

Dalla «sovranità digitale» alla «sovranità tecnologica»: lo *European Technological Sovereignty Package*

di Paolo Passaglia

1. – 3 giugno 2026: la Commissione presenta lo *European Technological Sovereignty Package*, un insieme di iniziative molto articolato, che segna il momento iniziale di un percorso di concretizzazione di istanze da tempo emerse e progressivamente radicatesi nella coscienza continentale. Istanze che, nei mesi anteriori, avevano conosciuto un processo di incubazione sotto l'insegna dell'affermazione di una «sovranità digitale» europea.

Per comprendere la portata di questo nuovo – a lungo atteso – *package*, non è forse ozioso soffermarsi sul significato della nozione di «sovranità digitale», della quale la neonata «sovranità tecnologica» sembra essere l'evoluzione.

XIX

2. – Negli ultimi anni, l'espressione «sovranità digitale» ricorre con sempre maggiore frequenza nelle trattazioni che attengono al diritto delle nuove tecnologie. Si può anzi constatare che, quando gli aspetti prettamente giuridici si accompagnano a considerazioni di altro genere (in particolare, di ordine geopolitico), il richiamo dell'espressione è divenuto praticamente inevitabile.

La frequenza nell'uso non può celare una certa difficoltà a cogliere il reale significato dell'espressione. E fors'anche un certo disagio nel dar concretezza all'abbinamento tra due termini che fino a non molto tempo fa sembravano appartenere a mondi distanti.

Se è vero che l'aggettivo «digitale» non è l'unico che viene oggi abbinato alla sovranità (si pensi alla «sovranità alimentare», ad esempio), ma questa constatazione non può valere, da sola, a giustificare l'uso invalso, andando piuttosto a rafforzare il disagio di cui sopra nel percepire il rischio di una qualche banalizzazione di un concetto così carico di significato e di implicazioni, quale di certo è la sovranità.

Quando si parla di enti «sovrani», in effetti, ci si riferisce, inevitabilmente, a enti che possono dirsi: *originari*, perché traggono la propria validità da sé stessi e non da altri; *supremi*, perché non riconoscono al loro interno alcuna autorità superiore; *indipendenti*, perché nella proiezione esterna si pongono in posizione di almeno parità rispetto a qualunque altro ente.

Di primo acchito, che questi attributi possano essere riferiti all'ambito digitale pare tutt'altro che scontato. Stante questa incertezza, il diritto comparato può rivestire una funzione di chiarificazione di grande importanza: a fronte di un concetto che neppure chi lo ha coniato, o almeno diffuso, è riuscito davvero a chiarire (P. Bellanger, *De la souveraineté en général et de la souveraineté numérique en particulier*, in *Les Echos*, 30/08/2011, parla, assai genericamente, di un «controllo del nostro presente e del nostro destino così come si manifestano e si orientano attraverso l'uso delle tecnologie e delle reti informatiche»), bisogna probabilmente rifarsi alle sue concretizzazioni nei vari ordinamenti per trarre qualche utile orientamento (sull'importanza del diritto comparato per comprendere la portata della «sovranità digitale», v. G. Smorto, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE Online*, 2023, n. 57).

3. – Un primo aspetto da sottolineare è l'applicazione profondamente frammentata del concetto.

La «sovranità digitale» non è un'espressione dotata di rilevanza apprezzabile nel dibattito statunitense, e lo stesso può dirsi per molti altri paesi, compresi alcuni di quelli nei quali le problematiche della regolamentazione delle nuove tecnologie si è manifestata prima e con più forza (il Brasile è un esempio emblematico, in tal senso).

La sovranità digitale viene evocata soprattutto in Europa e in Cina, nonché – in una accezione più ristretta – in Russia, dove si enfatizza l'«Internet sovrano».

