettive future*, in questa Rivista, 2020, n. 1.

[18]In tal senso, Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni *Governance e politica di Internet, il ruolo dell'Europa nel forgiare il futuro della governance di Internet*, doc. COM(2014) 72 del 12 febbraio 2014.

[19]*Principles for the Governance and Use of the Internet*, elaborati nell'ambito del Council Working Group on

International Internet-Related Public Policy Issue, Brasile, 2012.

[20]Le *International Telecommunication Regulations* (ITRs), adottate dall'ITU nel 1998 a Melbourne a conclusione della *World administrative telegraph and telephone conference*, costituiscono la fonte di regolamentazione internazionale delle telecomunicazioni. Poiché le ITRs erano inizialmente applicabili alle sole comunicazioni radiotelegrafiche e telefoniche con esclusione della Rete Internet, si è svolta, a Dubai nel dicembre 2012, la *World Conference on International Telecommunication* (WCIT-2012), su impulso dell'International Telecommunication Union (ITU) per assicurare il necessario adeguamento di tali norme al progresso tecnologico del sistema delle comunicazioni, in attuazione della Resolution 146 (Antalya, 2006), *Rewiew of the International Telecommunication Regulations*.

[21]L.S., *A digital cold war?*, in "The Economist", 14 December 2012.

[22]Sul tema, si rinvia alle osservazioni di T. Natoli, *Il ruolo delle organizzazioni internazionali nella gestione delle reti digitali globali*, in F. Marcelli, P. Marsocci, M. Pietrangelo (a cura di), "La Rete Internet come spazio di partecipazione politica. Una prospettiva giuridica", Editoriale Scientifica, 2015, p. 116 ss.

[23]Nel corso dei lavori dell'*Internet Governance Forum* di Rio de Janiero del 2007, ad esempio, è stato approfondito l'attuale meccanismo di gestione della radice di Internet indirettamente affidata agli USA per il tramite dell'ICANN.

[24]A. Di Corinto, *Splinternet, la frammentazione della Rete è servita, e dobbiamo preoccuparci*, in "Italian.Tech", 11 giugno 2021.

[25]L'ICANN, costituita il 18 settembre 1998, su impulso del Dipartimento del Commercio degli Stati Uniti d'America, nella forma di un organismo privato, malgrado il riconoscimento di una sfera di autonomia ed indipendenza (avvenuto ad opera dell'*Affirmation of Commitments* del 2009), resta comunque in qualche modo legata al governo americano (anche attraverso un contratto di consulenza rinnovato ogni tre anni). L'ICANN rappresenta l'organismo di vertice della governance di Internet, che esercita la funzione primaria di gestione della radice logica di Internet, mediante la configurazione delle risorse di identificazione (indirizzi IP e nomi di dominio), l'assegnazione e la gestione dei nomi di dominio, degli indirizzi IP e la supervisione dei tredici *root server*, di cui la cd. *root authority* (o *root administration*), contenente il database ufficiale di tutti i Tld registrati, e regola la struttura gerarchica dei nomi di dominio. L'ICANN esercita, pertanto, un rilevante potere di regolamentazione della Rete che manifesta implicazioni formalmente tecniche, ma dal sostanziale contenuto politico. Per un approfondimento: D. De Grazia, *L'Internet Governance tra tecnica, politica e diritto*, in "Informatica e Diritto", 2009, n. 1, pp. 29-45.

[26]Emblematico il caso della Cina, cha ha implementato il cd. "Great Firewall" in grado di controllare l'accesso al cyberspazio nazionale, limitando la fruizione di determinati contenuti veicolati online. P. Banerjee, *How nationalism gave birth to the splinternet*, in "Mint", 18 February 2021.

[27]Cfr. E. Claessen, *Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU*, in "Journal of Cyber Policy", vol. 5, 14 February 2020, n. 1, p. 140-157.

[28]Sulla falsariga del modello cibernetico predisposto dalla Corea del Nord: cfr. J. McCurry, *North Korea only has 28 websites, according to leak of official data*, in "The Guardian", 21 September 2016.

