DOPPIOZERO

L’Internet “delle cose” darà ancora spazio all’umano?

Francesca Musiani

24 Novembre 2021

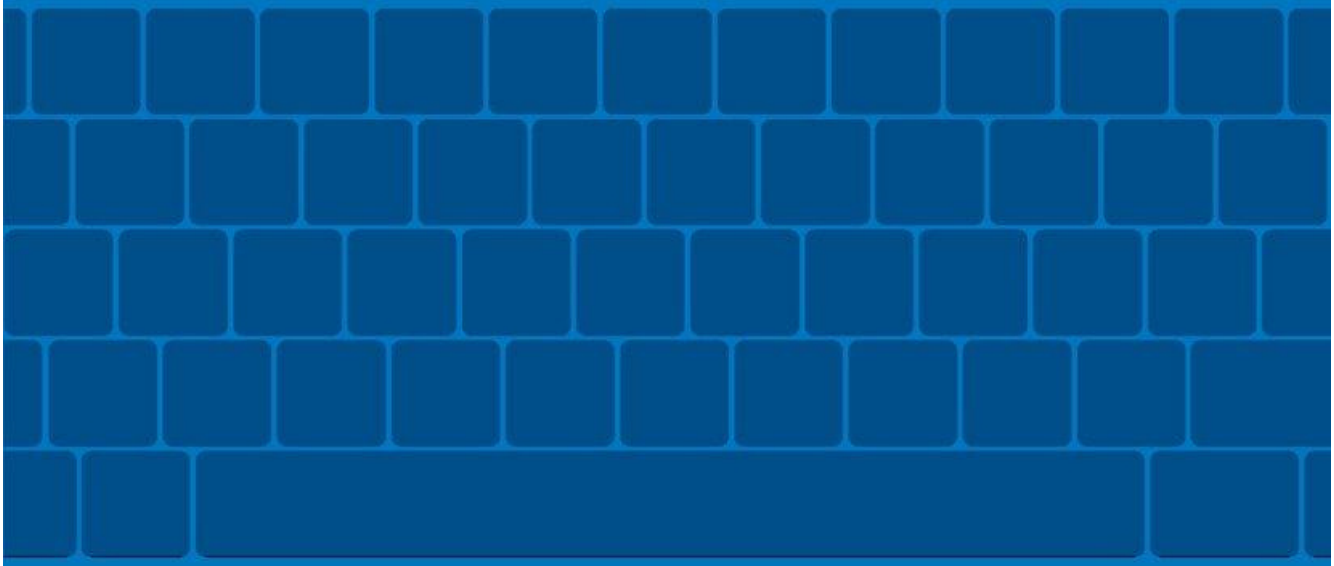
In *Internet in Ogni Cosa: Libertà, Sicurezza e Privacy nell’Era degli Oggetti Iperconnessi* (trad. it. di A. D, Signorelli, LUISS University Press, 202), Laura DeNardis presenta un panorama delle minacce, dei rischi, ma anche delle opportunità, in sintesi dei pro e dei contro dell’“Internet delle cose” (*Internet of Things* o IoT). Il libro intende fornire una valutazione di ampio respiro della relazione tra comunicazione umana e dispositivi tecnologici; malgrado uno scenario necessariamente complesso e ad alta densità di acronimi, il lettore si trova a navigare agevolmente nel paesaggio dei confini, spesso incerti, tra il regno tangibile e quello cibernetico, tra sorveglianza e privacy, tra sicurezza e convenienza d’uso. Con quest’opera, la prima dell’autrice tradotta in italiano, Laura DeNardis continua a costruire il suo lavoro di lunga data sulla governance di Internet, iniziato con *Protocol Politics* (2009) e continuato con *The Global War for Internet Governance* (2014) e il nostro lavoro comune *The Turn to Infrastructure in Internet Governance* (2016).

Il principale centro di interesse dell’autrice in questo libro è la questione seguente: quali sono le implicazioni dell'IoT per la sicurezza e la privacy dei consumatori e la sicurezza degli Stati nazionali? Si tratta di un problema complesso e con vari aspetti, che l’autrice esamina sostenendo una tesi di fondo: la governance della sicurezza informatica (la *cybersecurity*) è necessaria, ma ugualmente necessario è di mantenere la libertà di espressione nel modo più ampio possibile.

