AI, Big Data e Cybersecurity: per una sovranità tecnologica europea e costituzionale[1]

di Oreste Pollicino[2]

Vorrei partire da un punto semplice, ma decisivo. Questo rapporto[3], curato da IFAB, ASTRID e OXERIA non è solo un documento tecnico. È un esercizio di visione. Perché oggi parlare di tecnologie strategiche – di intelligenza artificiale, di Big Data, di supercalcolo, di cloud – significa parlare del modo in cui un Paese sceglie di stare nel mondo. Significa decidere chi controlla l'infrastruttura digitale e, in fondo, chi controlla il futuro.

L'Italia, come mostra il documento, si trova in una fase cruciale. Abbiamo imprese eccellenti, università di livello internazionale, un capitale umano che può dire la sua. Ma abbiamo anche un sistema di piccole e medie imprese che fatica a tenere il passo, un mercato frammentato e un quadro normativo che spesso cambia più velocemente di quanto le imprese riescano ad adattarsi.

La domanda è: come facciamo a colmare questo divario, senza snaturare i principi che ci rendono europei – e, direi, costituzionalmente umani?

1. *Dalla iper-regolazione alla strategia industriale*

Il primo messaggio del rapporto è chiarissimo: non servono altre norme. Serve attuare bene quelle che già abbiamo. Negli ultimi anni l'Europa ha costruito una vera "costituzione del digitale": GDPR, AI Act, Data Act, Cyber Resilience Act,

[1] Intervento al seminario su "Quali policy per le tecnologie strategiche del XXI secolo?", tenutosi il 24 ottobre 2025, presso la Fondazione Astrid (Roma, Corso Vittorio Emanuele II n. 142) e organizzato dall'Osservatorio sulle dinamiche dell'IA della Fondazione, in collaborazione con il Centro Nazionale di Ricerca in *HPC, Big Data* e *Quantum Computing* e l'*International Foundation Big Data and Artificial Intelligence for Human Development* (iFAB).

[2] Ordinario di diritto costituzionale e *AI Law*, Università Bocconi. *Founder* e *Managing Partner*, Pollicino & Partners AIdvisory.

[3] Vedi L. Megale; G. Mensah; A. Perrucci; E. Barelli; E. Gallo; G. Sechi; M. Zanaroli, *Quali policy per le tecnologie strategiche del XXI secolo?*, maggio 2025, accessibile al seguente link: https://www.astrid-online.it/static/upload/ifab/ifab-booklet-osservatorio_a4--1-1.pdf.

DORA, NIS2. Ma adesso la sfida non è scrivere nuove regole – è metterle in coerenza, semplificarle, renderle comprensibili.

Siamo bravissimi a regolare, meno bravi a far funzionare. E allora la raccomandazione che condivido pienamente è questa: dopo la stagione normativa, deve arrivare quella industriale. La regolazione deve diventare una leva di competitività, non un freno.

In altre parole, il diritto deve imparare a respirare al ritmo dell'innovazione, non a inseguirla. L'Italia, su questo, ha bisogno di una regia che tenga insieme Bruxelles, il governo e i territori, evitando di moltiplicare sovrastrutture che rallentano anziché semplificare.

2. *Un capitale digitale per le PMI*

C'è poi un'idea che trovo di grande valore nel documento: quella del "capitale informatico" pubblico. Significa che i dati, le infrastrutture, le competenze delle istituzioni non devono restare chiuse, ma diventare risorse condivise per le imprese – in particolare per le piccole e medie, che sono la spina dorsale del Paese.

È un'idea semplice, ma rivoluzionaria. Vuol dire passare da una logica di controllo a una logica di abilitazione. Lo Stato non deve solo vigilare: deve mettere a disposizione strumenti, ambienti di test, dati pubblici accessibili in sicurezza.

E qui entra in gioco la cybersicurezza. Perché questo modello di condivisione può funzionare solo se il dato pubblico è protetto, tracciabile, gestito in un ecosistema affidabile. In questo senso, il ruolo dell'Agenzia per la Cybersicurezza Nazionale è fondamentale: è la cerniera tra innovazione e sicurezza, tra apertura e tutela.

3. *Sovranità digitale non è chiusura*

La parola "sovranità" fa spesso paura. Ma nel mondo digitale non significa isolamento. Significa poter decidere come usare i dati, dove archiviarli, chi li elabora e con quali regole. È una sovranità interdipendente, fatta di cooperazione, non di muri.

Oggi l'Europa rischia la frammentazione: ogni Stato ha la sua strategia cloud, le sue regole sui dati, le sue infrastrutture. Il rapporto IFAB invita a superare questo labirinto: serve un mercato unico del dato e del cloud, integrato e sicuro. Solo così potremo

competere con Stati Uniti e Cina. Ma serve anche fiducia reciproca tra Stati membri, e una visione comune su dove vogliamo arrivare.

4. *Big Data e formazione: la vera infrastruttura è umana*

C'è un altro passaggio che mi ha colpito: quello sui Big Data. La sfida non è solo avere dati – è saperli usare. E qui emerge il grande tema del capitale umano.

L'Italia soffre una carenza strutturale di competenze STEM. Servono percorsi di formazione specializzata, ma anche una cultura digitale diffusa, che unisca competenza tecnica e senso critico. Dobbiamo formare persone che sappiano leggere un algoritmo ma anche capire le sue implicazioni etiche e sociali. È la logica dell'"educazione circolare" citata nel rapporto: imparare, disimparare, reimparare.