[29]Come prevede, ad esempio, il progetto di riforma predisposto in Russia, recante modifiche alle leggi federali in materia di comunicazioni, tecnologie informatiche e protezione dei dati. In particolare, la *ratio* dell'intervento legislativo mira ad assicurare l'introduzione di misure di protezione finalizzate a garantire il funzionamento stabile di Internet nel rispetto di stringenti regole di instradamento del traffico, mediante una gestione centralizzata dei contenuti per fronteggiare possibili disconnessioni dalla Rete globale in caso di minacce esterne suscettibili di pregiudicare la sicurezza e la stabilità dei servizi essenziali del Paese. Per un approfondimento A. Shcherbovich, *The Russian Bill On Internet Sovereignty Adopted By The State Duma In First Reading*, in "CyberBRICS", 27 February 2019.

[30]Cfr. *Russia Plants Its Flag in the Digital Realm*, in "Worldview", 19 March 2019.

[31]Cfr. *Digital Economy National Program*.

[32]J. Wakefield, *Russia 'successfully tests' its unplugged internet*, in "BBC", 24 December 2019. Si veda anche G. Porro, *La Russia sta facendo passi avanti nella costruzione della sua internet indipendente*, in "Wired.it", 12 aprile 2021.

[33]In attuazione della Strategia per la sicurezza nazionale, che ha recepito la cd. "Information Security Doctrine", la Russia mira a neutralizzare i fattori esterni di destabilizzazione derivanti dalla superiorità tecnologica di alcuni Paesi (come, ad esempio, gli USA), in grado di dominare il cyberspazio, per evitare il rischio di subire un controllo, da parte di forze straniere, sul flusso di informazioni veicolate nello spazio virtuale della Rete. A tal fine, nell'ottica di proteggere l'infrastruttura critica del paese, la Russia ha implementato il funzionamento affidabile di una rete nazionale sovrana completamente isolata per garantire, in caso di minacce esterne, un controllo centralizzato delle risorse digitali attraverso nodi di accesso autorizzati ed elencati in un apposito registro governativo, nel rispetto delle prescrizioni indicate dalla legge "Sovereign internet" n. 608767-7.

[34]Per un approfondimento si veda M. Smeltzer, I. Linzer, *Russian Elections Will Put the Kremlin's Internet Controls to the Test*, in "Freedom House", 14 September 2021.

[35]Si veda lo studio *Splintered Speech - Digital Sovereignty and the Future of the Internet*, in "PEN America".

[36]Cfr. K. O'Hara, W. Hall, *The dream of a global internet is edging towards destruction*, in "Wired.co.uk", 24 December 2019.

[37]S. Hoffman, D. Lazansky, E. Taylor, *Standardising the splinternet: how China's technical standards could fragment the internet*, in "Journal of Cyber Policy", vol. 5, 29 August 2020, n. 2, p. 239-264.

[38]Particolarmente rilevante è l'iniziativa "Internet Plus" con cui la Cina mira a stimolare l'innovazione tecnologica incentivando lo sviluppo di un florido ecosistema nazionale per sostenere la crescita economica del Paese (cfr. Z. Wang, C. Chen, B. Guo, Z. Yu, X. Zhou, *Internet Plus in China*, in "IT Professional", vol. 18, 2016, n. 3, p. 5-8). Pechino ha, inoltre, realizzato il vasto programma internazionale di sviluppo infrastrutturale cd. "Belt and Road Initiative" (anche noto come cd. "via della seta digitale"), che prevede una strategia di esportazione tecnologica del modello di governance digitale cinese mediante il consolidamento di relazioni bilaterali con circa 40 altri Paesi (cfr. A. Chatzky, J. McBride, *China's Massive Belt and Road Initiative*, in "Council on Foreign Relations", 28 January 2020).

[39]Sul tema J.Min, *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, in "SAIS Review of International Affairs", Project MUSE, vol. 30, 2010, n. 2, p. 71-89.

[40]Si riscontra la tendenza a frammentare Internet soprattutto nei regimi autoritari, ove reti nazionalizzate prevedono barriere tecnologiche di blocco anche per reprimere proteste pacifiche di mobilitazione pubblica (cfr. *Report #KeelptOn 2019*, AccessNow, 22 June 2019). Peraltro, la pandemia "Covid-19" ha ulteriormente accentuato il ricorso a svariate forme di li-

mitazione generale della libertà di informazione, giustificando a tal fine la legittimità del controllo statale per la salvaguardia della salute e dell'ordine pubblico (cfr. *COVID-19 Civic Freedom Tracker*, International Center for Not-for-Profit Law, European Center for Not-for-Profit Law).

