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

Sulla governance di Internet

di Vinton G. Cerf

Traduzione a cura di Laura Abba, CNR

La versione originale in lingua inglese, dal titolo "On Internet Governance", è stata pubblicata il 16 febbraio 2022 in apertura del numero speciale della Rivista italiana di informatica e diritto (RIID) dedicato a La Internet governance e le sfide della trasformazione digitale. La RIID è edita dal CNR – Istituto di Informatica Giuridica e Sistemi Giudiziari.

Il saggio analizza la complessa sfida di introdurre misure di governance volte a preservare l'efficienza del sistema Internet e garantire la sicurezza dei cittadini, sanzionando coloro che approfittano delle possibilità offerte dall'accesso a Internet per commettere abusi.

Vinton G. Cerf, Vice Presidente e Chief Internet Evangelist di Google, conosciuto come uno dei "Fathers of the Internet", è lo studioso americano co-designer del protocollo TCP/IP e dell'architettura iniziale di Internet. Con il suo lavoro, ha completamente rivoluzionato la trasmissione delle informazioni consentendone il flusso illimitato in tutto il mondo.

Si ringrazia l'autore per aver acconsentito a pubblicare questa traduzione.

1. Introduzione

Cosa intendiamo quando parliamo di "Internet Governance"?

All'inizio del terzo decennio del XXI secolo ci troviamo coinvolti in una pandemia globale. Tra le tante lezioni tratte da questa intensa esperienza, abbiamo scoperto che la rete Internet gioca un ruolo fondamentale per gran parte di circa il 60% della popolazione mondiale che ad essa ha accesso. Naturalmente, la qualità, il costo e l'affidabilità dell'accesso ai servizi della rete variano di paese in paese e ci sono aree del mondo dove l'accesso è scarso o inefficiente. Tuttavia, i benefici della Rete sono stati evidenti, soprattutto per coloro che hanno potuto lavorare da remoto e ottenere, attraverso essa, accesso alle informazioni. L'accesso a Internet ha favorito la collaborazione scientifica, accelerando lo sviluppo dei vaccini contro il virus SARS-COV-2, che ha diffuso l'infezione da COVID-19.

Le potenzialità di Internet e delle applicazioni che sono state sviluppate utilizzando la piattaforma del World Wide Web che opera attraverso Internet hanno incrementato la consapevolezza dei governi, del settore privato, del mondo accademico e dell'opinione pubblica non solo sui possibili benefici ma anche sui rischi che tale sistema comporta. L'ottimismo dei primi giorni di Internet e del World Wide Web ha lasciato il passo alla presa d'atto che persone che non hanno a cuore l'interesse generale possano abusare e già abusino di questo potente insieme di tecnologie. Con l'avvento dei *social media*, come Facebook, Twitter, Tik-Tok e YouTube, è emersa la possibilità di aggregare gruppi di persone, sia su scala globale che locale. Più in generale queste nuove piattaforme tecnologiche hanno notevolmente favorito la proliferazione di canali di informazione, trascurando però la qualità dei contenuti diffusi. I possibili usi scorretti di Internet sono aumentati e diventati sia più visibili che potenzialmente più dannosi (si pensi ai ransomware e ai malware distruttivi, alla disinformazione e alla misinformazione, al phishing e allo spam), al punto da indurre i governi a considerare necessario un qualche tipo di intervento di regolazione, sorretto da procedure sanzionatorie.

È in questo contesto che questo lavoro si propone di analizzare la complessa sfida di introdurre misure di governance volte a preservare l'efficienza del sistema Internet e garantire la sicurezza dei cittadini, sanzionando coloro che approfittano delle possibilità offerte dall'accesso a Internet per commettere abusi.

2. La prospettiva tecnica

È importante che le parti interessate alla governance di Internet comprendano i diversi livelli su cui si basa Internet (incluso il World Wide Web), perché i diversi interventi di governance possibili variano a seconda del livello in cui emergono le questioni che richiedono una regolamentazione.

Internet è progettata come un sistema a strati. Gli strati inferiori della sua implementazione definiscono le modalità di trasporto fisico dei contenuti digitali, basato sulla tecnologia della *commutazione di pacchetto*. Possiamo, in tal senso, immaginare, per comprenderne il funzionamento, l'uso di cartoline postali elettroniche che hanno alcuni contenuti da trasmettere e gli indirizzi del *mittente* e del *destinatario*. I pacchetti Internet, come le cartoline, non sanno con quale mezzo vengono trasportati. Potrebbero viaggiare su fili, cavi coassiali, fibre ottiche, radio e canali satellitari. Inoltre i pacchetti Internet, come le cartoline, non conoscono quali contenuti stanno trasportando. Questa "ignoranza" è in realtà un elemento di vantaggio del sistema. Quando si sviluppano nuove tecnologie di trasmissione, è possibile utilizzarle facilmente per trasportare i pacchetti digitali di Internet.

