

SOVRANITA' TECNOLOGICA, DEMOCRAZIA E LIBERTA'

Il ruolo degli asset digitali nello
scenario geopolitico

DI

Francesco Custureri

Introduzione	1
Tecnologia, Potere e Geopolitica	2
Impatti democratici e nuove dipendenze	7
Sovranità tecnologica come tutela dello Stato democratico	10
Raccomandazioni strategiche	13
Conclusioni	16
Bibliografia	



FRANCESCO CUSTURERI

Francesco Custureri è un ingegnere con una forte passione per l'innovazione, la tecnologia e il modo in cui queste possono contribuire concretamente alla società.

Il suo percorso unisce competenze scientifiche, interesse per l'Intelligenza Artificiale e attenzione ai temi della salute, della telemedicina, della cybersecurity e dell'impatto sociale delle nuove tecnologie.

Accanto all'attività professionale, partecipa a iniziative associative e culturali, confrontandosi con progetti legati all'innovazione e allo sviluppo sociale.

È inoltre iscritto all'**Ordine degli Ingegneri** della Provincia di Roma.

Ha approfondito temi come l'intelligence economica, l'interesse nazionale, la geopolitica, l'etica dell'Intelligenza Artificiale.

Ha partecipato a diversi percorsi formativi e scuole di alta formazione.

È curioso, orientato alla condivisione e alla collaborazione.

Ama viaggiare, cucinare e conoscere persone e contesti diversi, convinto che l'innovazione abbia valore soprattutto quando riesce a migliorare la vita delle persone.

INTRODUZIONE

La trasformazione digitale rappresenta oggi uno dei principali fattori di ridefinizione degli equilibri economici, sociali e geopolitici globali. Le tecnologie digitali non costituiscono più soltanto strumenti di innovazione o crescita economica, ma asset strategici in grado di influenzare competitività, sicurezza nazionale, stabilità democratica ed esercizio delle libertà fondamentali.

Negli ultimi anni, la crescente centralità di infrastrutture digitali, piattaforme globali, dati e sistemi di intelligenza artificiale ha modificato profondamente il rapporto tra cittadini, imprese e istituzioni. La capacità di raccogliere, elaborare e controllare informazioni su larga scala è diventata una leva di potere strategico, incidendo tanto sulle dinamiche economiche quanto sulla formazione del consenso, sulla circolazione dell'informazione e sulla tutela dei diritti individuali.

La trasformazione digitale apre opportunità rilevanti in termini di inclusione, partecipazione e accesso ai servizi. La digitalizzazione può migliorare l'efficienza della pubblica amministrazione, ampliare l'accesso alla conoscenza e ridurre alcune barriere territoriali ed economiche. Tuttavia, tali benefici non sono automaticamente distribuiti in modo equo. Persistono disuguaglianze significative legate all'accesso alle infrastrutture, alle competenze digitali e alla capacità di partecipare consapevolmente alla società digitale.

In questo contesto, il tema della sovranità tecnologica assume una rilevanza crescente per gli Stati democratici. La dipendenza da infrastrutture, servizi digitali e tecnologie controllate da soggetti esterni può generare vulnerabilità politiche, economiche e sociali. Le tensioni geopolitiche, le campagne di disinformazione, gli attacchi cyber e l'utilizzo strategico dei dati dimostrano come il dominio tecnologico sia oggi una delle principali leve di influenza internazionale.

La democrazia contemporanea si trova dunque di fronte a una duplice sfida. Da un lato deve sfruttare il potenziale della tecnologia per rafforzare innovazione, crescita e partecipazione; dall'altro deve preservare autonomia decisionale, pluralismo informativo, trasparenza e tutela dei diritti fondamentali in un ecosistema digitale sempre più concentrato e interdipendente. La tecnologia non è più un settore separato della vita pubblica, ma l'ambiente nel quale si esercitano diritti, libertà e potere.

1. TECNOLOGIA, POTERE E GEOPOLITICA

1.1 La tecnologia come nuova leva di potere strategico

Nel contesto contemporaneo, la tecnologia rappresenta una delle principali dimensioni attraverso cui si esercita il potere economico, politico e strategico degli Stati. La capacità di sviluppare, controllare e proteggere infrastrutture digitali, dati, semiconduttori e sistemi avanzati di intelligenza artificiale costituisce oggi un elemento determinante della competitività internazionale e della sicurezza nazionale.

