

DYNAMES

Governance di Forze e Sistemi

PAPER & DOSSIER

WHITE PAPER

Sovranità tecnologica: la nuova frontiera della democrazia europea



FRANCESCO CUSTURERI

2026



Paper Series
White Paper

White Paper

SOVRANITÀ TECNOLOGICA: LA NUOVA FRONTIERA DELLA DEMOCRAZIA EUROPEA

A CURA DI	Francesco Custureri
DATA	15/07/2026
AREA TEMATICA	Tecnologie e sistemi complessi
CATEGORIA	White Paper
VERSIONE	1.0

Documento di analisi strategica

Cloud, dati, semiconduttori e intelligenza artificiale non sono più semplici strumenti di innovazione: sono infrastrutture di potere. Governarle significa difendere autonomia, diritti e libertà democratiche.

Qualifica / affiliazione: Ingegnere

Summary

Sommario del White Paper

<i>Sovranità tecnologica: la nuova frontiera della democrazia europea.....</i>	<i>4</i>
<i>Tecnologia e potere: la nuova geografia delle dipendenze.....</i>	<i>5</i>
<i>La democrazia nell’ambiente digitale.....</i>	<i>6</i>
<i>Una strategia europea per autonomia, sicurezza e libertà.....</i>	<i>7</i>
<i>Fonti essenziali.....</i>	<i>8</i>

NOTA EDITORIALE

Il presente documento è un contributo di analisi strategica pubblicato da DYNAMES. Non costituisce pubblicazione scientifica peer-reviewed, salvo diversa indicazione. Le opinioni espresse sono attribuibili all'autore e non impegnano necessariamente la linea editoriale della rivista o degli enti collegati.

Sovranità tecnologica: la nuova frontiera della democrazia europea

Cloud, dati, semiconduttori e intelligenza artificiale non sono più semplici strumenti di innovazione: sono infrastrutture di potere. Governarle significa difendere autonomia, diritti e libertà democratiche.

Per anni la tecnologia è stata raccontata come un fattore neutrale di progresso: più efficienza, più accesso ai servizi, più opportunità economiche. Oggi questa rappresentazione non basta più. Le infrastrutture digitali, le piattaforme, i dati, i semiconduttori, il cloud e l'intelligenza artificiale sono diventati asset strategici capaci di determinare la competitività di un Paese, la continuità dei servizi essenziali e perfino la qualità del dibattito pubblico. La questione tecnologica è dunque entrata stabilmente nel campo della politica e della geopolitica.

La domanda centrale non è soltanto chi sappia sviluppare le tecnologie più avanzate, ma chi possieda le infrastrutture che le rendono possibili, chi controlli i dati necessari al loro funzionamento e secondo quali regole vengano utilizzate. Uno Stato che dipende integralmente da soggetti esterni per il cloud, le capacità computazionali, le reti, i sistemi operativi o i modelli di intelligenza artificiale conserva formalmente la propria sovranità, ma vede restringersi la sua capacità di scelta. È da questa tensione che nasce il concetto di sovranità tecnologica.

La sovranità tecnologica non coincide con l'autarchia digitale né con la chiusura dei mercati. Indica, piuttosto, la capacità di evitare dipendenze critiche, proteggere gli asset strategici e mantenere un controllo democratico sulle infrastrutture da cui dipendono istituzioni, imprese e cittadini. In altre parole, non significa produrre tutto da soli, ma poter decidere senza che un altro soggetto abbia la possibilità di spegnere l'interruttore.

Tecnologia e potere: la nuova geografia delle dipendenze

La competizione geopolitica contemporanea si gioca sempre più lungo filiere tecnologiche complesse. I semiconduttori sono indispensabili per industria, difesa, telecomunicazioni e intelligenza artificiale; il cloud ospita dati e servizi essenziali; le piattaforme mediano comunicazioni, informazione e attività economiche; i sistemi di AI richiedono enormi quantità di dati, energia e capacità computazionale. Il controllo di questi elementi genera vantaggi economici, ma anche influenza politica e capacità di pressione internazionale.

La centralità dei dati è particolarmente evidente. I dati alimentano modelli predittivi, sistemi di raccomandazione, servizi pubblici digitali e processi decisionali automatizzati. Chi li raccoglie e li elabora dispone di una conoscenza dettagliata dei comportamenti individuali e collettivi. Per questo la governance dei dati non può essere ridotta a un tema tecnico o commerciale: riguarda la sicurezza, la concorrenza, la protezione della persona e la possibilità stessa di esercitare diritti in modo consapevole.