Il libro si compone di tre parti. La prima, “Dalla comunicazione al controllo”, esamina i cambiamenti profondi che sono stati generati dal mutamento di

Internet in un mondo che è sempre più “ciber-fisico”, per esempio la grande frammentazione che caratterizza il campo dell’ IoT rispetto ad alcuni dei valori fondamentali che sono stati lungamente alla base di internet, quali l’universalità. La seconda parte, “La politica globale dei sistemi cyber-fisici”, introduce nuovi aspetti della privacy, della sicurezza cyber-fisica e delle politiche di interoperabilità, esponendo i pericoli del *ransomware* e la necessità di equilibrare il bisogno di accesso a certi dati da parte delle forze dell'ordine; questa sezione dettaglia l’ecosistema nascente in cui i consumatori IoT diventano dipendenti da uno o più fornitori per soddisfare le loro esigenze ciber-fisiche. La terza parte, “Ripensare la libertà e la governance di Internet”, ridefinisce le libertà e i diritti civili su Internet, e spiega la direzione in cui la governance globale di Internet dovrebbe procedere in questo momento storico, definito della “politica ciber-fisica”. Questa sezione conclusiva fa luce sul passaggio di Internet da una rete di comunicazione a una rete di controllo incorporata nel mondo fisico, e sul suo utilizzo da parte del potere politico come strumento di azione e reazione; come già vari lavori di Laura DeNardis in passato, il messaggio soggiacente a questa sezione è che l’attenzione politica è attualmente troppo concentrata sui contenuti digitali, e sarebbe auspicabile che si spostasse ugualmente sull’infrastruttura digitale.

THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE



EDITED BY FRANCESCA MUSIANI, DERRICK L. COGBURN, LAURA DENARDIS, AND NANETTE S. LEVINSON

INFORMATION TECHNOLOGY AND GLOBAL GOVERNANCE



In questo libro, la complessa rete di necessità e diritti generata dalla crescita economica, dai diritti individuali, dai modelli di business e dagli accordi di governance nell’era digitale è considerata come un'opportunità per plasmare il nostro futuro. Tuttavia, è importante riconoscere che le interconnessioni informatiche che si annidano negli oggetti materiali fanno sì che il digitale attraversi i confini nazionali in un modo che può complicare le giurisdizioni degli Stati. Rimangono, beninteso, molte domande aperte a cui solo il futuro potrà rispondere; l’autrice mette però sin d’ora in rilievo che la governance, la concertazione, il consenso, sono altrettanti modi per provare a costruire una certa quale stabilità nella gestione dell’IoT.

Una parte importante del libro è consacrata all’esplorazione dei molteplici sistemi in cui l’introduzione di un Internet di tipo “ciber-fisico” è percepita come conveniente, e quindi particolarmente difficile da resistere. Questo porta il lettore a riflettere su di una questione centrale: l’IoT si intrometterà nella vita umana che le persone lo vogliano o meno? L’autrice traccia una serie di principi che gli internauti/consumatori farebbero bene a considerare e seguire per ridurre questo rischio: per esempio, considerare gli aspetti legati alla sicurezza informatica prima di portare giocattoli “intelligenti”, interattivi e interconnessi nello spazio personale dei loro figli, a rischio di facilitare forme di sfruttamento, di frode di identità e di sorveglianza.

Laura DeNardis è però lungi dal limitarsi all’allarmismo per quanto riguarda questi dispositivi. Il libro presenta ugualmente l’utilità dei sistemi cyber-fisici, in relazione all'innovazione e al miglioramento delle prestazioni tecniche, che si nutrono di quella stessa raccolta di enormi quantità di dati che può porre problemi etici e sociali. Le stesse innovazioni che possono ridurre la privacy dei bambini possono aiutare i disabili e gli anziani; o rafforzare il settore agricolo riducendo la necessità di pesticidi, massimizzando la produzione di cibo e riducendo il consumo di acqua; o possono segnalare delle fughe di gas o di petrolio, o di sostanze potenzialmente pericolose, che altrimenti si tradurrebbero in disastri ambientali; o ancora, possono migliorare l’efficacia del sistema di polizia e mantenimento dell’ordine, per esempio tramite lettori di targhe capaci di identificare veicoli rubati o criminali ricercati.