[41] F. Kenyon, *China's 'splinternet' will create a state-controlled alternative cyberspace*, in "The Guardian", 3 June 2021.

[42] A tal fine, il governo cinese configura la cd. "sovranità informatica" come peculiare paradigma del dominio nazionale fondante l'infrastruttura normativa e tecnologica dello Stato, da cui discendono stringenti poteri di controllo sulle informazioni pubblicate in Rete. Cfr. State Council Information Office of People's Republic of China (SCIO), *Full Text: White paper on the Internet in China*, in "China Daily", 6 August 2010.

[43] Secondo il report *Freedom on the Net 2019*, in Cina, per il quarto anno consecutivo, si registrano le peggiori violazioni della libertà di Internet a causa di livelli di censura "senza precedenti", unitamente alla circolazione di contenuti a "senso unico" di sostegno al regime politico in grado di plasmare il conformismo ideologico di massa orientato a supportare la visione governativa, con il risultato di ridurre sensibilmente il pluralismo informativo soprattutto in relazione alla discussione su argomenti politici, economici e militari ritenuti "sensibili" dal regime.

[44] Il cd. "Great Firewall", noto anche come *Golden Shield Project*, è il progetto di censura e sorveglianza di Internet del governo cinese che, nel perseguire l'obiettivo di incrementare la competitività della Cina secondo standard di sviluppo occidentale, promuove l'uso e la diffusione delle tecnologie come strumenti in grado di stimolare la crescita economica del Paese, evitando però il rischio che l'accesso generalizzato ad Internet possa minare la stabilità politica interna mediante un sistema di filtraggio dei contenuti, reso ancor più efficace – in contrapposizione all'ideologia occidentale – dalla dominante cultura cinese dell'autocensura, alimentata da un pervasivo controllo delle informazioni realizzato con il supporto di volontari reclutati per segnalare contenuti offensivi, oggetto di denunce indirizzate alle forze di polizia. Nel rispetto di quanto previsto da una recente legge in materia di sicurezza informatica che impone la raccolta e la conservazione di tutti i dati personali nel territorio cinese, allo scopo di proteggere i cittadini cinesi da interferenze esterne di governi stranieri, anche le aziende tecnologiche straniere sono tenute ad adeguarsi, per evitare l'interruzione dei propri servizi, alle disposizioni normative vigenti, localizzando obbligatoriamente i prescritti dati su server gestiti da società statali cinesi. Per un approfondimento generale sul tema si rinvia a G.R. Barme, S. Ye, *The Great Firewall of China*, in "Wired.com", 1 June 1997.

[45] Prendendo atto del rilevante impatto delle tecnologie emergenti grazie al progressivo incremento della potenza di calcolo dei sistemi automatizzati, il 12 febbraio 2019, il Parlamento europeo ha approvato la Risoluzione "su una politica industriale europea globale in materia di robotica e intelligenza artificiale", ove si sottolinea la necessità di promuovere una «società supportata dall'intelligenza artificiale e dalla robotica», come fattore indispensabile per migliorare la produttività delle imprese, la crescita economica e il benessere sociale delle persone. Si tratta pertanto di una prioritaria azione di intervento, che richiede la necessaria predisposizione di regole chiare e omogenee, evitando la frammentazione del quadro normativo, per gestire le opportunità e le minacce dell'IA, alla luce degli attacchi informatici che possono mettere in pericolo la sicurezza pubblica e privata, con conseguenti rischi per la democrazia e per la tutela dei diritti fondamentali degli utenti, anche a causa della possibile manipolazione di contenuti personalizzati in grado di provocare distorsioni della percezione della realtà, da cui discendono effetti negativi sulla formazione delle opinioni pubbliche e sulla libertà di scelta delle persone. A tal fine, il 20 ottobre 2020, il Parlamento ha adottato un documento che illustra le coordinate di regolamentazione dell'Unione europea in materia di IA, con l'intento di promuovere l'innovazione, garantire il rispetto degli standard etici ed assicurare la fiducia nell'uso consapevole della tecnologia, mediante l'elaborazione di raccomandazioni volte a sollecitare il potere di iniziativa della Commissione europea, che, il 21 aprile 2021, ha ufficialmente formulato la Proposta di Regolamento del Parlamento europeo e del Consiglio recante regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale).