È proprio da quest'ultimo che conviene partire, perché la legge del 2019 – che ha veicolato questa idea di sovranità nell'ottica di eliminare la diffusione di informazioni non attendibili pregiudizievoli agli interessi dei singoli e della collettività – si è tradotta in un effettivo rafforzamento dell'autorità dei pubblici poteri, in grado di sorvegliare l'Internet soprattutto grazie all'affermata *indipendenza* dal resto del mondo, conseguente a una partizione della rete capace di isolare la Russia. Come dire che il richiamo agli attributi tradizionali della sovranità è stato funzionale all'incremento delle possibilità di esercitare sulla rete poteri che la rete, in quanto struttura geneticamente interconnessa di matrice transnazionale, tenderebbe di per sé ad affievolire.

L'esperienza russa suggerisce una alternatività tra la preservazione della rete per come si è sviluppata e l'affermazione di una sovranità (digitale). Da qui si può partire per formulare due osservazioni.

La prima attiene agli Stati Uniti. La lettura appena proposta della sovranità digitale potrebbe spiegare il motivo per cui l'espressione non trova spazio Oltreoceano: la tendenziale rarefazione della regolamentazione e il far riferimento alle dinamiche del mercato nella strutturazione dei servizi digitali e della *governance* della rete appaiono assai poco compatibili con l'affermazione di una «sovranità» da parte dei pubblici poteri (se del caso, in nome del loro legame di rappresentanza con il popolo). In altri termini, la sovranità digitale si porrebbe come un'alternativa alla centralità dei privati e avrebbe quindi una valenza rivendicativa che l'attuale amministrazione evidentemente non ha (o meglio, che non ha sotto il profilo dell'esercizio diretto di una regolamentazione, restando impregiudicata la possibilità di

controllo dei grandi operatori digitali attraverso forme di condizionamento di tipo diverso). Non è probabilmente un caso che, quando l'espressione «*digital sovereignty*» (anche nella variante «*cyber-sovereignty*») compare, la sua funzione è – nel migliore dei casi – quella di avanzare dubbi sulla strategia che ne è alla base (cfr., ad es., U.S. Department of State, *United States International Cyberspace & Digital Policy Strategy*, May, 6, 2024, <https://2021-2025.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>: «l'ascesa di una crescente narrativa sulla sovranità digitale che è stata abbracciata da alcuni dei nostri stretti *partners* e alleati ha il potenziale per minare gli obiettivi chiave dell'economia digitale e della sicurezza informatica»).

La seconda osservazione riguarda la Repubblica popolare cinese, che ha fatto propria un'idea di sovranità digitale non troppo lontana da quella russa, nella misura in cui si associa a un controllo della rete e delle sue infrastrutture, sezionando, in qualche modo, la rete globale onde poterla porre sotto il controllo dell'apparato governativo. Emblematica, al riguardo, è la definizione di *cyber-sovereignty* data da Xi Jinping nel 2015, in occasione della *Second World Internet Conference*, a Wuzhen: «il diritto di ciascun paese di scegliere il proprio percorso di sviluppo di *Internet*, il proprio modello di gestione di *Internet*, le proprie politiche pubbliche concernenti *Internet*, e [il diritto] a partecipare in condizioni di parità alla *governance* del cyberspazio internazionale, evitando la cyber-egemonia e le interferenze negli affari interni da parte dei altri Paesi» (in inglese in S. Arsène, *Global Internet Governance in Chinese Academic Literature*, in *China Perspectives*, 2016, n. 2, 25 ss.).

Appare piuttosto lampante l'eco della definizione classica della sovranità, come supremazia interna e come indipendenza esterna. Nella specie, la concretizzazione di questi principi si traduce, però, in uno statocentrismo che giustifica e sostiene: (a) la difesa dello Stato dalle narrazioni sfavorevoli, controllando le informazioni diffuse *online*, (b) il controllo dello Stato sui dati (anche e soprattutto attraverso la loro localizzazione entro il territorio nazionale), (c) il rafforzamento della protezione della struttura tecnologica, onde ridurre la vulnerabilità all'influenza straniera e affermare la predominanza statale nello sviluppo della tecnologia informatica (cfr. H.T. Hung, *Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach*, in *Journal of Computational Social Science*, 2025, vol. 8, n. 24, <https://doi.org/10.1007/s42001-024-00346-8>).