Le infrastrutture digitali non sono più considerate semplici strumenti di supporto alle attività economiche e amministrative, ma componenti essenziali per il funzionamento dello Stato moderno. *Cloud computing*, reti di telecomunicazione, data center, capacità computazionale, piattaforme e *supply chain* tecnologiche sono ormai alla base di servizi pubblici, sistemi finanziari, comunicazioni, difesa e capacità industriale. La loro disponibilità e affidabilità incidono direttamente sulla continuità operativa delle istituzioni e sulla resilienza del sistema economico.

In tale scenario, la dipendenza tecnologica da attori esterni può trasformarsi in un fattore di vulnerabilità geopolitica. L'accesso a tecnologie critiche, semiconduttori, infrastrutture cloud o piattaforme digitali non è più soltanto una questione industriale, ma una componente dell'autonomia strategica. La competizione tra potenze globali si gioca sempre più sulla capacità di controllare le filiere tecnologiche e di garantire la sicurezza delle infrastrutture digitali.

L'attenzione crescente verso la sovranità tecnologica nasce proprio da questa consapevolezza: il controllo degli asset digitali influenza la capacità di uno Stato di preservare stabilità, sicurezza e autonomia decisionale. Le principali potenze globali stanno investendo nello sviluppo di capacità autonome nei settori chiave della trasformazione digitale, riconoscendo nella tecnologia una nuova dimensione del potere internazionale.



1.2 Dati, piattaforme e intelligenza artificiale nella competizione geopolitica

La crescente centralità dei dati ha ridefinito le dinamiche economiche e geopolitiche globali. La capacità di raccogliere, elaborare e utilizzare informazioni su larga scala rappresenta oggi un vantaggio competitivo strategico sia per gli Stati sia per le grandi piattaforme tecnologiche. I dati sono la base per lo sviluppo di servizi digitali avanzati, modelli predittivi, sistemi di intelligenza artificiale e strumenti di influenza economica e sociale.

La **Commissione Europea** considera i dati una risorsa essenziale per crescita economica, competitività, innovazione e progresso sociale. La strategia europea sui dati punta alla creazione di un mercato unico dei dati, fondato su controllo, fiducia e valorizzazione degli asset informativi a beneficio di cittadini e imprese. Questo approccio evidenzia come la governance dei dati non sia soltanto una questione tecnica, ma un elemento centrale della sovranità digitale europea.

Parallelamente, le piattaforme digitali globali hanno assunto un ruolo crescente nella gestione dell'informazione, nella mediazione delle comunicazioni e nella distribuzione dei contenuti online. Tale concentrazione di potere tecnologico ed economico ha generato nuove riflessioni sul rapporto tra mercato, sovranità e tutela democratica. In molti casi, il controllo delle piattaforme consente di influenzare flussi informativi, opinione pubblica e dinamiche economiche transnazionali.

Anche l'intelligenza artificiale si colloca ormai al centro della competizione geopolitica internazionale. Le applicazioni AI influenzano settori strategici quali sicurezza, difesa, cybersicurezza, finanza, industria e gestione dei servizi pubblici. La leadership nello sviluppo di modelli avanzati di AI è percepita come un elemento decisivo per crescita economica, capacità industriale e proiezione geopolitica futura.

La competizione sull'AI non riguarda soltanto gli algoritmi, ma l'intero ecosistema che li rende possibili: dati, capacità computazionale, semiconduttori, energia, cloud e competenze specialistiche. In altri termini, non basta "avere l'AI", come se fosse una funzione magica da attivare in un menu. Serve controllare la catena materiale e infrastrutturale che la sostiene.

1.3 Modelli geopolitici e sovranità tecnologica

L'attuale scenario internazionale evidenzia l'emergere di differenti modelli di governance tecnologica, coerenti con le impostazioni politiche, economiche e culturali delle principali potenze globali. La tecnologia diventa così non soltanto un settore produttivo, ma un riflesso dei modelli istituzionali e dei valori che orientano le società.



Gli **Stati Uniti** hanno storicamente favorito un modello trainato dall'innovazione privata, dal capitale di rischio e dalla leadership delle grandi aziende tecnologiche. Tale modello ha consentito una forte capacità di sviluppo industriale e di scalabilità globale, ma ha anche prodotto una significativa concentrazione di potere in capo a pochi operatori privati.



La **Cina**, invece, ha sviluppato un approccio fortemente orientato al controllo strategico statale delle tecnologie digitali, integrando trasformazione tecnologica, sicurezza nazionale e politica industriale.



L'**Unione Europea** si colloca in una posizione differente, cercando di coniugare innovazione tecnologica, competitività economica e tutela dei diritti fondamentali. Il modello europeo punta a promuovere una trasformazione digitale coerente con i principi democratici, lo Stato di diritto, la protezione dei dati personali e la trasparenza algoritmica. Iniziative normative come il **Digital Services Act**, il **Digital Markets Act** e l'**AI Act** riflettono il tentativo europeo di costruire un ecosistema tecnologico più sicuro, equo e resiliente.