L’autrice riconosce che i pro e contro dei sistemi cyber-fisici rappresentano un dilemma articolato e complicato, che rende particolarmente difficile l’ottenimento di un largo consenso. In effetti, gli oggetti ciber-fisici e le loro connessioni sono al centro di un vasto mosaico di preoccupazioni, dalla discriminazione sociale alla sorveglianza governativa, dall’azione dell’intelligence straniera al controllo dei confini, dall’anonimato alla riservatezza, dalla diffusione di informazioni personali alla sicurezza e salute, fino alla preservazione di un certo numero di diritti civili quali l’integrità della propria identità o il diritto all’oblio (per chi fosse interessato ad approfondire tali questioni in relazione all’IA, alla robotica ed agli algoritmi, mi permetto di segnalare l’uscita di questo recentissimo libro per i tipi di Carocci).

Attualmente, sottolinea l’autrice, c’è una discrepanza nel modo in cui le politiche pubbliche considerano i vantaggi e i danni della vasta raccolta e aggregazione di dati provocata dal big data: i primi vengono considerati come un bene pubblico, e i secondi come un problema individuale; di conseguenza, secondo l’autrice, i sistemi cyber-fisici presentano le più grandi complicazioni per la privacy che l’umanità si sia mai trovata ad affrontare.

Il libro esamina poi la questione della sicurezza legata ai sistemi ciber-fisici. Secondo DeNardis, la capacità degli stati ad agire su e via Internet, ivi compreso in modi aggressivi ed al limite della legalità, è cresciuta nel tempo. L’accumulo (sovente deliberato) di vulnerabilità digitali è diventato la norma rispetto ad un passato recente in cui i fabbricanti di hardware e software si sentivano legati ad un (ufficioso) codice di condotta, il che crea preoccupazioni ancora maggiori per la sicurezza umana e la stabilità di Internet, e forte incertezza sul ruolo che l’infrastruttura ciber-fisica svolge e può svolgere nell'economia digitale globale e nella sua democrazia.

Alla base di questo fondamentale cambiamento, sostiene Laura DeNardis, è una mutazione fondamentale nella “natura” di Internet, che da rete di comunicazione si è rapidamente evoluta in reti di controllo che si stanno infiltrando nelle case e negli spazi privati. Questo cambiamento ha degli effetti diretti sugli equilibri politici, poiché genera una sfocatura sempre più importante dei confini tra il regno fisico e quello virtuale, e offusca la possibilità di comprensione della stessa

Internet da parte dei suoi utenti. Allo stesso modo, è sempre meno possibile relegare le grandi “imprese del digitale” e della comunicazione (come AT&T, Comcast, Vodafone, Facebook e Google) a questo solo campo: esse sono ormai degli attori economici globali, che ambiscono a produrre e fornire una meta-infrastruttura per tutte le altre infrastrutture.

In conclusione, “Internet in Ogni Cosa” è un libro sulle opportunità e le (numerose) sfide di un’era, che si sta aprendo, in cui politiche pubbliche e pervasività del mondo ciber-fisico saranno, e dovranno essere, sempre più legate. Il timore dell’autrice è che senza una maggiore trasparenza, rappresentatività, *accountability*, gli interessi economici e la ricerca del potere politico faranno dell’IoT uno strumento incredibilmente potente di censura, sorveglianza e violazione della privacy, che sorpasserà largamente i suoi potenziali effetti positivi.

Per ridimensionare questo rischio, è importante che i potenziali regolatori di Internet si concentrino non solo (e forse non prevalentemente) sui contenuti digitali, ma che si rendano conto pienamente del ruolo centrale dell’infrastruttura digitale come strumento di governance. Questo libro, fusione felice di specializzazione accademica e comunicazione verso un pubblico più ampio, rivelatore del dilemma tra le irresistibili comodità dell’IoT e i pericoli che derivano dalla nostra inevitabile resa ad esso, contribuisce a portare alla ribalta politica e sociale la questione dell’Internet ciber-fisica, esplorandone le implicazioni per la sicurezza dei consumatori e degli Stati, per la privacy, per gli sviluppi futuri della governance di Internet.

Se continuiamo a tenere vivo questo spazio è grazie a te. Anche un solo euro per noi significa molto.
Torna presto a leggerci e SOSTIENI DOPPIOZERO

INTERNET IN OGNI COSA

LAURA DENARDIS

LIBERTÀ, SICUREZZA
E PRIVACY
NELL'ERA DEGLI OGGETTI
IPERCONNESSI



LUISS