4. – Poste queste premesse, si sarebbe tentati di abbinare il richiamo alla sovranità digitale a una limitazione della libertà sulla rete, nel quadro di sistemi che non si ispirano alla democrazia liberale. In quest'ottica, l'ostilità degli Stati Uniti sarebbe una conferma *a contrario*.

È a questo punto che si innesta il discorso da fare relativamente all'Unione europea e al suo impegno per il raggiungimento di una sovranità digitale. Una sovranità digitale che non può essere quella russa o cinese, ma che, al contempo, non può non segnare una divaricazione rispetto agli Stati Uniti, a meno che l'espressione non sia puramente pleonastica.

Per cogliere ciò che, nel contesto europeo, debba intendersi per «sovranità digitale», la strada più semplice è, ovviamente, rifarsi ai testi che sono stati prodotti. Non si tratta di testi normativi (almeno per ora), giacché di sovranità (ancora) «digitale» si parla solo in rapporti o studi che le istituzioni hanno reso pubblici. Neppure il testo più «solenne» fino a oggi adottato ha uno *status* che può ambire a qualcosa di più rispetto a quello di uno strumento di *Soft Law*. Il riferimento è alla Dichiarazione per la sovranità digitale europea, che è stata approvata il 18 novembre 2025, in occasione di un *summit ad hoc* svoltosi a Berlino.

Proprio la lettura di quest'ultimo testo risulta di grande interesse. Per un paio di motivi, come minimo.

(a) Innanzi tutto, nella parte iniziale, si ha un tentativo di definizione della «sovranità digitale». Anzi, se ne hanno almeno due. La sovranità viene subito definita come «la possibilità per l'UE e per gli Stati membri di agire autonomamente e di scegliere liberamente le proprie soluzioni»: la scelta del primo avverbio pone oggettivamente qualche problema, perché confonde l'autonomia con l'indipendenza, rischiando così di svilire il concetto che si vuole affermare. Il danno è peraltro in parte sanato da una seconda definizione, secondo cui sovranità digitale «significa assicurare che l'Europa possa agire con indipendenza e in maniera autodeterminata».

Se ci si fermasse, qui, al netto della confusione terminologica, si potrebbe ancora qualificare la sovranità digitale europea come la proiezione nel cyberspazio della sovranità appresa nei manuali di diritto costituzionale. Il fatto è che la Dichiarazione di Berlino consta di oltre 1.300 parole, di cui un sesto circa è contenuto nella parte iniziale, di taglio puramente definitorio (o forse declamatorio, a seconda dei punti di vista). E dalla lettura emergono elementi concettualmente incompatibili con la nozione di sovranità, per come consolidatasi nel sistema post-vestfaliano. In una rapida rassegna non possono omettersi, almeno: (i) l'impegno a strutturare il proprio sistema normativo, non già in maniera *sovrana*, bensì «in conformità con i principi internazionalmente accettati», sancendo così la subordinazione del proprio diritto a fonti esterne; (ii) il fatto che questa conclusione sia ribadita dai riferimenti che si evocano per l'inquadramento della propria azione autodeterminata, che si deve basare, nell'ordine, su «il diritto internazionale, il proprio diritto, i propri valori e interessi securitari»; (iii) l'estensione del riferimento alla capacità di agire con indipendenza nel mondo digitale ben oltre il titolare della sovranità o il suo esercente, accomunando «individui, imprese e istituzioni in Europa».

Evidentemente, non si sta parlando della stessa sovranità che integra uno degli elementi costitutivi dello stato.

(b) Il dubbio sulla tenuta concettuale della sovranità in ambito digitale si rafforza sensibilmente allargando l'analisi agli elementi di contorno dei primi paragrafi della Dichiarazione. Questi elementi, peraltro, sono di contorno solo se si intende definire la sovranità secondo i criteri tradizionali. Se, invece, si abbandona questo presupposto, ci si accorge che gli elementi in discorso sono, in realtà, centrali, per lo spazio che occupano e per l'enfasi con cui sono espressi.