Anche le grandi piattaforme digitali hanno assunto una funzione quasi infrastrutturale. Organizzano l'accesso alle informazioni, stabiliscono la visibilità dei contenuti e orientano il funzionamento di interi mercati. I loro algoritmi non si limitano a ordinare ciò che vediamo: contribuiscono a definire quali temi emergano, quali opinioni acquistino rilevanza e quali comportamenti siano premiati. Quando questa capacità è concentrata in pochi operatori globali, il potere privato può incidere sullo spazio pubblico con una forza che le istituzioni nazionali faticano a bilanciare.

I principali attori globali hanno sviluppato modelli differenti. Gli Stati Uniti hanno favorito un ecosistema trainato dall'innovazione privata, dal capitale di rischio e dalla crescita di grandi imprese tecnologiche. La Cina ha integrato sviluppo digitale, politica industriale e controllo statale. L'Unione europea tenta di costruire una terza via, fondata sulla combinazione tra innovazione, regolazione, tutela dei diritti e autonomia strategica. Il Digital Services Act, il Digital Markets Act, l'AI Act, la normativa sui dati e il Chips Act sono tasselli di questo tentativo.

La democrazia nell'ambiente digitale

La trasformazione tecnologica modifica anche il modo in cui si forma il consenso. Le piattaforme sono diventate uno dei principali luoghi della partecipazione politica e della comunicazione pubblica. Questo ha ampliato l'accesso alla conoscenza e reso più immediata l'interazione tra cittadini e istituzioni, ma ha anche favorito polarizzazione, profilazione e campagne di disinformazione. La velocità della circolazione dei contenuti rende più difficile distinguere informazione verificata, propaganda e manipolazione coordinata.

La democrazia contemporanea non vive soltanto nelle aule parlamentari o nei processi elettorali. Vive anche negli spazi digitali in cui le persone si informano, discutono e costruiscono la propria percezione della realtà. Se tali spazi sono governati da logiche opache, orientate principalmente alla massimizzazione dell'attenzione o del profitto, il pluralismo può essere formalmente garantito ma sostanzialmente indebolito. Difendere la democrazia significa quindi rendere trasparenti e responsabili anche le architetture digitali che organizzano il dibattito pubblico.

La stessa attenzione deve essere riservata alle disuguaglianze. Il digital divide non riguarda più soltanto la disponibilità di una connessione. Comprende la qualità delle infrastrutture, l'accesso ai dispositivi, le competenze e la capacità di comprendere l'effetto delle tecnologie sulle proprie scelte. Quando servizi pubblici, istruzione, sanità e lavoro diventano digitali, chi resta privo di strumenti o conoscenze adeguate rischia una forma concreta di esclusione dalla cittadinanza.

La diffusione dell'intelligenza artificiale rende il problema ancora più delicato. Sistemi automatizzati possono intervenire nella selezione del personale, nella concessione del credito, nella diagnosi medica, nella sicurezza e nell'erogazione di prestazioni pubbliche. In questi ambiti non basta che un algoritmo sia efficiente: deve essere verificabile, proporzionato, comprensibile e sottoposto a responsabilità umana. La dignità della persona non può dipendere da decisioni opache, né la tecnologia può diventare un alibi per sottrarre le scelte pubbliche al controllo democratico.

Una strategia europea per autonomia, sicurezza e libertà

Per l'Europa, la sovranità tecnologica è prima di tutto capacità di scelta. Richiede investimenti coordinati nei semiconduttori, nel cloud, nella connettività, nella cybersicurezza, nell'intelligenza artificiale e nella ricerca. Richiede inoltre infrastrutture interoperabili, standard comuni e politiche industriali che riducano le dipendenze più rischiose senza rinunciare alla cooperazione internazionale.

La cybersicurezza è una componente decisiva di questa strategia. Energia, telecomunicazioni, finanza, sanità, trasporti e amministrazioni pubbliche dipendono da sistemi digitali interconnessi. Un attacco contro queste infrastrutture può interrompere servizi essenziali, compromettere dati, generare sfiducia e produrre effetti sociali paragonabili a quelli di una crisi materiale. La direttiva NIS2 e le strategie europee e nazionali di sicurezza cyber riconoscono che la resilienza digitale è ormai parte della sicurezza collettiva.

Accanto alle infrastrutture servono competenze. Senza capitale umano, gli investimenti tecnologici rischiano di produrre dipendenze nuove invece di ridurre quelle esistenti. L'Europa deve rafforzare la formazione specialistica, l'alfabetizzazione digitale, la capacità amministrativa e il rapporto tra università, ricerca, imprese e istituzioni. Le competenze non sono soltanto un fattore di competitività: consentono ai cittadini di comprendere le tecnologie, valutarne i rischi e partecipare alle decisioni che ne regolano l'uso.