In questo contesto, la sovranità tecnologica non implica isolamento o autosufficienza assoluta. Piuttosto, indica la capacità di ridurre dipendenze critiche, proteggere asset strategici e preservare autonomia decisionale in un ambiente globale sempre più competitivo e interdipendente. La questione non è chiudersi al mondo, ma evitare che il mondo possa spegnerti l'interruttore.

1.4 Tecnocrazia, modelli di governance tecnologica e concentrazione del potere digitale

L'evoluzione degli ecosistemi digitali globali ha alimentato il dibattito sul rapporto tra tecnologia, democrazia e concentrazione del potere. In tale contesto, alcune correnti culturali e imprenditoriali emerse all'interno dell'ecosistema tecnologico statunitense hanno promosso una visione della tecnologia non soltanto come motore economico, ma come possibile elemento di ridefinizione dei modelli tradizionali di governance politica ed economica.



Il modello **democratico-liberale** statunitense storicamente fondato sull'equilibrio tra mercato, istituzioni democratiche, innovazione privata e regolazione pubblica.

Il modello **tecno-libertario** esasperato di **Peter Thiel** attribuisce crescente centralità alle infrastrutture digitali private, alle capacità computazionali e alle grandi piattaforme come principali motori di progresso, efficienza e governance. Nel saggio *The Education of a Libertarian* del 2009, Thiel esprime una critica nei confronti delle democrazie contemporanee, considerate eccessivamente lente e burocratiche rispetto alla velocità dell'innovazione tecnologica. Secondo tale impostazione, i processi democratici tradizionali e l'eccessiva regolazione rischierebbero di rallentare innovazione, competitività e sviluppo tecnologico.



All'interno di questa visione, la tecnologia assume progressivamente un ruolo di infrastruttura di potere, favorendo l'emergere di modelli tecnocratici nei quali capacità computazionale, controllo dei dati e infrastrutture digitali diventano elementi centrali della governance contemporanea. Il concetto di tecnocrazia si riferisce infatti a sistemi nei quali il potere tende a concentrarsi nelle mani di soggetti dotati di competenze tecniche, controllo infrastrutturale o superiorità tecnologica.

Pur partendo da presupposti ideologici profondamente differenti, alcuni modelli tecnolibertari occidentali e il paradigma tecnologico cinese condividono una crescente centralità della tecnologia come infrastruttura di potere e governance. In entrambi i casi, il controllo di dati, capacità computazionale, piattaforme e infrastrutture digitali tende ad assumere un valore strategico superiore rispetto ai tradizionali strumenti economici e industriali.

L'Unione Europea tenta invece di sviluppare una terza via fondata sul concetto di sovranità tecnologica democratica, cercando di coniugare innovazione, competitività economica e tutela dei diritti fondamentali. In questo scenario, il tema della sovranità tecnologica non riguarda esclusivamente sviluppo industriale o innovazione economica, ma la capacità degli Stati democratici di preservare autonomia decisionale, pluralismo e controllo sulle infrastrutture critiche della società digitale.

2.IMPATTI DEMOCRATICI E NUOVE DIPENDENZE

2.1 Trasformazione digitale e impatti sulla cittadinanza democratica

La trasformazione digitale ha modificato profondamente il rapporto tra cittadini, istituzioni e informazione, ridefinendo gli spazi della partecipazione democratica e della comunicazione pubblica. Le piattaforme digitali rappresentano oggi uno dei principali luoghi nei quali si formano opinione pubblica, consenso sociale e dibattito politico.

Questa evoluzione ha favorito nuove opportunità di inclusione, accesso alla conoscenza e partecipazione. Tuttavia, ha anche generato criticità rilevanti per il funzionamento delle democrazie contemporanee. La concentrazione del dibattito pubblico all'interno di piattaforme private globali attribuisce a soggetti non statali una capacità significativa di influenzare la circolazione delle informazioni, la visibilità dei contenuti e, indirettamente, la formazione dell'opinione pubblica. Algoritmi di raccomandazione, sistemi pubblicitari e meccanismi di profilazione possono incidere sulla qualità del dibattito democratico, favorendo polarizzazione, manipolazione informativa e diffusione di contenuti disinformativi. La rapidità con cui le informazioni vengono prodotte e distribuite rende inoltre più complessa la distinzione tra contenuti verificati, propaganda e manipolazione.