Ciò che più conta, comunque, è che si tratta di elementi che non mirano a determinare o a precisare la qualità di un soggetto o di un attributo (*id est*, ciò che deve essere proprio del sovrano o della sovranità), ma che sono

volti, piuttosto, a disegnare *orientamenti* e *direttive di azione*, cioè a dare veste alla concretizzazione della sovranità che si afferma.

La «sovranità» si esprime, quindi, anche – e forse soprattutto – in riferimento a tre grandi indirizzi.

Il primo consiste nel rifiuto dell'«isolazionismo o [del] protezionismo», motivato dai «benefici della collaborazione con *partners* globali, *quando possibile*» (quest'ultimo inciso non milita esattamente a favore di una proiezione di autentica sovranità...). Si pongono così le basi per la ricerca di una «cooperazione internazionale con i [...] *partners* che condividono i valori e i principi europei», una cooperazione che sia efficace, ma che non si traduca in un «indebito affidamento ad attori esterni» (altro riferimento non proprio in linea con l'idea di indipendenza veicolata dal concetto di sovranità ...).

Il secondo indirizzo si lega proprio alla «conservazione dei valori democratici europei nel mondo digitale» e alla tutela di questi valori e delle democrazie europee, attraverso il rafforzamento di «sicurezza economica, competitività, resilienza e fiducia».

Il terzo si sostanzia in un'ulteriore definizione della sovranità digitale, come «la capacità degli Stati membri [ma presumibilmente anche della stessa Unione europea] di regolare la propria infrastruttura digitale, i propri dati e le proprie tecnologie».

A ben vedere, più che una definizione della sovranità, si è qui in presenza di un programma di politica del diritto. In effetti, appare chiaro che ciò che viene proposta è una serie di *policies*.

Ma se così è, allora la portata della Dichiarazione in esame cambia sensibilmente: essa non è tanto la rivendicazione di una «sovranità digitale», quanto semmai l'affermazione di un *impegno* a porre in essere politiche che possano produrre una situazione di fatto idonea a richiamare la sovranità, almeno nella sua dimensione esterna (non a caso è sull'indipendenza che si pone l'accento, oltre che sull'autonomia). D'altra parte, le preposizioni sono importanti: se si scrive una dichiarazione *per* la sovranità digitale, e non *sulla* sovranità digitale, evidentemente è perché la sovranità digitale è un obiettivo e non un dato di fatto.

Onde fugare i residui dubbi, è sufficiente andare oltre i capoversi introduttivi e proseguire la lettura scorrendo il lungo elenco di principi che «stabiliscono gli orientamenti e le priorità comuni», nell'ottica di assicurare con «coerenza, equilibrio e apertura» il rafforzamento della «capacità dell'Europea di agire nella sfera digitale».

5. – Riletta in questa luce la Dichiarazione di Berlino, le preoccupazioni teoriche per una torsione, se non addirittura per uno svilimento del concetto di sovranità risultano grandemente affievolite. Ad assumere una sicura centralità sono invece le strategie elaborate e l'agenda dettagliata delle azioni poste in essere o da porre in essere per giungere alla situazione di fatto auspicata (sul punto, v. A. Shoker, *Digital Sovereignty Strategies for Every Nation*, in *Applied Cybersecurity & Internet Governance*, 2022, n. 1, 1 ss.).

A questo proposito, la dottrina tende a individuare tre livelli: quello fisico (sovranità sull'infrastruttura fisica di *Internet* e sulle attività a essa connesse), quello del codice (sovranità sui nomi di dominio, sugli *standards*

di *Internet* e sulle normative) e quello dei dati (proprietà, flussi e utilizzo) (così, ad es., A. Chander – H. Sun, *Sovereignty 2.0*, in *Vanderbilt Journal of Transnational Law*, vol. 55, 2023, 292), con l'aggiunta del presupposto di fondo dato da un grado di sviluppo adeguato in seno alla società di competenze e di partecipazione digitali (cfr., ancora ad es., E. Görnemann, *Digital Sovereignty*, Berlin, Weizenbaum Institute, 2024, <https://doi.org/10.34669/wi.fund/2.de.web>).