Inoltre, se viene sviluppata una nuova applicazione che ha bisogno di interpretare la parte di dati trasmessi destinata all'utente (si pensi alle cose scritte sulla cartolina), per la rete nulla cambia perché essa non discrimina fra le applicazioni. Dal momento che questo meccanismo produce una rete c.d. "best efforts" ["che fa del suo meglio"], piuttosto che una rete dedicata esclusivamente ad applicazioni specifiche, Internet è stata in grado di adattarsi ad un numero considerevole di applicazioni, come la *posta elettronica*, l'*accesso remoto a computer condivisi*, lo *streaming audio e video*, le *video conferenze*, i *(video)giochi in tempo reale*, il *controllo remoto dei dispositivi* (si pensi all'*Internet delle cose* - IOT) e una miriade di altre.

È importante avere chiaro che la rete Internet non coincide né con il World Wide Web né con tutte le applicazioni che la utilizzano. Allo scopo di questo lavoro si può fare riferimento a Internet come il sistema di trasporto che sposta i pacchetti di dati dal punto di origine alla destinazione. Esistono numerosi *protocolli* (si pensi alle prassi, alle procedure, ai formati standard dei dati) che consentono a Internet di spostare i pacchetti. Diversi *protocolli principali* costituiscono l'Internet di base. Si tratta dell'Internet Protocol (IP), del Transmission Control Protocol (TCP) e dell'User Datagram Protocol (UDP). Si può descrivere l'IP come un tradizionale servizio postale. I pacchetti IP hanno indirizzi numerici per tutti i punti di origine e le destinazioni presenti in Internet e un metodo per trovare i percorsi dal punto di origine alla destinazione. Il TCP assicura che tutte le cartoline vengano consegnate interamente e in ordine, introducendo uno strato sopra il protocollo IP per raggiungere tali obiettivi. Si occupa di riordinare i pacchetti che potrebbero arrivare fuori posto, di ritrasmettere quelli che potrebbero sembrare persi, di filtrare i pacchetti duplicati e di gestire il flusso del traffico per evitare che il destinatario riceva un carico eccessivo. Il protocollo UDP dà accesso al trasporto a basso ritardo su IP senza svolgere le specifiche funzioni del protocollo TCP. Pertanto, i pacchetti dati trasmessi tramite UDP possono arrivare più velocemente (con più bassa latenza) ma con il rischio che arrivino in maniera disordinata e duplicata. L'insieme dei protocolli che costituiscono l'Internet di base è comunemente chiamato *suite di protocolli TCP/IP*. Include altri protocolli come quelli che regolano l'instradamento (*routing*) del traffico attraverso la rete globale, la crittografia dei pacchetti per garantire la riservatezza, la traduzione dei nomi a dominio (ad esempio: cnr.it) in indirizzi IP.

Per l'implementazione delle applicazioni che utilizzano Internet esistono altri protocolli. L'accesso remoto a computer e data center in time-sharing, il trasporto di posta elettronica, il trasporto di file e lo streaming audio e video sono esempi di applicazioni che usano Internet. Il World Wide Web è implementato con un proprio insieme di protocolli (*Hypertext Transport Protocol* - HTTP e *Hypertext Markup Language* - HTML) che rappresenta uno strato che opera al disopra del TCP/IP.

Un rilevante momento di innovazione per lo sviluppo delle applicazioni in rete è stato l'introduzione dell'*iPhone* di Apple nel 2007, che ha portato alla creazione di milioni di applicazioni per gli smartphone da parte di diversi fornitori. Gli sviluppatori di queste applicazioni devono soltanto conoscere le condizioni con cui gli smartphone accettano e forniscono dati attraverso le API (*Application Programming Interfaces*) senza preoccuparsi di tutti i dettagli di come avviene concretamente la trasmissione dei dati e della voce, via etere e attraverso reti in fibra. Lo smartphone ha reso Internet più accessibile e Internet ha reso lo smartphone più

utile. È sempre più vero che gli smartphone sono essenzialmente da considerare *endpoint* [nodo della Rete] secondo i protocolli di Internet e sono direttamente raggiungibili tramite i protocolli TCP/IP e UDP. Le applicazioni che si trovano sugli smartphone sono sempre più strumenti di accesso a server Web distribuiti nei data center di tutto il mondo. La comunicazione vocale sta rapidamente diventando *Voice over IP* (VOIP) rispetto alla precedente configurazione analogica a commutazione di circuito del passato. Ciò vale anche per le reti telefoniche tradizionali che hanno abbandonato la *commutazione di circuito in favore della commutazione di pacchetto* che ha costi minori e risulta più flessibile.