Le campagne di disinformazione, spesso amplificate da strumenti automatizzati e reti coordinate, rappresentano oggi un elemento stabile della competizione geopolitica. In questo scenario, la tutela della qualità dell'informazione e della partecipazione democratica assume una rilevanza strategica crescente. La democrazia non si difende più soltanto nelle istituzioni, ma anche negli spazi digitali in cui si costruisce il consenso.

2.2 Diseguaglianze digitali e nuove forme di dipendenza

La trasformazione tecnologica non produce effetti uniformi all'interno della società. Persistono differenze significative legate all'accesso alle infrastrutture digitali, alle competenze tecnologiche e alla capacità di utilizzo consapevole degli strumenti digitali. Il *digital divide* non riguarda più soltanto la disponibilità di connessione o dispositivi, ma comprende aspetti economici, culturali, territoriali e formativi.

La digitalizzazione crescente dei servizi pubblici, dell'istruzione, del lavoro e dell'informazione rischia di amplificare vulnerabilità sociali preesistenti. In un contesto sempre più digitale, la mancanza di competenze tecnologiche o di infrastrutture adeguate può tradursi in una riduzione concreta delle opportunità di partecipazione economica, sociale e democratica.

Accanto alle disuguaglianze sociali emergono nuove forme di dipendenza tecnologica. La forte concentrazione del mercato digitale globale in pochi grandi operatori internazionali determina un crescente livello di dipendenza da piattaforme, infrastrutture cloud, sistemi operativi, semiconduttori e servizi tecnologici sviluppati prevalentemente al di fuori dei confini nazionali o europei. Queste dipendenze possono limitare la capacità degli Stati di esercitare pienamente il controllo sui propri asset strategici, esponendo istituzioni e sistemi economici a vulnerabilità operative, economiche e geopolitiche. In tale scenario, la sovranità tecnologica assume anche una dimensione sociale: garantire accesso equo alle tecnologie e ridurre dipendenze critiche diventa essenziale per preservare coesione sociale, resilienza economica e stabilità democratica.

2.3 Libertà fondamentali, sicurezza e governance tecnologica

La crescente digitalizzazione della società pone un delicato equilibrio tra innovazione tecnologica, sicurezza e tutela delle libertà fondamentali. Tecnologie avanzate come intelligenza artificiale, sistemi di sorveglianza, riconoscimento biometrico e analisi predittiva offrono opportunità rilevanti in termini di efficienza, sicurezza e gestione dei servizi. Tuttavia, introducono anche rischi significativi per privacy, protezione dei dati personali, libertà individuali e pluralismo democratico.

L'utilizzo estensivo dei dati digitali può determinare forme sempre più pervasive di monitoraggio e profilazione, sia da parte di attori pubblici sia privati. In assenza di adeguati sistemi di governance, trasparenza e controllo democratico, l'evoluzione tecnologica rischia di compromettere principi fondamentali quali libertà di espressione, autodeterminazione individuale e uguaglianza davanti alle decisioni automatizzate.

L'approccio europeo alla governance digitale si inserisce proprio in questa prospettiva. Attraverso strumenti normativi come **GDPR**, **AI Act**, **Digital Services Act** e **Digital Markets Act**, l'**Unione Europea** mira a costruire un ecosistema tecnologico che coniughi innovazione, competitività e tutela dei diritti fondamentali. L'**AI Act**, in particolare, adotta un approccio basato sul rischio, prevedendo restrizioni e obblighi più stringenti per i sistemi che possono incidere su sicurezza, diritti e libertà delle persone.

La governance della tecnologia diventa quindi una questione non soltanto tecnica o economica, ma politica e istituzionale. Gli Stati democratici devono costruire ecosistemi digitali capaci di garantire sicurezza e resilienza senza compromettere libertà individuali e principi democratici. Il punto non è frenare l'innovazione, ma evitare che l'innovazione diventi un modo elegante per centralizzare controllo senza chiamarlo controllo.

3. SOVRANITA' TECNOLOGICA COME TUTELA DELLO STATO DEMOCRATICO

3.1 Sovranità tecnologica e autonomia strategica

Nel contesto geopolitico contemporaneo, la sovranità tecnologica rappresenta uno degli elementi centrali per la tutela della sicurezza, della resilienza economica e della stabilità democratica degli Stati. La crescente dipendenza da infrastrutture digitali globali, piattaforme tecnologiche e *supply chain* esterne ha trasformato la tecnologia in una componente essenziale dell'autonomia strategica nazionale ed europea.

La progressiva centralità di *cloud computing*, semiconduttori, reti di telecomunicazione, intelligenza artificiale e dati strategici evidenzia come il controllo delle infrastrutture digitali non rappresenti più soltanto una questione industriale, ma una dimensione fondamentale della capacità decisionale e operativa degli Stati moderni.