Come dire che, in Europa, parlare di sovranità digitale (o tecnologica) implica, oggi, il dover sorvolare su tematiche capitali di qualunque discorso sulla sovranità, e cioè sulle sue caratteristiche, sulla struttura e sui suoi limiti. Parlare di sovranità digitale vuol dire descrivere quello che il non-ancora-sovrano deve e/o può fare per poter diventare sovrano.

Diventa quindi inevitabile uno spostamento dell'asse dell'attenzione, che dalla Dichiarazione di principio del novembre 2025 non può non dirigersi verso le misure che, a livello eurounitario, ma anche a livello nazionale, segnano il percorso da intraprendere per dar corpo alle aspirazioni.

Chiaramente non si parte da zero, perché anzi il diritto eurounitario può contare su un arsenale già considerevolmente sviluppato, specie nel livello c.d. del codice e in quello dei dati. Sarebbe, tuttavia, del tutto improvvido non ammettere che molto resta da fare e che di quello che è stato fatto una parte non irrilevante è ampiamente perfettibile (v., ad es., V.L. Benabou, *European Digital Sovereignty: From Naïveté to Sustainability?*, in *Network Law Review*, special issue *Industrial Policy and Competitiveness* (ed. Thibault Schrepel & Dirk Auer), Fall 2025, <https://www.networklawreview.org/benabou-digital-sovereignty/>).

Ha peraltro poco senso fare bilanci, a questo stadio. Nel novembre 2025 si è data «solennità» a un obiettivo, che era già presente nella politica eurounitaria ma che aveva probabilmente bisogno di essere fissato. Lo si è fatto; e si è anche disegnata una strategia che appare coerente con i principi di base dell'integrazione europea (D. Di Marco – S. Thabit Gonzalez – A. Kotsev – A. Friis-Christensen – M. Minghini et al., *Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty*, European Commission, Ispra, 2025, JRC144908). Quello che resta da chiarire è se la strategia sia compatibile con il contesto geopolitico in cui si inserisce, ma questo potrà essere valutato davvero soltanto *ex post*.

I primi elementi concreti per questa valutazione sono contenuti proprio nello *European Technological Sovereignty Package*, che intende proporre una strategia globale e articolata per raggiungere, appunto, l'obiettivo della «sovranità tecnologica».

6. – La ricostruzione sin qui svolta è stata rivolta a individuare le radici di questo *package*, ponendolo in continuità con una storia recente, ma già piuttosto ricca, a livello eurounitario. Una continuità che esiste, senza dubbio, ma che è lungi dal potersi dire assoluta: il mutamento dell'aggettivo da riferire alla sovranità è, di per sé, più che eloquente. Una continuità nella rottura, allora, giacché se la «sovranità tecnologica» è espressione che pare destinata a oscurare quella di «sovranità digitale», è altrettanto vero che i collegamenti tra le due sono molto stretti, pur nella loro diversità.

Onde dare concretezza a queste osservazioni possono richiamarsi le parole stesse che la Commissione utilizza per definire la «nuova» nozione: «La sovranità tecnologica indica la capacità dell'Europa di sviluppare, controllare e far crescere le tecnologie critiche, le infrastrutture, i servizi e i dati – inclusi gli ecosistemi digitali – che sorreggono la sua economia, la sua sicurezza e la sua società, riducendo al contempo i rischi e diversificando le catene di approvvigionamento e l'esposizione tecnologica, al fine di diminuire le dipendenze strategiche e resistere alle interferenze straniere» (Commissione europea, *Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy*, 03/06/2026, COM(2026) 503 final, <https://ec.europa.eu/newsroom/dae/redirection/document/129100>).