[46] Al riguardo, l'ultima edizione del report *Automating Society 2020* descrive le prospettive future caratterizzanti lo sviluppo evolutivo dei sistemi decisionali automatizzati, evidenziando rilevanti criticità e aspetti problematici derivanti dalla crescente diffusione di dispositivi e sensori in grado di raccogliere un'enorme quantità di dati processati da algoritmi sempre più sofisticati: cfr. F. Chiusi, S. Fisher, N. Kayser-Bril, M. Spielkamp (eds.), *Automating Society Report 2020*, AlgorithmWatch, October 2020.

[47] Cfr. L. Damiano, L. Franchina, *Cyberwar sulle infrastrutture critiche: i nuovi scenari*, in "Agendadigitale.eu", 29 marzo 2021.

[48] Diventa prioritaria la pianificazione operativa di strategie militari in grado di realizzare il cd. "dominio dell'identità" per finalità antiterroristiche e contro-insurrezionali, mediante la raccolta di un'ingente quantità di dati biometrici per tracciare le persone sospettate di essere una potenziale minaccia per la sicurezza: cfr. M. Hu, *Cautionary tale: The Taliban could get access to Afghans' biometric data collected by the US*, in "Scroll.in", 1 September 2021.

[49] Cfr. *Number of connected IoT devices will surge to 125 billion by 2030*, in "Semiconductor Digest", 2017.

[50] In particolare, l'Unione europea, al fine di proteggersi dalle minacce informatiche provenienti dall'esterno dei suoi confini, collabora con il Servizio europeo per l'azione esterna e gli Stati membri per l'attuazione coordinata di una risposta diplomatica congiunta in caso di attività informatiche dannose, nell'ambito di concrete forme di cooperazione e di dialogo in grado di predisporre misure preventive contro gli attacchi informatici. Parimenti rilevanti risultano, altresì, in materia di difesa nel ciberspazio le attività dell'Agenzia europea per la difesa, nonché dell'ENISA, dell'Europol e della direzione generale della Commissione responsabile dell'industria della difesa: cfr. European Commission, *Cybersecurity Policies*.

[51] Per costruire un'Europa resiliente, verde e digitale, è stata adottata nel 2020 la Strategia UE per la cibersicurezza che (come pilastro chiave del documento *Shaping Europe's Digital Future*, in attuazione del *Recovery Plan for Europe* e della *Strategia per l'Unione della sicurezza 2020-2025*), prevede una serie di interventi legislativi finalizzati a tutelare gli utenti contro il rischio di minacce informatiche. Prendendo atto del crescente aumento del numero di attacchi informatici, l'Unione europea si impegna a realizzare un ecosistema digitale sicuro e tecnologicamente sovrano, mediante l'elaborazione di standard tecnici affidabili definiti nell'ambito di un quadro omogeneo di certificazione unico a presidio delle infrastrutture critiche. A tal fine, la Commissione europea ha anche proposta nel 2020 una revisione della direttiva NIS 2016/1148 sulla sicurezza delle reti e dei sistemi informativi per intensificare la lotta contro la criminalità informatica. Inoltre, nell'ottica di migliorare le capacità esistenti in materia di cibersicurezza, la Commissione europea ha sviluppato la piattaforma *Atlante*, unitamente all'istituzione del *Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza*, con il compito di costruire un'agenda comune per gli investimenti nella sicurezza informatica e decidere le priorità di finanziamento per la ricerca, lo sviluppo e l'implementazione di

soluzioni di sicurezza informatica. In attuazione della strategia dell'UE per la cibersicurezza e della strategia dell'UE per l'Unione della sicurezza, è stata inoltre prevista la costituzione del *Joint Cyber Unit* per garantire una risposta coordinata dell'UE a crisi e incidenti informatici verificabili su larga scala.

[52]Oltre a terra, mare, aria e spazio.

[53]Cfr. Consiglio dell'Unione europea, *Cybersecurity: how the EU tackles cyber threats*.

[54]*Ibidem*.

