Il Mulino - Rivisteweb

Mauro Santaniello

Recensione di Roberto Baldoni, Charting digital sovereignty: a survival playbook

(doi: 10.53227/113114)

Rivista di Digital Politics (ISSN 2785-0072)
Fascicolo 3, luglio-settembre 2023

Ente di afferenza:
()

Copyright © by Società editrice il Mulino, Bologna. Tutti i diritti sono riservati.
Per altre informazioni si veda https://www.rivisteweb.it

Licenza d'uso

Questo articolo è reso disponibile con licenza CC BY NC ND. Per altre informazioni si veda https://www.rivisteweb.it/

Mauro Santaniello

Roberto Baldoni, *Charting digital sovereignty: a survival playbook*

Il libro «*Charting Digital Sovereignty: A Survival Playbook*»[1], uscito a febbraio come pubblicazione indipendente di Roberto Baldoni, offre una rigorosa analisi di quelle trasformazioni globali che si dispiegano all'intersezione tra geopolitica, sicurezza nazionale e tecnologia digitale. Il libro, concepito come una sorta di manuale di sopravvivenza digitale per le organizzazioni governative e per i decisori pubblici, rappresenta una significativa novità nel contesto, sempre più ampio, degli studi sulla sovranità digitale. Se gran parte della letteratura esistente sul tema, infatti, si concentra sulle dinamiche politiche della costruzione del discorso pubblico sulla sovranità digitale, o sulle sfide connesse all'implementazione di un insieme sempre più articolato di politiche pubbliche, il testo di Baldoni percorre un sentiero originale. L'autore circoscrive sin da subito la questione della sovranità digitale a un ambito estremamente limitato, quello della sicurezza nazionale, e lo esplora in profondità dalla prospettiva di chi ha responsabilità di governo. È evidente, nel tracciato di questo percorso, una visione unica e privilegiata, funzione delle specificità biografiche dell'autore. Baldoni, dopo aver consolidato una carriera accademica come professore ordinario di ingegneria informatica, ha ricoperto importanti ruoli istituzionali, prima come vicedirettore generale del Dipartimento delle informazioni per la sicurezza (Dis), e poi come primo Direttore Generale dell'Agenzia nazionale per la sicurezza cibernetica italiana (Acn). Da questi punti di osservazione, Baldoni elabora un suo peculiare approccio alla sovranità digitale, che fa tesoro di una vasta conoscenza dei più reconditi mec-

[1] Baldoni, R. (2024), *Charting Digital Sovereignty: A Survival Playbook. How to Assess and to Improve the Level of Digital Sovereignty of a Country*, Independently published, Isbn-13: 9798877326712.

ISSN 2785-0072
© Società editrice il Mulino

canismi sottostanti le sfide che gli Stati affrontano nel contesto cibernetico. In questo libro, l'esperienza di Baldoni si materializza in un'analisi completa e aggiornata delle minacce e delle opportunità che il mondo digitale presenta per la sicurezza delle nazioni.

Il libro si compone di quattro parti. Nella prima, l'autore offre una rapida ricostruzione storica della trasformazione digitale, evidenziando come questa traiettoria si sia di recente spostata dall'ambito prettamente economico della globalizzazione verso un terreno più marcatamente geopolitico. Uno slittamento avvenuto contestualmente a un salto evolutivo dell'innovazione digitale, rappresentato dalla diffusione di nuove e più potenti tecnologie come il *cloud computing*, l'Internet delle Cose, i network 5g e 6g, l'Intelligenza artificiale, le *blockchain*, i microprocessori ad alta prestazione e i supercomputer. La fase della globalizzazione, sostiene l'autore, ha condotto a un'economia digitale basata su lunghe catene di approvvigionamento che integrano aree tra loro molto distanti, geograficamente e politicamente, all'interno di un tessuto di scambi e di suddivisione del lavoro su scala planetaria. Questa organizzazione economica, inoltre, ha condotto all'ascesa dei giganti della tecnologia, prima negli Stati Uniti e poi in Cina, che hanno beneficiato di ingenti investimenti pubblici e di una benevola legislazione nei rispettivi Paesi, e di un mercato digitale pressoché senza limiti. La tesi di Baldoni è che una serie di fattori abbiano impresso, nel corso dei primi due decenni del secolo, una svolta nei rapporti interstatali tale da curvare in senso geopolitico anche la trasformazione digitale. Gli attentati dell'11 settembre, la crisi economica del 2008, e in seguito la politica isolazionista dell'amministrazione Trump e il ritiro americano dall'Afghanistan avrebbero indebolito le democrazie occidentali, mentre stati autocratici come Cina e Russia avrebbero rafforzato il proprio potere, economico e tecnologico la prima, energetico la seconda, giungendo a contestare apertamente l'ordine internazionale. A complicare il quadro, l'ascesa di nuove potenze regionali come il Pakistan, l'India, il Vietnam, il Brasile, l'Iran e la Nigeria. In questo contesto, i Paesi occidentali, e soprattutto gli Stati Uniti, tradizionalmente promotori di una visione economica e globale della rete, hanno ingaggiato un confronto tecnologico con le potenze rivali, soprattutto con la Cina, ristrutturando le proprie *supply chain* di materiali, componenti e prodotti tecnologici, e avviando iniziative sanzionatorie o comunque ostili nei confronti dei digital *champions* avversari.