È anche fondamentale riconoscere che Internet è stata progettata per essere espandibile. Si tratta di una *Rete di reti* progettata per consentire l'interconnessione di un numero indeterminatamente alto di reti. Ogni rete è gestita indipendentemente dalle altre, ma tutte seguono gli stessi protocolli standard in modo da ottenere l'interoperabilità tra tutte. Qualsiasi cosa, ovunque su Internet, può comunicare con qualsiasi altra cosa su Internet, indipendentemente dalle reti componenti a cui sono collegati i dispositivi di origine e di destinazione.

3. La prospettiva organizzativa

Così come è importante conoscere il funzionamento della infrastruttura tecnica di Internet e del World Wide Web, allo stesso modo è rilevante comprendere il ruolo delle organizzazioni nella implementazione e nella operazione della rete. Ad esempio, sono attori chiave del sistema Internet i fornitori che, via cavo e attraverso la fibra, portano i servizi Internet nelle case, nelle aziende, nelle istituzioni e negli uffici pubblici. Del pari, i fornitori di servizi wireless fanno la stessa cosa via etere. Altri forniscono il servizio di cavi sottomarini che collegano parti della rete Internet intorno al mondo.

Rientrano tra gli attori del sistema anche i produttori di *router*, che implementano il sistema IP di interconnessione di rete, o di smartphone. L'Internet delle cose (*Internet of Things* - IOT) si riferisce a un numero crescente di dispositivi, pronti per essere connessi a Internet, realizzati da produttori che desiderano sfruttare la connettività globale per fornire agli utenti apparecchi ed eventualmente servizi correlati, come il monitoraggio o l'aggiornamento software. Altri ancora producono risolutori dei nomi di dominio e server per tradurre i nomi di dominio in indirizzi IP. Aziende come Apple, Microsoft e Google realizzano sistemi operativi come OSX, IOS, Windows o Android utilizzati in molti smartphone, tablet, laptop e dispositivi IOT.

Oltre alle organizzazioni e alle aziende che producono dispositivi che rendono possibile la connessione o che possono connettersi ad Internet, esistono, come già accennato, i fornitori di servizi Internet (*Internet service providers* - ISPs) che forniscono l'accesso a Internet. Si tratta di servizi per telefoni cellulari, servizi via fibra e via cavo e servizi forniti da satelliti in orbita terrestre bassa, media e geostazionaria. Altre organizzazioni gestiscono gli *Internet Exchange Point* (punti di interscambio) che permettono l'interconnessione efficiente delle molte reti che compongono Internet. Nella maggior parte dei casi, questi operatori si concentrano solo sulla consegna dei pacchetti Internet e non sull'interpretazione dei contenuti, tranne che nel caso in cui essi siano parte del sistema di controllo operativo di Internet, come, ad esempio, del sistema di instradamento BGP (*Border Gateway Protocol*).

Le "Società Piattaforma" come Google, Facebook, Microsoft, Amazon, IBM e altre gestiscono diversi *data center* distribuiti in tutto il mondo, interconnessi spesso da reti private in fibra che sono, a loro volta, connesse all'Internet pubblica. Queste piattaforme ospitano una parte significativa dei servizi Internet e basati sul Web. Inoltre, esistono aziende, come Akamai, che gestiscono le c.d. Reti per la consegna di contenuti (*Content Distribution Networks* - CDN), che forniscono contenuti attraverso server che sono collocati vicino agli utenti finali, nelle centrali telefoniche o nelle vicinanze di un *Internet Exchange Point* (punto di interscambio).

Innumerevoli aziende producono software applicativi che funzionano nei vari data center o CDN per servire gli utenti di queste applicazioni. Altre, come Netflix e Amazon e i tradizionali produttori cinematografici, creano contenuti che vengono distribuiti in streaming sul World Wide Web. Le banche forniscono servizi finanziari e milioni di altre aziende creano siti web per servire i loro clienti. La pubblicità è una componente importante dell'Internet del XXI secolo, con aziende della rete che offrono servizi gratuiti agli utenti in cambio della presentazione di messaggi pubblicitari, pagati da aziende che desiderano offrire prodotti e servizi al grande pubblico.