[55]Più del 90% dei dati provenienti dall'Occidente risulta, infatti, ospitato e custodito negli Stati Uniti d'America, a causa della mancanza di server di raccolta europei. Pertanto, nell'ottica di colmare tale ritardo e attenuare le condizioni di arretratezza tecnologica è stato sviluppato il progetto *Gaia-X*, come infrastruttura di dati fondante un ecosistema digitale aperto, trasparente e sicuro. Peraltro, rispetto al primato economico dei cd. "Colossi del web" (identificati dall'acronimo "GAFA" che comprende, tra le più importanti realtà tecnologiche del mondo, note aziende americane leader nel settore tecnologico), non risultano invece aziende europee classificate nella Top 20 delle migliori imprese "high-tech"; cfr. S. Fleming, *What is digital sovereignty and why is Europe so interested in it?*, in "The European Sting", 16 March 2021.

[56]Cfr. C. Hobbs, *op. cit.*

[57]K. Propp, *Waving the flag of digital sovereignty*, in "New Atlanticist", 11 December 2019.

[58]Per un'analisi esaustiva sul tema della sovranità europea si rinvia a M. Leonard, J. Shapiro, *op. cit.*

[59]Lo studio *PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution* afferma che entro il 2030 l'IA genererà ricavi stimati pari a 15,7 trilioni di dollari, con un aumento del 26% del PIL globale grazie al miglioramento della produttività globale di circa il 40%, mentre il 65% del PIL globale sarà digitalizzato entro il 2022 con una stima di oltre 6,8 trilioni di dollari nel prossimo triennio; cfr. *Idc FutureScape: Worldwide digital transformation 2021 predictions*.

[60]G. Gressel, *Protecting Europe against hybrid threats*, European Council on Foreign Relations, 25 June 2019. In particolare, l'autore ricostruisce la nozione di "minacce ibride" per indicare «l'uso di attori sponsorizzati dallo Stato, ma non ufficialmente affiliati (negabili), che non ricorrono alla violenza fisica [...] Lo scopo delle minacce ibride è costringere l'oggetto di una minaccia a conformarsi agli interessi strategici dell'aggressore», come insidioso pericolo configurabile nell'ambito di una "guerra non lineare", "conflitto asimmetrico" e "sovversione".

[61]L. Cerulus, *Europe raises flags on China's cyber espionage*, in "Politico.eu", 4 ottobre 2018.

[62]La disinformazione online è un fenomeno sempre più dilagante che, a causa della creazione di cd. "bolle di filtro", favorisce la circolazione di fake news con conseguente "polarizzazione ideologica" degli utenti attirati da informazioni (anche se false o distorte) corrispondenti alle proprie convinzioni personali e inconsapevolmente sottoposti a sofisticate tecniche di manipolazione predisposte, anche mediante l'uso di falsi account e bot automatizzati, per "inquinare" il dibattito pubblico. Al riguardo, lo studio *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation*, sottolinea che «rispetto a 48 paesi nel 2018 e 28 paesi nel 2017 [...] in ogni paese, c'è almeno un partito politico o un'agenzia governativa che utilizza i social media per plasmare gli atteggiamenti pubblici a livello nazionale [...] per sopprimere i diritti umani fondamentali, screditare gli oppositori politici e soffocare le opinioni dissenzienti». Il report *Misinformation Review* mette in evidenza gli effetti della cd. "infodemia" nella diffusione di informazioni false e fuorvianti pubblicate sui social network per manipolare l'opinione pubblica (A. Bridgman, E. Merkley, P.J. Loewen, T. Owen, D. Ruths, L. Teichmann, O. Zhilin, *The causes and consequences of COVID-19 misperceptions: Understanding the role of news and social media*, in "The Harvard Kennedy School Misinformation Review", vol. 1, 18 June 2020, n. 3, Special Issue on *COVID-19 and Misinformation*).

[63]La ricerca *Survey on the Future of Democracy in the Digital Age* prospetta un progressivo peggioramento del sistema politico democratico entro il 2030 a causa dell'uso strategico dei social media utilizzati per veicolare disinformazione in grado di minare la fiducia delle persone nei confronti delle istituzioni, esponendo inoltre gli utenti al rischio di violazioni della privacy, nonché a forme svariate di controllo realizzato da sistemi massivi di sorveglianza e censura per scopi politici.

[64]Si pensi alla regolamentazione vigente in materia di protezione dei dati, sicurezza informatica e antitrust, oltre al recente intervento normativo realizzato nel settore dell'Intelligenza Artificiale. Sul tema si rinvia a A. Grotto, M. Schallbruch, *The Great Anti-China Tech Alliance*, in "Foreign Policy", 16 September 2019.