Il caso dei semiconduttori è particolarmente significativo. La **Commissione Europea** riconosce i chip come asset strategici per le catene industriali e per la trasformazione digitale, sottolineando come le recenti carenze globali abbiano reso evidente la dipendenza da un numero limitato di attori in un contesto geopolitico complesso.

Le recenti tensioni geopolitiche e la crescente esposizione a cyber minacce rafforzano la necessità di sviluppare capacità tecnologiche autonome, in grado di garantire continuità operativa, protezione delle infrastrutture critiche e indipendenza strategica nei settori chiave della trasformazione digitale. La sovranità tecnologica non coincide con autosufficienza assoluta, ma con la capacità di non trovarsi ostaggi delle proprie dipendenze.

3.2 Cybersecurity, resilienza e protezione delle infrastrutture critiche

La digitalizzazione crescente delle economie e delle istituzioni ha ampliato significativamente la superficie di esposizione a minacce cyber avanzate. Infrastrutture energetiche, telecomunicazioni, sistemi finanziari, sanità, trasporti e pubbliche amministrazioni dipendono oggi da ecosistemi digitali altamente interconnessi e vulnerabili ad attacchi sempre più sofisticati.

La cybersicurezza assume quindi una funzione sempre più vicina a quella tradizionalmente attribuita alla difesa strategica. Non si tratta soltanto di proteggere sistemi informatici, ma di garantire continuità operativa, fiducia istituzionale e stabilità democratica. Un attacco cyber contro una infrastruttura critica può produrre effetti economici, sociali e politici comparabili a quelli di una crisi fisica tradizionale.

La **Direttiva NIS2** istituisce un quadro comune europeo per aumentare il livello di cybersicurezza in settori critici, ampliando il perimetro di applicazione, rafforzando requisiti di gestione del rischio, obblighi di segnalazione e strumenti di cooperazione tra Stati membri.

Anche il panorama delle minacce conferma questa centralità. **ENISA** evidenzia come i gruppi cyber stiano prendendo di mira in modo sempre più sistematico la resilienza delle infrastrutture digitali europee, sfruttando vulnerabilità, dipendenze e interconnessioni lungo le *supply chain*.

In tale contesto, la resilienza tecnologica non riguarda esclusivamente aspetti tecnici, ma la capacità dello Stato di mantenere continuità operativa e proteggere servizi essenziali anche in presenza di crisi digitali o tensioni geopolitiche. La sicurezza digitale diventa così una componente strutturale della sicurezza democratica.

3.3 Tecnologia, democrazia e resilienza istituzionale

La sovranità tecnologica assume una rilevanza crescente anche nella protezione dei processi democratici e delle istituzioni pubbliche. La dipendenza da piattaforme digitali esterne, infrastrutture cloud concentrate e servizi tecnologici gestiti da soggetti transnazionali può generare vulnerabilità sistemiche difficilmente controllabili a livello nazionale.

Le istituzioni europee hanno progressivamente riconosciuto come autonomia strategica e resilienza democratica siano sempre più interdipendenti. La capacità di preservare controllo sui dati, garantire continuità dei servizi pubblici digitali e ridurre dipendenze critiche rappresenta oggi un elemento fondamentale per la tutela dello Stato di diritto e della sovranità democratica.

Anche sul piano nazionale, la *Strategia Nazionale di Cybersicurezza italiana* evidenzia la necessità di rafforzare capacità operative, protezione delle infrastrutture strategiche e autonomia tecnologica come condizioni per la sicurezza e la resilienza del Paese. Questo livello nazionale è importante perché consente di collegare il quadro europeo alle priorità concrete dello Stato italiano.

La resilienza istituzionale non dipende più soltanto dalla robustezza delle norme o dall'efficienza degli apparati pubblici, ma anche dalla capacità di proteggere le infrastrutture digitali attraverso cui tali apparati operano.

La democrazia contemporanea vive dentro sistemi informativi, reti, piattaforme e basi dati. Fingere che siano “solo strumenti” è un modo elegante per non vedere dove si sta spostando il potere.

3.4 Dignità umana e intelligenza artificiale: una chiave etica e antropologica

Il dibattito contemporaneo sulla sovranità tecnologica e sulla governance digitale ha assunto una rilevanza crescente anche sul piano etico, culturale e antropologico. La pubblicazione dell'enciclica *Magnifica humanitas* di **Papa Leone XIV**, dedicata alla custodia della persona umana nel tempo dell'intelligenza artificiale, rappresenta un segnale significativo di questa evoluzione. Il documento, pubblicato il **25 maggio 2026** e firmato il 15 maggio in coincidenza con il 135° anniversario della *Rerum novarum*, colloca la rivoluzione digitale nel solco delle grandi trasformazioni sociali affrontate dalla dottrina sociale della Chiesa.