Esiste, poi, tutto un altro tipo di organizzazioni che sono legate più strettamente alle tecnologie di Internet. Alcune creano e mantengono gli standard tecnici per Internet, tra cui l'*Internet Engineering Task Force* (IETF) sponsorizzata dalla *Internet Society*; il *World Wide Web Consortium* (W3C) per gli standard Web;

l'Organizzazione internazionale per la Normazione (ISO), il 3GPP (per gli standard delle applicazioni *mobile*), l'Unione internazionale delle Telecomunicazioni (ITU) e i suoi organismi di normazione ITU-R (radio) e ITU-T (telecomunicazioni) e l'*Institute of Electrical and Electronics Engineers* (IEEE) insieme a vari organismi nazionali come il *British Standards Institution* (BSI), l'*American National Institute of Standards and Technology* (NIST), l'*European Telecommunications Standards Institute* (ETSI) e l'Ente nazionale italiano di unificazione (UNI).

È importante riconoscere nel contesto della governance che ci sono molti soggetti che si occupano del "codice della strada" sia di Internet sia del WWW. Fra questi vi sono anche organizzazioni della società civile e la comunità accademica oltre ai governi e le amministrazioni pubbliche a tutti i livelli. È per questo motivo che il principio della "Governance Multistakeholder di Internet" ha rappresentato un filo conduttore nella storia di Internet e del Web. Esiste un numero enorme di soggetti interessati, soggetti che hanno il potere di sviluppare ed attuare norme e regolamenti e soggetti che sono destinatari degli effetti prodotti dalle regole adottate.

4. La Governance di Internet

Veniamo ora al punto centrale di questo saggio: come deve essere attuata la governance di Internet con l'obiettivo di preservare l'enorme valore che il libero flusso di informazioni ha avuto nei decenni di funzionamento di Internet (dal 1983) e del World Wide Web (dal 1991). L'approccio "multistakeholder" per lo sviluppo delle *policy* di Internet – che coinvolge i governi, la società civile, le comunità scientifiche, le organizzazioni degli standard e il settore privato – rimane la migliore soluzione auspicabile che permette di tenere conto dei vari punti di vista – nella definizione delle policy, dei regolamenti e dei metodi di applicazione delle norme – e di verificare le potenziali ricadute nei vari settori.

Mentre l'applicazione delle politiche può ricadere su un gruppo più ristretto di attori, uno sviluppo delle policy informato da un gruppo più ampio è stato vantaggioso per l'Internet ed il World Wide Web nel corso della loro evoluzione.

C'è una urgente necessità di applicare il principio di *sussidiarietà*. Cioè, applicare meccanismi di regolamentazione ai livelli di volta in volta adeguati tenuto conto degli attori che prendono parte all'ecosistema Internet. Ad esempio, una frammentazione dell'infrastruttura Internet di base a favore della cosiddetta "sovranità dei dati" minaccia il libero flusso di informazioni a livello globale. Il valore di questo libero flusso è vitale per la condivisione e la ricerca di informazioni a beneficio di tutti. Se la protezione delle informazioni è di rilievo prioritario, e lo è per molti ambiti, compresi i *dati personali*, si può fare uso di mezzi crittografici sia per la protezione delle informazioni, in transito e memorizzate, che per forme di autenticazione forte degli utenti per consentire l'accesso alle informazioni sensibili solo a chi è autorizzato. Non è necessario confinare le informazioni in specifiche aree geografiche per ottenere questo effetto. Una geo-frammentazione parcellizzata di Internet ha conseguenze negative tra cui l'impossibilità di replicare i dati in diversi data center per evitarne la perdita anche in caso di guasti catastrofici.

Se un contenuto è inaccettabile in determinati contesti, l'azione di inibirne l'accesso bloccando Internet a livello di indirizzi IP è un meccanismo estremamente brutale. Lo stesso può dirsi per il blocco dei nomi a dominio. Ragionando per analogia, se qualcuno vende droghe illegalmente in un appartamento, arrestare tutti gli occupanti del medesimo edificio penalizza molte persone innocenti. In presenza di contenuti considerati assolutamente inaccettabili, come il materiale pedopornografico, è da esigere la rimozione dai server che li ospitano. Naturalmente, poiché Internet e il Web sono globali, la rimozione potrebbe richiedere la cooperazione dei governi nazionali, come previsto dalle proposte in materia di "Cooperazione digitale" del Segretario generale delle Nazioni Unite. In assenza di cooperazione, i governi nazionali potrebbero scegliere di applicare strumenti molto più brutali.