[65]Secondo l'analisi di C. Hobbs, *op. cit.* Si veda anche F. Gueham, *Digital sovereignty - steps towards a new system of internet governance*, Fondation pour l'innovation politique, February 2017.

[66]Definita sulla base delle indicazioni formalizzate nel *Rapporto finale* del Working Group on Internet Governance, June 2005.

[67]L'IGF, convocato per la prima volta nel 2006 ad Atene, è giunto alla sua 16ma edizione che si è recentemente svolta a Katowice dal 6 al 10 dicembre 2021.

[68]Cfr. *Tunis Agenda for the Information Society*, cit., p. 73. Nel rispetto del mandato delineato dall'Agenda di Tunisi nel 2005, l'IGF è stato rinnovato per 5 anni nel 2010 (2011-2015) e nel 2015 per altri 10 anni (2016-2025): cfr. revisione WSIS + 10 attuata dalla Risoluzione ONU 68/198 del 20 dicembre 2013, tenuto conto delle modalità di attuazione dei risultati indicati in occasione del vertice mondiale sulla Società dell'Informazione di cui alla Risoluzione ONU 68/31 del 31 luglio 2014.

[69]Nel tentativo di realizzare un sistema più "statalista" di governance di Internet, è stata costituita nel 2001, da Cina, Kazakistan, Kirghizistan, Russia, Tagikistan e Uzbekistan, l'Organizzazione internazionale per la cooperazione di Shanghai, creata nel 2001 come modello alternativo di governo digitale, fondato sul diritto sovrano degli Stati nazionali, osteggiato dagli USA e dall'UE. Si veda S. McKune, *An Analysis of the International Code of Conduct for Information Security*, in "The Citizen Lab", 28 September 2015.

[70]Nel rispetto della metodologia applicativa indicata nel documento *A Toolkit to assist communities in establishing the IGF initiatives* che descrive i requisiti di base per realizzare un'iniziativa IGF in conformità ai principi fondamentali di inclusività, apertura, trasparenza e multi-partecipazione, al fine di facilitare lo scambio di idee e opinioni.

[71]Su tali problematiche L. Abba, *Carenze attuali e soluzioni future nei meccanismi per la cooperazione digitale*, in questa Rivista, 2021, n. 1, delinea le future prospettive dell'ecosistema digitale emerse in occasione della pubblicazione, da parte delle Nazioni Unite, della *Road map for digital cooperation* alla luce delle criticità riscontrate negli attuali meccanismi intergovernativi adottati a livello internazionale.

[72]I cd. "Colossi del Web" stanno dimostrando indiscutibili capacità imprenditoriali orientate alla massimizzazione del profitto in grado di realizzare un costante incremento del fatturato aziendale grazie all'implementazione di servizi e strumenti, in regime di strapotere tecnologico (resi ancor più indispensabili, nello svolgimento della maggior parte delle attività quotidiane, dalla situazione emergenziale della pandemia "Covid-19"). Al contempo, però, essi manifestano anche un'inclinazione "politica" che potrebbe entrare presto in rotta di