L'enciclica propone una lettura dell'intelligenza artificiale non come tecnologia neutrale, ma come strumento che assume il volto di chi la pensa, la finanzia, la regola e la utilizza. Questo passaggio è particolarmente rilevante per il presente *White Paper*, perché consente di collegare il tema della sovranità tecnologica a una dimensione più profonda: quella della dignità umana, della responsabilità e del bene comune.

Il richiamo di **Papa Leone XIV** al “disarmo” dell'intelligenza artificiale introduce una prospettiva critica rispetto all'uso delle tecnologie digitali come strumenti di dominio, esclusione o morte. La questione non riguarda soltanto la regolazione dei sistemi AI, ma il modello di società che tali sistemi contribuiscono a costruire. Se l'intelligenza artificiale viene sviluppata esclusivamente secondo logiche di profitto, competizione geopolitica o superiorità militare, il rischio è che la tecnologia si trasformi da strumento di progresso a infrastruttura di disumanizzazione.

Questa chiave di lettura si intreccia direttamente con i temi centrali del documento: concentrazione del potere digitale, dipendenza da piattaforme globali, tutela dei diritti fondamentali, governance democratica e autonomia strategica. L'enciclica ricorda che la sovranità tecnologica non può essere ridotta alla capacità di possedere infrastrutture o sviluppare tecnologie autonome. Essa implica anche una responsabilità collettiva nel garantire che l'innovazione rimanga orientata alla persona, alla giustizia sociale e alla pace.

In questo senso, la riflessione etica e antropologica non è un'aggiunta ornamentale al dibattito geopolitico, ma una sua componente essenziale. Quando intelligenza artificiale, dati e infrastrutture digitali incidono sulla libertà, sul lavoro, sull'informazione e sulle decisioni pubbliche, la questione tecnologica diventa inevitabilmente una questione umana.

4. RACCOMANDAZIONI STRATEGICHE

4.1 Rafforzare la sovranità tecnologica europea

La crescente competizione geopolitica nel dominio digitale evidenzia la necessità di rafforzare la sovranità tecnologica europea attraverso investimenti strategici, sviluppo industriale e riduzione delle dipendenze critiche da attori extraeuropei. La capacità di controllare infrastrutture digitali, *supply chain* tecnologiche e dati strategici rappresenta oggi un elemento centrale della resilienza economica e democratica dell'**Unione Europea**.

Il rafforzamento della sovranità tecnologica richiede un approccio coordinato su più livelli. Da un lato, occorre sostenere capacità industriali europee nei settori dei semiconduttori, del cloud, dell'intelligenza artificiale, della connettività e della cybersicurezza. Dall'altro, è necessario promuovere standard comuni, interoperabilità e infrastrutture condivise in grado di rafforzare l'autonomia strategica senza trasformarla in isolamento.

Il programma europeo per il **Decennio Digitale** definisce obiettivi e meccanismi di cooperazione tra **Commissione** e Stati membri, concentrandosi su competenze digitali, infrastrutture sicure e sostenibili, digitalizzazione delle imprese e servizi pubblici digitali.

La sovranità tecnologica europea deve quindi essere intesa come capacità di scelta. Non chiusura, non autarchia, non nostalgia industriale con il Wi-Fi. Piuttosto, possibilità concreta di decidere quali tecnologie utilizzare, secondo quali regole, con quali garanzie e con quale livello di controllo pubblico.

4.2 Investire in resilienza e cybersecurity

La cybersicurezza rappresenta una componente essenziale della sicurezza nazionale e della stabilità democratica. La crescente esposizione delle infrastrutture digitali a minacce cyber avanzate richiede un approccio sistemico orientato alla resilienza, alla prevenzione e alla cooperazione tra settore pubblico e privato.

Investire in cybersicurezza significa rafforzare capacità di monitoraggio, *incident response*, *threat intelligence*, gestione del rischio e protezione delle *supply chain*. Significa inoltre sviluppare procedure coordinate a livello nazionale ed europeo, in modo da garantire continuità operativa anche in presenza di attacchi o crisi sistemiche.

La **Direttiva NIS2** rafforza il quadro europeo di protezione delle infrastrutture critiche, introducendo requisiti di governance, gestione del rischio, obblighi di segnalazione e strumenti di cooperazione transfrontaliera.

La protezione delle infrastrutture digitali deve dunque essere considerata una priorità politica e strategica, non soltanto tecnica. In un sistema democratico digitalizzato, la disponibilità e l'integrità dei servizi essenziali incidono direttamente sulla fiducia dei cittadini nelle istituzioni.