La definizione appena riportata non si discosta in maniera significativa dai contenuti rintracciabili nella Dichiarazione di Berlino sulla sovranità digitale. A cambiare, semmai, è l'impostazione di fondo: anziché partire dalla sfera digitale per poi andare a inglobare – in una strategia complessiva – tutto quanto a questa sfera si collega, si persegue, adesso, sin da subito, un approccio onnicomprensivo, nel quale la sovranità dell'Europa non si misura in relazione alla (sola) sfera digitale, bensì in relazione a tutto quanto determina le capacità tecnologiche e, con esse, anche la struttura della sfera digitale.

Le quattro iniziative nelle quali il *package* si sostanzia danno corpo a questa evoluzione concettuale.

(a) La prima iniziativa è la proposta di un nuovo regolamento, il c.d. *Chips Act 2.0*, che prende evidentemente spunto dallo *European Chips Act* (reg. UE 2023/1781 del 13 settembre 2023), destinato a venire abrogato. L'idea del *Chips Act 2.0* è quella di andare oltre i limiti sin qui mostrati dal diritto vigente e dalla politica dell'Unione, onde riuscire a concretamente rafforzare l'industria europea dei semiconduttori, riducendo le sue dipendenze strategiche, aumentando la domanda di chip e sostenendo la progettazione e la produzione di chip avanzati.

Lo *European Chips Act* ha prodotto qualche progresso, tuttavia è indubbio che l'UE sia tutt'oggi dipendente da Paesi terzi nella produzione avanzata di chip o nella progettazione di semiconduttori. Considerando l'evoluzione del mercato globale, soprattutto con le componenti legate all'intelligenza artificiale, si pone l'esigenza strategica di occupare una posizione e ritagliarsi quote di mercato ben più rilevanti rispetto a quelle attuali.

Più in particolare, si mira con il *Chips Act 2.0* a: migliorare le condizioni per gli investimenti e la competitività nel sistema dei semiconduttori (rafforzamento della ricerca, accelerazione delle procedure di autorizzazione, sviluppo industriale, coordinamento con *partners* strategici); stimolare la domanda dei chip (stabilimento di rapporti privilegiati tra produttori e utilizzatori di chip, stimolazione della domanda, anche attraverso la crescita economica); rafforzare l'offerta (finanziamento di progetti innovativi, individuazione di progetti strategici, attrazione di investimenti, istituzione di «*Semiconductor Regions of Excellence*»); aumentare la resilienza e ridurre le dipendenze (creazione di una piattaforma di fornitura di semiconduttori *business-to-business*, sostegno per i settori ripetutamente esposti a rischi sistemici, riduzione dell'eccessiva dipendenza da fornitori esterni).

(b) La seconda iniziativa è un'altra proposta di regolamento, il c.d. *Cloud and AI Development Act*, che nelle intenzioni della Commissione è chiamato a rafforzare la sovranità e la competitività europea relativamente a *cloud* e intelligenza artificiale.

A fronte della crescita esponenziale della domanda di intelligenza artificiale, l'UE risulta, al momento, un attore geopolitico marginale nella competizione globale. Si impongono, quindi, cambiamenti significativi nelle procedure di autorizzazione, nell'accesso ai finanziamenti, nell'uso di materiali e di energia, al fine di rendere l'Europa più competitiva nel contesto globale.

In questa logica, un ruolo centrale è assunto dai servizi *cloud*, per i quali, attualmente, si constata una dipendenza molto pronunciata da fornitori di Paesi terzi, con tutti i rischi che questo provoca in termini di sovranità dei dati.

Nel porre in essere queste misure, si individuano tre aree principali: «*Research, Development and Innovation*» (sostegno allo sviluppo di tecnologie all'avanguardia, specie in certi settori dell'intelligenza artificiale, introduzione di «*grand challenges*» per orientare impegni e obiettivi, garanzia dell'adozione di determinati *cloud* e sistemi di intelligenza artificiale in settori strategici); «*Capacity*» (triplicazione delle capacità dei *data centers* nell'UE entro i prossimi cinque/sette anni, semplificazione nell'autorizzazione dei *data centers*, agevolazioni nell'accesso alle risorse, garanzia di una capacità di elaborazione sufficiente); «*Autonomy*» (elaborazione di un quadro comune di valutazione del grado di sovranità tecnologica, accelerazione del lancio e dello sviluppo di sistemi di *cloud* e di intelligenza artificiale per settori critici, promozione dell'innovazione, rafforzamento del potere di acquisto delle amministrazioni, sostegno a soluzioni *open source*).