collisione con la visione "tecno-nazionalistica" – spesso conservativa e poco lungimirante – degli apparati statali nella ricerca di soluzioni regolatorie del cyberspazio. Non a caso, rispetto al tradizionale approccio *soft-law*, ricognitivo di un atteggiamento neutrale a lungo manifestato dai governi nei confronti delle grandi aziende digitali, cominciano ora ad intensificarsi le "tensioni" tra i contrapposti "players". Ad esempio, negli USA, contestualmente alle indagini antitrust avviate dalla Federal Trade Commission per limitare il potere monopolistico detenuto dalle "Big Tech" come necessaria misura correttiva proconcorrenziale in grado di stimolare l'innovazione nell'economia digitale, l'amministrazione Biden ha più volte annunciato l'avvio di un'organica riforma della Sezione 230 del "Communications Decency Act" del 1996 che, per favorire la libertà di innovazione a tutela dello spazio "autarchico" di Internet, garantisce agli intermediari telematici un esonero di responsabilità dalle conseguenze dannose, riconoscendo uno specifico "scudo legale" di immunità contro il rischio di pubblicazione di contenuti illeciti online immessi dagli utenti terzi. Nella stessa direzione si sta muovendo il governo in Cina, ove si registra un accentuato interventismo legislativo motivato dalla necessità di salvaguardare inderogabili esigenze di stabilità politica e di sicurezza nazionale nella gestione centralizzata dei dati e nel controllo del flusso comunicativo veicolato online. Pertanto, dopo un'iniziale fase di tendenziale libertà imprenditoriale generalmente riconosciuta in assenza di sostanziali restrizioni, come precisa scelta strategica di accelerazione espansionistica del proprio modello capitalistico, le autorità cinesi, in un mutato clima più ostile ai comportamenti anticoncorrenziali, hanno multato il gigante di Internet Alibaba per pratiche anticoncorrenziali in conseguenza della violazione della legge antimonopolio, contestualmente all'adozione di un provvedimento inibitorio volto alla revisione della governance delle controllate della holding societaria. Anche in Europa sono in corso riforme legislative dirette a contenere lo strapotere delle imprese "high-tech" in un'ottica di liberalizzazione dei mercati, come si evince dal "pacchetto" *Digital Services Act* e *Digital Markets Act*, al pari della Direttiva UE "Copyright" 2019/790, sino alla recente proposta di Regolamento europeo in materia di Intelligenza Artificiale, caratterizzata dalla medesima *ratio* applicativa. Sul tema, A. Alù, *Stati contro le big tech: siamo allo scontro finale? La linea dura di Ue, Usa e Cina*, cit.

[73]Pur nell'ottica di migliorare il processo decisionale dell'IGF, rendendolo più efficace e incidente nella formulazione delle proposte che emergono all'esito dei relativi lavori, l'istituzione di una sorta di "Leadership Panel", come organismo multistakeholder di "alto livello", è stata duramente contestata da alcune organizzazioni della società civile che, contrarie alla formazione di tale gruppo, hanno chiesto di boicottarne la relativa procedura di nomina, per evitare di alterare le originarie caratteristiche fondanti il *forum*, mediante la creazione di speciali categorie di attori differenziati per "status", al punto da compromettere la partecipazione "bottom-up" del *meeting*; cfr. M. Mueller, *Civil Society Groups Resist IGF "Leadership Panel"*, Internet Governance Project, 26 November 2021.

[74]Prendendo atto del declino degli attuali processi internazionali esistenti, di fronte alle sfide che la cooperazione geopolitica della Rete pone, il rapporto *The Open Internet on the Brink: Recommendations for a Future Model*, prospetta una possibile riforma della governance di Internet. A tal fine, si prevede la creazione di una sorta di "Nato per Internet", come vera e propria "Alleanza per le infrastrutture e la difesa digitale", con il compito di valutare e orientare lo stato di salute dell'ecosistema digitale, delineando un nuovo modello di "internazionalismo" su Internet, caratterizzato da un maggiore e più accentuato coinvolgimento politico dei governi nazionali in grado di contrapporsi alla visione "nazionalistica" della Rete frammentata sostenuta da alcuni Stati.

[75]Sul tema, J. Pohle, T. Thiel, *Digital sovereignty*, in "Internet Policy Review", vol. 9, 17 December 2020, n. 4.

[76]A. Grotto, M. Schallbruch, *op. cit.*

[77]Secondo l'autorevole analisi di C. Hobbs, *op. cit.* L'autore, in particolare, individua l'esistenza di una rete "Internet statunitense" di matrice imprenditoriale costituita dal complesso di regole stabilite dalle principali società che forniscono i servizi digitali utilizzati in tutto il mondo; una "Internet cinese", come rete di riferimento per i governi autoritari, controllata a livello nazionale da Pechino, funzionale al perseguimento degli interessi generali dello Stato mediante un sistema integrale di sorveglianza massiva; e una "Internet europea" dalla configurazione più spiccatamente democratica, orientata alla promozione proattiva della concorrenza nella regolamentazione dei mercati digitali e alla protezione dei diritti dei consumatori/utenti/fruitori dei servizi telematici.

[78]Cfr. J.P. Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation, 8 February 1996.

[79]Cfr. A. Chander, *The Racist Algorithm?*, in "Michigan Law Review", vol. 115, 2017, n. 6; I. Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, in "Cardozo Law Review", vol. 41, 10 March 2016, n. 5.

[80]Sul tema sia consentito rinviare ad A. Alù, *Algoritmi che incitano all'odio? Così i video alterano le opinioni e amplificano la violenza*, in "Agendadigitale.eu", 6 maggio 2021.