Senza questa formazione continua, la transizione digitale rischia di restare una transizione per pochi.

5. *Cloud ed Edge: la sicurezza nella prossimità*

Il documento dedica pagine molto chiare al tema del cloud e dell'Edge Computing. Non sono questioni tecniche per addetti ai lavori: sono scelte di architettura democratica.

Spostare i dati "ai margini", cioè vicino al punto in cui vengono generati, significa ridurre la vulnerabilità, migliorare la sicurezza e restituire controllo locale. L'Edge Computing, se ben regolato, può diventare un presidio di sovranità e un argine contro la concentrazione di potere nelle mani di pochi grandi provider globali.

Per questo è essenziale la sperimentazione pubblico-privata: testare, insieme, nuove soluzioni di Edge sicuro, sostenibile e interoperabile. È un terreno su cui l'Europa può giocare da protagonista, se saprà unire innovazione e sicurezza.

6. *Supercalcolo e chip: un'infrastruttura di libertà*

C'è poi il capitolo sull'High-Performance Computing. Qui l'Italia parte da una posizione di forza: il Tecnopolo di Bologna, i supercomputer del CINECA, la nuova Fondazione Chips-IT. Abbiamo il 7% della potenza di calcolo mondiale – ma serve una strategia per non disperdere questo vantaggio.

Le raccomandazioni parlano chiaro: meno interventi generici, più investimenti mirati, concentrati su centri e imprese ad alto potenziale. Serve anche una visione condivisa sui semiconduttori, sulla filiera del chip, sulla collaborazione con l'Europa. E occorre, soprattutto, rendere accessibili le capacità di calcolo anche alle PMI, magari attraverso un modello federato di risorse HPC: un'infrastruttura aperta, con standard comuni, che unisca pubblico e privato.

L'obiettivo è ambizioso ma concreto: fare del supercalcolo non solo uno strumento tecnico, ma una garanzia di libertà tecnologica.

7. Energia e sostenibilità: la nuova frontiera del digitale

C'è un passaggio, nel documento, che va preso molto sul serio: il legame tra AI ed energia. Un grande data center può consumare quanto una città di centomila abitanti. Se non rendiamo sostenibile questo modello, l'AI diventerà presto un lusso per pochi.

La transizione ecologica e quella digitale devono andare insieme. Senza energia accessibile, la sovranità tecnologica resta sulla carta. Servono regole più chiare, tempi certi per gli allacciamenti, incentivi per le rinnovabili e per l'efficienza delle infrastrutture digitali. Anche qui, la sostenibilità non è più solo ambientale: è costituzionale. È la condizione perché il diritto all'innovazione valga per tutti.

8. AI e Cybersecurity: due percorsi che si intrecciano

Il rapporto non lo dice in modo diretto, ma il collegamento è evidente: non esiste AI senza cybersecurity, e non esiste cybersecurity efficace senza AI.

L'intelligenza artificiale può essere una straordinaria risorsa per proteggere le reti, prevenire attacchi, individuare vulnerabilità. Ma se non è gestita in sicurezza, può diventare a sua volta un rischio sistemico.

Ecco perché serve una integrazione profonda tra governance dell'AI e sicurezza cibernetica, a partire dalle regole europee. Le valutazioni d'impatto sui diritti fondamentali (FRIA) previste dall'AI Act, ad esempio, dovrebbero essere coordinate con le analisi di rischio richieste da NIS2 e DORA. Non come adempimenti separati, ma come parti di un'unica architettura di fiducia.

È qui che la visione dell'ACN può dare un contributo decisivo: un approccio che unisce resilienza tecnologica e garanzie democratiche, dove la sicurezza non è una deroga ai diritti, ma la loro condizione di effettività.

9. Tre priorità operative

Se dovessi riassumere le linee d'azione per l'Italia, ne vedrei tre:

Primo, semplificare e coordinare. Creare un quadro unico di riferimento per le regole su AI, dati, cyber e infrastrutture. Meno frammentazione, più chiarezza.

Secondo, industrializzare la sicurezza. Far capire che la sicurezza non è un costo ma un vantaggio competitivo. Chi investe in sicurezza merita incentivi, non burocrazia.

Terzo, federare le risorse. Collegare università, centri HPC, imprese e istituzioni in una rete nazionale di AI e cybersecurity, capace di dialogare con l'Europa e di condividere potenza, dati e competenze.

10. Dalla strategia alla fiducia

In conclusione, il messaggio più profondo del rapporto IFAB è che la politica tecnologica è una politica dei diritti. Il modo in cui regoliamo l'AI, gestiamo i dati o costruiamo il cloud dice molto del tipo di società che vogliamo essere.

L'innovazione non deve sostituire la libertà, ma darle nuovi strumenti.
La sicurezza non deve limitare la democrazia, ma renderla più solida.
E la regolazione non deve bloccare la competitività, ma orientarla verso un futuro sostenibile.

Se riusciremo a unire queste tre dimensioni – innovazione, sicurezza e diritti – allora l'Italia potrà davvero giocare un ruolo da protagonista nel nuovo ecosistema digitale europeo. Perché, come dice il documento, la sfida non è solo tecnologica.
È, prima di tutto, una sfida di responsabilità.