4.3 Costruire competenze e cultura digitale

La sovranità tecnologica non può essere perseguita esclusivamente attraverso infrastrutture e investimenti industriali. La disponibilità di competenze avanzate rappresenta uno dei principali fattori competitivi nel contesto digitale globale. Senza capitale umano qualificato, anche le migliori strategie restano dichiarazioni ben impaginate, cioè l'habitat naturale della retorica istituzionale. È necessario promuovere alfabetizzazione digitale diffusa, formazione specialistica in intelligenza artificiale e *cybersecurity*, aggiornamento continuo della pubblica amministrazione e collaborazione stabile tra università, ricerca, industria e istituzioni. Le competenze digitali non sono soltanto un fattore economico, ma una condizione per la cittadinanza consapevole e la partecipazione democratica.

Il **Decennio Digitale** europeo individua nelle competenze una delle direttrici principali della trasformazione digitale, insieme a infrastrutture, imprese e servizi pubblici.

La cultura digitale deve quindi essere costruita a più livelli: tecnico, civico, amministrativo e strategico. Una società che utilizza tecnologie complesse senza comprenderne impatti, limiti e rischi diventa più vulnerabile a manipolazione, esclusione e dipendenza.

4.4 Promuovere una governance democratica dell'intelligenza artificiale

L'intelligenza artificiale rappresenta una delle tecnologie più trasformative del contesto contemporaneo, con impatti rilevanti su economia, sicurezza, informazione e diritti fondamentali. Per tale motivo, è essenziale promuovere modelli di governance dell'AI fondati su trasparenza, accountability, supervisione umana e centralità della persona.

L'**AI Act** europeo introduce un approccio regolatorio basato sul rischio, distinguendo tra sistemi a rischio minimo, limitato, alto e inaccettabile. Tale impostazione mira a garantire che i sistemi più impattanti siano sottoposti a obblighi più stringenti in termini di sicurezza, controllo umano, documentazione e tutela dei diritti fondamentali.

Una *governance* democratica dell'AI dovrebbe prevedere trasparenza algoritmica, auditabilità dei modelli, valutazione degli impatti sui diritti, controllo umano significativo e responsabilità chiara lungo l'intero ciclo di vita dei sistemi. Tali principi sono particolarmente importanti nei settori ad alto impatto, come giustizia, sanità, lavoro, sicurezza, credito e pubblica amministrazione.

L'obiettivo non è ostacolare l'innovazione, ma garantire che l'innovazione non eroda le condizioni stesse della democrazia. L'AI può sostenere servizi pubblici, ricerca, produttività e sicurezza, ma deve rimanere sottoposta a regole, responsabilità e controllo democratico. Altrimenti si finisce a delegare decisioni sociali a modelli opachi addestrati da soggetti che rispondono prima al mercato che alla cittadinanza.

4.5 Rafforzare cooperazione internazionale e autonomia strategica

La natura globale delle infrastrutture digitali rende necessario sviluppare modelli di cooperazione internazionale capaci di coniugare interoperabilità, sicurezza e autonomia strategica. Nessuno Stato democratico può affrontare da solo la complessità delle *supply chain* tecnologiche, delle cyber minacce e della governance dell'intelligenza artificiale.

L'**Unione Europea** è chiamata a rafforzare il coordinamento con partner internazionali, organizzazioni multilaterali e alleanze strategiche, promuovendo standard condivisi e modelli di governance coerenti con principi democratici. La cooperazione internazionale deve però essere accompagnata da una maggiore capacità europea di investimento, produzione e controllo sugli asset tecnologici critici.

Autonomia strategica e cooperazione non sono concetti opposti. Al contrario, una cooperazione efficace richiede soggetti capaci di contribuire in modo autonomo e credibile. La dipendenza passiva non è cooperazione; è soltanto *outsourcing* con una *brochure* migliore.

In questa prospettiva, l'Europa dovrebbe rafforzare la propria diplomazia tecnologica, sostenere ricerca e innovazione coordinate, promuovere standard internazionali su AI e cybersecurity e costruire partnership resilienti con Paesi e organizzazioni che condividono principi democratici e tutela dei diritti fondamentali.



CONCLUSIONI

La trasformazione digitale ha progressivamente ridefinito il rapporto tra tecnologia, potere e democrazia, rendendo infrastrutture digitali, dati, piattaforme e intelligenza artificiale elementi centrali degli equilibri geopolitici contemporanei. In tale contesto, la sovranità tecnologica emerge non soltanto come questione economica o industriale, ma come componente essenziale della resilienza democratica, della sicurezza nazionale e della tutela delle libertà fondamentali.