La seconda parte del libro definisce la sovranità digitale entro un framework concettuale che, come s'è detto, ricalca il perimetro della sicurezza nazionale. Per Baldoni la sovranità digitale di una nazione comprende quattro

elementi. Il primo è il controllo legale e tecnico sui dati prodotti dai cittadini, dalla pubblica amministrazione e dalle aziende. Il secondo riguarda la capacità tecnologica e la disponibilità di forza lavoro altamente qualificata. Il terzo elemento è la consapevolezza sociale dei rischi cibernetici, mentre il quarto è la capacità di un paese di costruire alleanze sul piano internazionale per governare sfide complesse e di portata globale. L'autore procede poi a una mappatura delle minacce alla sovranità digitale, dai cyber-attacchi alle manomissioni delle reti virtualizzate del 5g o dei server del *cloud*, dalla disinformazione ai rischi connessi alle interdipendenze delle *supply chain* dei prodotti tecnologici, dalla politicizzazione dei processi di standardizzazione all'acquisizione straniera di compagnie strategiche, dalla militarizzazione dell'intelligenza artificiale alla disponibilità di forza lavoro adeguata, fino alle sfide, ancora tutte da valutare, di un mondo post-digitale dominato dal *quantum computing*.

Nella terza parte del libro, Baldoni disegna un originale modello di governo della sovranità digitale. Il modello comprende sia una tassonomia delle minacce alla sovranità digitale, che vengono organizzate in una matrice a doppia entrata (visibili/coperte, persistenti/non-persistenti), sia uno «schema concettuale di sovranità digitale» in cui le minacce rappresentano l'input del processo di *decision-making*, e la postura nazionale (economica, politica, tecnologica, ecc.) determina un insieme di opzioni di risposta a disposizione dell'autorità politica, cui spetta il compito di produrre output decisionali nelle forme di politiche, strategie, tattiche, e collaborazioni internazionali. Su tale modello, Baldoni progetta un'architettura di riferimento per l'analisi sistematica della capacità dei Paesi di fronteggiare le minacce alla propria sovranità digitale. L'architettura prevede la combinazione gerarchica di quelle che l'autore definisce «celle di fusione». Ciascuna cella è dedicata a una specifica minaccia, che ne definisce la missione, e si compone di autorità civili e militari che producono informazioni, opzioni di policy e azioni per il lungo e il breve periodo. Le celle di cui si compone la sovranità digitale, nell'architettura di Baldoni, sono sette: *Safe Ai, Cyber resilience and response, Disinformation, Supply chain security, Workforce, Emerging and disruptive technologies*, e una cella di coordinamento. A sua volta, la sovranità digitale è una cella di una più ampia architettura di sicurezza nazionale, in cui hanno un ruolo di primo piano le comunità dei militari, dell'intelligence e delle forze di polizia.

La quarta parte del libro elabora un sistema di valutazione delle architetture nazionali di sovranità digitale che discende dal framework concettuale e dall'architettura di governance della sovranità digitale elaborati nelle parti precedenti. Il sistema comprende quattro criteri qualitativi di valutazione. Il

primo è la capacità di un Paese di governare i propri dati, sia con misure legali che tecniche. Il secondo criterio è la capacità di implementare le politiche di sovranità digitale, e riguarda tanto le politiche industriali quanto il sistema di formazione della forza lavoro. Il terzo criterio fa riferimento alla consapevolezza dei rischi cibernetici da parte del settore pubblico, delle aziende e dei cittadini. Il quarto criterio concerne la capacità di creare alleanze internazionali. Attraverso questo sistema di valutazione, Baldoni sviluppa, negli ultimi quattro capitoli del volume, un'analisi del livello di sovranità digitale degli Stati Uniti d'America, della Cina, dell'Unione Europea e dell'Italia. Per ciascun caso, l'autore elabora una scheda di valutazione ed esplicita le condizioni che, nel prossimo futuro, possono influire sulle dinamiche di rafforzamento, o al contrario di restringimento, della capacità di ciascun Paese di tutelare e promuovere la propria sovranità digitale. Lo strumento di valutazione elaborato da Baldoni viene dunque testato su quattro casi molto diversi gli uni dagli altri, e dimostra l'efficacia del framework analitico in termini comparativi. Se la sovranità digitale è un concetto relazionale in cui le capacità di un'entità statale e le minacce che essa affronta sono funzione dell'azione congiunta di strategie e politiche implementate dagli altri attori dello scenario internazionale, è evidente che l'adozione di una prospettiva comparata rappresenti un passaggio cruciale per orientarsi nella competizione globale per il controllo delle reti e delle tecnologie digitali. Più in dettaglio, i quattro casi analizzati da Baldoni restituiscono un quadro complesso, in cui tendenze e sfide comuni a tutti i Paesi si intrecciano a specificità strategiche e peculiarità politiche e istituzionali.