[81]Si veda A. Alù, *Disinformazione social, Facebook distratta e i regimi se ne approfittano*, in "Agendadigitale.eu", 19 aprile 2021.

[82]Si rinvia all'analisi del rapporto *Splintered Speech - Digital Sovereignty and the Future of the Internet*, cit.

[83]H. Farrell, M. Levi, T. O'Reilly, *Mark Zuckerberg runs a nation-state, and he's the king*, in "Vox.com", 10 April 2018.

[84]Sul tema, E. Guo, *Facebook is now officially too powerful, says the US government*, in "MIT Technology Review", 9 December 2020.

[85]Si veda V.M. Schönberger, K. Cukier, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere. E già minaccia la nostra libertà*, Garzanti, 2013.

[86]Per un approfondimento R. Berman, Z. Katona, *Curation Algorithms and Filter Bubbles in Social Networks*, NET Institute Working Paper No. 16-08, 21 September 2019; E. Pariser, *Il Filtro. Quello che Internet ci nasconde*, Il Saggiatore, 2012.

[87]Emblematica, in tal senso, come peculiare manifestazione del nuovo prospettato sistema di governance, è la creazione, promossa da Facebook, di un'inedita struttura, denominata *Oversight Board*, presentata come una sorta di "Corte Suprema" (composta da 20 "giudici" - tra cui un ex Primo Ministro danese e un vincitore del Premio Nobel per la Pace – dotati di un *mix* diversificato di competenze specialistiche, con maggiore preminenza di cultura giuridica e istituzionale), molto simile al tradizionale modello dei tribunali. L'*Oversight Board* opera, infatti, come un organo giudicante indipendente, al quale gli utenti possono appellarsi in casi di controversie che riguardano la cancellazione di profili e post ritenuti ingiusti, per ottenere decisioni "definitive" e "vincolanti" sui contenuti consentiti e/o rimossi. Si tratta, pertanto, di un'iniziativa senza precedenti realizzata da un'impresa privata che sembra dotarsi di organi "para-giurisdizionali" sulla falsariga della tipica tripartizione dei poteri che caratterizza un ordinamento statale (cfr. A. Alù, *Oversight board di Facebook alla prima prova: così si disvela il suo ruolo*, in "Agendadigitale.eu", 1 febbraio 2021). Parimenti singolare risulta il progetto *Metaverso*, presentato in occasione dell'annuncio di Zuckerberg sulla ridenominazione della holding societaria, con l'obiettivo di realizzare una nuova versione di Internet, fondata sull'integrazione tra mondo fisico e digitale, come ambiente ibrido di interazioni reali

tra persone che – nella veste di "avatar" – lavorano, giocano, sviluppano relazioni interpersonali, incontrandosi secondo le dinamiche "normali" della vita quotidiana. Il sistema *Metaverso* sembra, invero, delimitare i confini virtuali di uno nuovo spazio "cyber-sovrano" popolato da quasi 3 miliardi di utenti sottoposti al rispetto delle regole prescritte dalla piattaforma che tende ad assumere le caratteristiche tipiche di uno "Stato digitale" (cfr. A. Alù, *Perché il Metaverso potrebbe (davvero) essere la nuova "internet revolution"*, in "Agendadigitale.eu", 2 novembre 2021).

* * *

Internet Governance beyond the States? The unprecedented traits of the future digital ecosystem

Abstract: The essay identifies the main questions that the future digital ecosystem poses, describing the phenomenon of Internet fragmentation as one of the most complex and problematic aspects that emerges in the current geopolitical scenery, where the tendency of States to elaborate "techno-nationalistic" aimed at the construction of an autonomous and independent network, technologically different from the original distributed and interoperable architecture on which the traditional operating model of the global Internet is based. In fact, various regulatory interventions proliferate in the global panorama that require the massive use of general surveillance tools to ensure centralized control of the Internet, as a strategic priority objective of technological supremacy established to protect the critical infrastructures of the States, to avoid the risk of possible external attacks capable of destabilizing the internal order. With respect to the progressive balkanization of the Internet, the economic and political power of the "Big Tech" in the guise of new dominant "players" is strengthening as an unexpected variable of the changed Internet ecosystem.

Keywords: Internet Governance – Internet fragmentation – Big-Tech – Splinternet – Digital sovereignty