È certamente utile per i soggetti chiamati a definirne le regole avere una conoscenza completa della struttura stratificata di Internet e del World Wide Web ed essere in grado di valutare la diversità dell'ecosistema della rete. L'applicazione delle politiche secondo meccanismi che consentano di riconoscere lo specifico ruolo dei soggetti presenti nel sistema può preservare i vantaggi di Internet in larga misura, determinando una regolamentazione adeguata. Vale la pena riconoscere che molte delle organizzazioni che popolano l'ecosistema della rete svolgono più ruoli. Alcune hanno componenti verticali che dovrebbero essere viste da una prospettiva che rispecchi la struttura stratificata della rete quando si valutano possibili risposte normative a problemi di governance.

5. Postilla

In questo breve saggio, non ho voluto affrontare alcuni problemi davvero seri come i malware, gli attacchi di denial of service (negazione del servizio), la diffusione della disinformazione (veicolata in rete con o senza dolo), gli effetti nocivi dei social network, il ruolo del pubblico e degli utenti nel difendersi da rischi e danni. Sembra tuttavia utile richiamare l'attenzione su alcune di queste questioni, per quanto sinteticamente. Gli utenti devono essere alfabetizzati sui potenziali pericoli della *vita online*. Devono disporre di strumenti di protezione come l'autenticazione a due fattori in aggiunta ai loro nomi utente e password. Devono essere in grado di rilevare probabili attacchi di *phishing*. Devono evitare di scaricare file e software da fonti discutibili. Devono evitare di fare clic sui collegamenti ipertestuali senza valutarne con spirito critico origini e scopi.

Lo sviluppo del software open source, da un lato, costituisce un vantaggio per i programmatori, ma, dall'altro lato, configura un grave pericolo perché si sottovaluta un'attenta valutazione del software presupponendo che "tutti i bug sono stati trovati". Purtroppo, più spesso ci troviamo nella situazione in cui "nessun bug è stato individuato". C'è un esempio recente: il bug *Log4J* che consente l'esecuzione da remoto di codice sul computer dell'utente infetto. Probabilmente si tratta di una delle vulnerabilità più pericolose degli ultimi decenni, in quanto il bug colpisce la libreria Log4j, estremamente diffusa. Gli attacchi alla *catena di approvvigionamento* che colpiscono software critici prodotti da piccole aziende non ben preparate a difendersi dalla intrusione e dall'alterazione dei loro prodotti hanno portato a conseguenze molto gravi sia per le aziende sia per i consumatori. Gli attacchi *ransomware* hanno avuto effetti collaterali a cascata come il quasi blocco del commercio sulla costa orientale degli Stati Uniti a causa della mancanza di carburante quando il sistema di oleodotti per prodotti petroliferi [Colonial Pipeline] è stato colpito da un attacco.

A causa del nostro zelo nell'identificare e autenticare gli utenti, è possibile creare massicce raccolte di dati biologici (volti, impronte digitali, scansioni dell'iride) che sono estremamente attraenti per gli hacker interessati a utilizzare o rivendere questo tipo di informazioni. Man mano che si riconosceranno gli aspetti potenzialmente dannosi dell'utilizzo dei social network, le aziende e i governi si affideranno ai consigli e alle intuizioni di sociologi, psicologi, neuro scienziati e persino di antropologi. Il comportamento umano è complesso ed è in parte determinato dalla fisiologia evolutiva in cui gli stimoli emotivi scatenano reazioni poco razionali (ad esempio lotta o fuga, pensiero veloce e pensiero lento).

Ho dato poco o nessuno spazio alla questione dell'inclusione digitale: rendere Internet accessibile (in entrambi i sensi), disponibile, conveniente, affidabile, sicura, protetta, in grado di garantire la privacy per tutti sul pianeta. Ci sono molti ostacoli al raggiungimento dell'accesso globale e anche questi aspetti meritano attenzione per quello che riguarda la governance, anche se non hanno ricevuto un trattamento adeguato in questo breve saggio.

Ma non c'è dubbio che una conferma significativa della via da seguire sia quella di occuparci dei potenziali rischi che corriamo usando computer e applicazioni in rete, e credo fermamente che dobbiamo essere consapevoli del rischio di perdere gran parte dei benefici attuali se non diventiamo consapevoli della complessità dell'ecosistema che abbiamo creato, della sua struttura e degli attori coinvolti.