Secondo questa analisi, gli Stati Uniti presentano la più avanzata struttura di governance della cybersicurezza tra le democrazie, e una forte capacità di protezione di infrastrutture e dati a livello di governo federale. Essi eccellono, inoltre, nella capacità di produrre tecnologie sicure, e hanno una forte capacità di leadership a livello internazionale, ove guidano numerose coalizioni. D'altra parte, la consapevolezza dei rischi cibernetici da parte delle piccole imprese e degli enti locali è bassa, come testimonia il dato sugli attacchi ransomware nel mondo, che vede le organizzazioni statunitensi al primo posto in quanto a numero di vittime. Si registra inoltre una significativa carenza di personale qualificato nel settore della sicurezza cibernetica.

La Cina ha sempre implementato stringenti politiche di controllo dei dati e della tecnologia, e grazie al famigerato *Great firewall* è riuscita a esercitare un efficace sistema di censura e sorveglianza del traffico dati, dentro il Paese, e tra il Paese e il mondo esterno. Nell'ultimo decennio ha inoltre implementato una serie stringente di normative sulla protezione dei dati e la sicurezza cibernetica. Le sue politiche industriali nel settore della tecnologia l'hanno condotta al dominio di molti mercati e a una situazione di leadership nello sviluppo di

importanti nuove tecnologie. La Cina, inoltre, produce un numero di laureati in materie Stem cinque volte più grande di quello degli Stati Uniti, e si accinge a doppiare il numero degli studenti di dottorato americani entro il 2025. Il governo cinese, sin dai primi anni del 2000, ha costruito alleanze internazionali in molteplici arene di policy relative alle reti digitali, assumendo posizioni di leadership assieme alla Russia.

L'analisi del caso europeo mostra con chiarezza una posizione di debolezza dell'Unione rispetto ai due casi precedenti, dovuta essenzialmente a una scarsa integrazione politica, industriale e di sicurezza. In questo contesto, sostiene Baldoni, la sovranità digitale europea è una giustapposizione della sovranità digitale degli stati membri. Ciononostante, importanti iniziative dell'Ue si registrano nel campo della disinformazione, della formazione della forza lavoro, e soprattutto della regolazione delle tecnologie digitali.

La valutazione della sovranità digitale italiana, infine, restituisce un quadro a tinte variabili. Il Paese manca di grandi player industriali nel mercato digitale, ma presenta un tessuto vitale e fitto di piccole e medie aziende di successo. Le iniziative e le partnership pubblico-privato non mancano, e il Paese si è dotato di legislazione all'avanguardia, come quella relativa al perimetro nazionale di cyber sicurezza o quella concernente l'esercizio del *Golden power* per evitare pratiche predatorie nei confronti delle industrie strategiche nazionali. L'analisi mostra anche come un problema specifico dell'Italia rispetto alle altre democrazie occidentali sia quello della mancanza di forza lavoro qualificata. Un problema che assume una doppia dimensione. Da un lato, la percentuale dei laureati in discipline Stem è pari a un misero 6,7%, contro una media Ue del 13%. Dall'altro, l'Italia soffre di un significativo *brain drain*, che porta una quota consistente delle sue professionalità più elevate a emigrare verso il nord Europa o gli Stati Uniti.

Il libro si chiude con un piccolo ma interessante glossario, che raccoglie definizioni e approfondimenti su minacce, norme, e strumenti per la difesa della sovranità digitale.

In definitiva, il nuovo libro di Roberto Baldoni mantiene la promessa di fornire a politici e decisori pubblici un manuale di sopravvivenza per affrontare le sfide alla sovranità digitale del proprio Paese. Da questo punto di vista, il testo offre una mappatura dettagliata ed esaustiva dei temi che le autorità politiche sono oggi chiamate ad affrontare, e rappresenta una fonte preziosa di dati per comprendere il linguaggio, le agende e i modelli politici di riferimento di quel mondo complesso che si estende sul margine convergente tra sicurezza cibernetica e trasformazioni geopolitiche.