(c) La terza iniziativa consiste in una *EU Open Source Strategy* elaborata dalla Commissione, finalizzata a collocare l'*open source* al cuore del processo diretto all'affermazione della sovranità tecnologica.

L'obiettivo fondamentale è rafforzare gli ecosistemi digitali aperti, sia nel settore pubblico che in quello privato, attraverso lo sviluppo, l'espansione e l'attuazione della sostenibilità a lungo termine delle tecnologie *open source*. Queste tecnologie sono ritenute imprescindibili per ridurre significativamente la dipendenza da tecnologie provenienti da Paesi terzi e poter quindi assumere il controllo sulle infrastrutture digitali.

Il ricorso all'*open source* è visto come una situazione *win-win*, in cui all'affermazione della sovranità si associano maggiori possibilità di scelta, la riduzione delle barriere all'accesso a soluzioni *software* avanzate, il potenziamento della trasparenza, della sicurezza e dell'affidabilità, nonché la creazione di opportunità nuove di sviluppo della ricerca, mediante l'allargamento di ecosistemi collaborativi.

Perché questi obiettivi possano dirsi realistici, si impongono finanziamenti a lungo termine, lo sviluppo dei progetti esistenti e la risoluzione delle difficoltà riscontrate nel passaggio dall'innovazione all'implementazione industriale.

Allo stato, le soluzioni attualmente presenti sono molto frammentate, a livello europeo, il che si traduce in una capacità di sviluppo limitata, derivante dal valore economico relativo che viene generato da ciascun progetto *open source*. Per superare questa situazione, sono considerati

necessari un coordinamento più forte a livello europeo, un miglioramento dei meccanismi di finanziamento, una maggiore efficacia nel sostegno a modelli aziendali *open source* sostenibili.

Vengono individuate alcune aree di intervento prioritario, tra le quali la promozione di soluzioni *open source* in abbinamento ad alcune politiche europee (ad es., il portafoglio europeo di identità digitale e il portafoglio aziendale europeo), il rafforzamento della collaborazione tra e con gli Stati membri (in particolare attraverso il Consorzio europeo per le infrastrutture digitali comuni), la creazione delle condizioni perché le pubbliche amministrazioni possano interagire con i consociati mediante sistemi *open source*, lo sviluppo di nuovi elementi costitutivi *open source* in aree tecnologiche critiche (come sistemi operativi, *cloud*, intelligenza artificiale, sicurezza informatica, infrastrutture di sviluppo *software*, semiconduttori e future architetture *Internet*).

(d) Infine, la quarta iniziativa è l'elaborazione di una *Strategic Roadmap for Digitalisation and AI in Energy*. È forse questa l'iniziativa che, più di tutte, giustifica il mutamento terminologico della sovranità da «digitale» a «tecnologica». Viene, infatti, proposto un approccio a livello di sistema integrato, che parte dal presupposto secondo cui la digitalizzazione è un fattore abilitante della transizione energetica lungo tutta la catena del valore energetico (generazione, trasporto, distribuzione, fornitura e consumo). In buona sostanza, transizione digitale e transizione energetica non possono essere disgiunte, per la semplice ragione che l'una implica l'altra.

La *roadmap* proposta affronta il tema della crescente domanda energetica delle infrastrutture digitali e illustra come l'intelligenza artificiale possa contribuire a un sistema energetico pulito, competitivo e sicuro. Solo per fare qualche esempio tra i più evocativi, le soluzioni digitali possono aiutare a spostare i consumi nelle ore in cui l'elettricità è più economica, ma la digitalizzazione può anche migliorare l'efficienza, ottimizzando, grazie all'intelligenza artificiale, il funzionamento e la manutenzione della rete elettrica.