La crescente concentrazione del potere tecnologico, le dipendenze infrastrutturali globali e la competizione strategica tra differenti modelli di governance evidenziano la necessità di sviluppare approcci capaci di coniugare innovazione, sicurezza e diritti. La tecnologia non rappresenta un elemento neutrale, ma una dimensione attraverso cui si esercitano influenza economica, capacità politica e controllo strategico.

L'Unione Europea sta cercando di costruire un modello fondato su autonomia strategica, regolazione democratica e centralità della persona umana, promuovendo una via alternativa sia alla centralizzazione statale del potere tecnologico sia alla concentrazione privata degli asset digitali. In tale prospettiva, strumenti normativi, investimenti infrastrutturali, sviluppo di competenze e cooperazione internazionale assumono un ruolo decisivo per preservare pluralismo, resilienza e autonomia decisionale.

La sfida dei prossimi anni non riguarderà esclusivamente la capacità di sviluppare tecnologie avanzate, ma soprattutto la possibilità di governarle in modo coerente con principi democratici, diritti fondamentali e stabilità istituzionale. La sovranità tecnologica si configura quindi come uno dei principali temi strategici del XXI secolo, destinato a influenzare profondamente il futuro delle democrazie contemporanee.

Per anni la tecnologia è stata raccontata come fattore neutrale di progresso ed efficienza. Oggi appare evidente che essa rappresenta anche una questione di potere, libertà e modello di società. Quando cloud, AI, dati e infrastrutture digitali incidono sulla capacità stessa degli Stati di esercitare autonomia politica e tutela democratica, la trasformazione digitale non riguarda più soltanto l'innovazione: riguarda il futuro della democrazia.

BIBLIOGRAFIA

- ACN, Strategia Nazionale di Cybersicurezza 2022-2026.
<https://www.acn.gov.it/portale/strategia-nazionale-cybersicurezza>
- Commissione Europea, AI Act.
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- Commissione Europea, Common European Data Spaces.
<https://digital-strategy.ec.europa.eu/en/policies/data-spaces>
- Commissione Europea, Digital Decade Policy Programme 2030.
<https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030>
- Commissione Europea, Digital Markets Act.
https://digital-markets-act.ec.europa.eu/index_en
- Commissione Europea, Digital Services Act.
<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- Commissione Europea, EU Cybersecurity Strategy.
<https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>
- Commissione Europea, European Chips Act.
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en
- Commissione Europea, European Strategy for Data.
<https://digital-strategy.ec.europa.eu/en/policies/strategy-data>
- Commissione Europea, NIS2 Directive.
<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- Commissione Europea, The Future of European Competitiveness, Rapporto Draghi.
https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en
- Consiglio d'Europa, Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.
<https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- ENISA, Threat Landscape 2025.
<https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
- NATO, Emerging and Disruptive Technologies Strategy.
https://www.nato.int/cps/en/natohq/official_texts_187617.htm
- OECD, AI Principles. <https://oecd.ai/en/ai-principles>
- OECD, Reinforcing Democracy Initiative.
<https://www.oecd.org/governance/reinforcing-democracy/>

- Parlamento Europeo, Technological Sovereignty.
[https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)659387](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)659387)
- Peter Thiel, The Education of a Libertarian, Cato Unbound, 2009.
<https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/>
- Stanford Encyclopedia of Philosophy, Technocracy.
<https://plato.stanford.edu/entries/technocracy/>
- UNESCO, Recommendation on the Ethics of Artificial Intelligence.
<https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- Vatican News, Magnifica humanitas.
<https://www.vaticannews.va/it/papa/news/2026-05/papa-leone-xiv-prima-enciclica-magnifica-humanitas-ia-25-maggio.html>



Cyber & Cyber tratta le principali tematiche che alimentano il settore: sicurezza, tecnologie, dati, policy, malware, hacking, difesa nazionale, guerra ibrida e geopolitica. Non insegue la notizia del giorno, ma guarda con particolare attenzione alla ricostruzione di scenari, alla valutazione dei contesti nazionali, all'analisi dei casi di studio, alla descrizione delle tecnologie, agli equilibri internazionali, il tutto nei principali domini fisici: terra, acqua, aria e spazio.

È anche e soprattutto un circuito autorevole di competenze (e un tessuto connettivo di aziende, università, centri di ricerca e singoli professionisti), che promuove occasioni di incontro e confronto come conferenze, workshop e appuntamenti conviviali, tra i membri della community.

CONTATTI



<https://cyberandcyber.com>



Cyber & Cyber



Cyber & Cyber



cyberandcyber