Infine, occorre una governance democratica dell'intelligenza artificiale. Trasparenza, auditabilità, supervisione umana, valutazione degli impatti e responsabilità lungo l'intero ciclo di vita dei sistemi devono diventare condizioni ordinarie, soprattutto nei settori ad alto impatto. L'obiettivo non è frenare l'innovazione, ma impedire che l'innovazione eroda le condizioni che rendono possibile una società libera.

La sfida europea non consiste nel replicare il modello statunitense o quello cinese. Consiste nel dimostrare che competitività, sicurezza e diritti possono sostenersi reciprocamente. Una sovranità tecnologica democratica non misura il proprio successo soltanto nel numero di brevetti, data center o modelli sviluppati, ma nella capacità di utilizzare questi strumenti senza trasformare cittadini e istituzioni in soggetti dipendenti da decisioni opache.

La tecnologia non è più un settore separato della vita pubblica: è l'ambiente nel quale si esercitano potere, libertà e cittadinanza. Per questo la sovranità tecnologica è una questione democratica. Proteggere infrastrutture, dati e competenze significa preservare la capacità delle istituzioni di decidere, dei cittadini di comprendere e della società di orientare l'innovazione verso il bene comune.

La domanda decisiva dei prossimi anni non sarà se l'intelligenza artificiale, il cloud o le piattaforme cambieranno le nostre società. Lo stanno già facendo. La domanda sarà chi governerà questo cambiamento, con quali responsabilità e nell'interesse di chi. Da questa risposta dipenderà non soltanto la posizione dell'Europa nella competizione globale, ma la qualità della sua democrazia.

“La sovranità tecnologica non significa produrre tutto da soli, ma poter decidere senza che un altro soggetto abbia la possibilità di spegnere l'interruttore.”

Fonti essenziali

- Commissione europea, Digital Decade Policy Programme 2030.
- Commissione europea, Artificial Intelligence Act.
- Commissione europea, Digital Services Act e Digital Markets Act.
- Commissione europea, European Strategy for Data e Common European Data Spaces.
- Commissione europea, European Chips Act.
- Commissione europea, Direttiva NIS2 e EU Cybersecurity Strategy.
- Parlamento europeo, Technological Sovereignty.
- ENISA, Threat Landscape 2025.
- ACN, Strategia nazionale di cybersicurezza 2022-2026.
- Consiglio d'Europa, Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.
- OECD, AI Principles e Reinforcing Democracy Initiative.
- UNESCO, Recommendation on the Ethics of Artificial Intelligence.

Lunghezza del corpo dell'articolo: 9.121 battute spazi inclusi.

DYNAMES

Difesa • Sicurezza • Resilienza

DYNAMES è una rivista registrata dedicata all'analisi dei temi strategici di difesa, sicurezza, comunicazione, geopolitica, resilienza e interesse nazionale.

Registrata al Tribunale di Busto Arsizio

N. 01/2026 del 25 febbraio 2026

Iscrizione ROC

n. 44335

Con sede in Via Carlo Noè 45 Gallarate (VA), C.F. 3800470126

Direttore responsabile Fabio Boscacci

Pubblicazione diffusa in formato digitale mediante il sito www.dynames.it e gli altri canali ufficiali della testata.

Tutti i diritti sono riservati. La riproduzione, distribuzione, comunicazione al pubblico, elaborazione o utilizzo, anche parziale, dei contenuti pubblicati è consentita nei limiti previsti dalla legge e previa corretta citazione della fonte, salvo diversa autorizzazione scritta dell'editore o dei titolari dei diritti. Restano consentiti gli utilizzi per finalità di cronaca, studio, ricerca, critica e discussione, nei limiti e secondo le condizioni previste dalla normativa applicabile.

Le immagini, i marchi, i loghi, i segni distintivi, le fonti documentali e gli eventuali materiali di terzi presenti nella pubblicazione appartengono ai rispettivi titolari e sono utilizzati, ove applicabile, per finalità informative, illustrative, scientifiche o di commento. Eventuali richieste di rettifica, segnalazioni relative ai diritti d'autore, comunicazioni legali o richieste di rimozione possono essere inviate a redazione@dynames.it.

Il trattamento dei dati personali eventualmente connesso alle attività editoriali della testata è effettuato nel rispetto della normativa applicabile in materia di protezione dei dati personali. L'informativa privacy aggiornata è disponibile all'indirizzo: redazione@dynames.it.