I pilastri fondativi della *roadmap* sono tre. Il primo è l'integrazione dei *data centers* nel sistema energetico, ciò che può prodursi attraverso un dialogo tra gli operatori dell'uno e dell'altro settore, con la partecipazione delle autorità pubbliche. Il secondo consiste nell'accelerazione dell'adozione di soluzioni digitali per il potenziamento della rete e per la diffusione dei contatori intelligenti. Il terzo è la costruzione di un quadro per la condivisione dei dati oltre le frontiere dell'UE, garantendo così una collaborazione transfrontaliera sicura.

Chiaramente, queste azioni rappresentano uno sviluppo e un approfondimento di piani di azione già in corso per la digitalizzazione dell'energia (cfr. *Digitalising the energy system – EU action plan*, COM/2022/552), segnatamente per il sostegno dello sviluppo di un mercato sostenibile e competitivo per i servizi energetici digitali, nel quadro di un sistema che tuteli la riservatezza e la sovranità dei dati e che sostenga gli investimenti nelle infrastrutture energetiche digitali.

7. – Un complesso di norme e programmi tanto ampio e variegato qual è lo *European Technological Sovereignty Package* non può essere condensato nelle poche righe che precedono; è ovvio. I suoi contenuti vanno approfonditi e, per così dire, metabolizzati, ciò che in queste pagine non era possibile, anche semplicemente per il fatto di essere state scritte a distanza di pochi giorni dalla presentazione.

Nonostante questa scarna e senz'altro troppo superficiale presentazione, si può comunque cogliere l'importanza del ruolo che il *package* è destinato a svolgere nel prossimo futuro. L'espansione dell'angolo visuale testimoniato dal mutamento dell'aggettivo che connota (l'obiettivo del) la sovranità, la moltiplicazione delle linee di intervento, l'approfondimento delle azioni rispetto al passato sono tutti indizi del fatto che il 3 giugno 2026 potrebbe segnare la data di inizio di una nuova fase, connotata da un approccio rinnovato dell'Unione europea nei confronti delle tematiche tecnologiche.

Senza troppi sforzi di immaginazione, si può sin da ora prevedere che sul *Tech Sovereignty Package* (come finirà forse per essere chiamato) i cultori del diritto delle nuove tecnologie avranno modo di concentrarsi a lungo. Ma il suo impatto è verosimile che sia tale da produrre effetti generali, attirando quindi l'attenzione di gran parte dei cultori del diritto dell'Unione.

E i comparatisti? La loro funzione non sarà affatto trascurabile. Anzi. Saranno chiamati a vagliare gli impegni e le realizzazioni alla luce degli obiettivi perseguiti, attraverso un confronto costante con gli altri attori geopolitici globali con i quali l'Unione europea non può non misurarsi (Stati Uniti e Cina *in primis*, evidentemente). Ma non solo: ai comparatisti spetterà il compito di monitorare il grado di armonia esistente tra i vari sistemi nazionali nel dar concretezza alle *policies* eurounitarie. Il compito sarà tanto delicato quanto essenziale, giacché uno dei fattori di debolezza che si è finora riscontrato con grande frequenza è stato proprio il diverso approccio proposto dai vari Stati membri, la difforme sensibilità sul tema della sovranità digitale e le conseguenti disparità negli impegni e, soprattutto, nelle realizzazioni.

L'auspicio è che il passaggio alla sovranità tecnologica possa tracciare anche il percorso verso una reale armonizzazione tra gli ordinamenti nazionali europei. E se proprio non dovesse raggiungersi il coordinamento di un'orchestra, sarebbe comunque auspicabile che, quanto meno, venissero cancellate le cacofonie delle iniziative troppo isolate.

Sui comparasti ricadrà l'onere di vigilare e, se del caso, segnalare. Prestando tutta l'attenzione che la crucialità della posta in gioco richiede.

Paolo Passaglia
Dip.to di Giurisprudenza
Università di Pisa
paolo.passaglia@unipi.it