Le politiche pubbliche europee per il digitale[1]

Antonio Manganelli, Luca Megale e Antonio Perrucci*

1. Premessa

L'Unione europea (UE), nel definire un nuovo approccio regolamentare al digitale, ha tenuto conto delle caratteristiche di pervasività di questa "tecnologia", che oramai investe l'intero sistema economico (e la società nel suo insieme). D'altro canto, la letteratura economica ha - da tempo - chiarito che le tecnologie digitali presentano le caratteristiche tipiche delle *general purpose technologies* (GPT), come indicate da Breshanan e Trajtenberg, trent'anni fa[2]. In sintesi, si tratta di tecnologie applicabili ai più vari settori e contesti, in continua evoluzione ed in grado di dar luogo a complementarità nell'innovazione e, quindi, di favorire l'innovazione anche nei settori che la utilizzano.

[1] Questo testo rappresenta una versione preliminare, che sarà oggetto di integrazione e revisione da parte degli autori, a seguito di un apposito seminario Astrid.

*Antonio Manganelli è professore straordinario presso l'Università di Siena e Research fellow presso il Centre on Regulation in Europe (CERRE). Luca Megale è ricercatore della Fondazione Astrid e Assegnista di ricerca in Diritto amministrativo, Università LUMSA di Roma. Antonio Perrucci è Direttore del Laboratorio sull'ecosistema digitale della Fondazione Astrid.

[2] T. F. Bresnahan e M. Trajtenberg, *General Purpose Technologies "Engines of Growth"?*, in *Journal of Econometrics*, 65, 1995, pp. 83-108.

ISSN 2038-1662

Di conseguenza, alla tradizionale regolazione settoriale dei mercati primariamente interessati dalla trasformazione digitale (comunicazioni elettroniche, audiovisivo, servizi postali), l'UE ha affiancato una serie di regolamenti di carattere orizzontale, che riguardano i mercati ed i servizi digitali, l'intelligenza artificiale e i big data[3].
Questo contributo si propone di illustrare e commentare il percorso avviato dall'Unione europea da quindici anni a questa parte, e che ora sta vivendo una particolare accelerazione. Nel capitolo 2, viene delineato lo stato della competizione internazionale nei principali mercati dell'ecosistema digitale – cloud, microchip, supercalcolo, reti satellitari, cavi sottomarini e large language model. Successivamente (cap. 3), si passa in rassegna il quadro normativo e di policy europeo sul digitale, articolato in otto cluster tematici. Si analizza quindi il passaggio dalla regolazione alla politica industriale (cap. 4), evidenziando i limiti strutturali dell'approccio regolatorio nel promuovere capacità produttive e scala competitiva. Il cap. 5 approfondisce l'evoluzione della politica industriale verso gli obiettivi di "sovranità digitale" e "autonomia strategica", distinguendo tra misure abilitanti e misure restrittive. Il cap. 6 esamina alcune criticità dell'evoluzione delle policy UE, con particolare riguardo all'implementazione della normativa da parte degli Stati membri e al recente ricorso alla tecnica legislativa dell'Omnibus. Infine, nel cap. 7 vengono formulate alcune considerazioni sulle azioni necessarie a rafforzare la sovranità digitale europea.

2. Lo stato dell'industria europea nell'ecosistema digitale

2.1 Le analisi sulla competizione internazionale nei mercati digitali

Le analisi sullo stato dell'industria digitale europea sono ormai numerose, sia di fonte istituzionale (Unione europea[4], Rapporto Draghi[5], Rapporto Letta[6]), sia svolte da centri studi, società di consulenza ed esperti.
Nel novero di queste analisi, è importante una distinzione di carattere metodologico, per i riflessi che può avere sull'impostazione delle politiche per il digitale europeo (e italiano). Accanto a un numero – limitato finora – di studi che considerano più settori tra quelli che compongono l'ecosistema digitale[7], si registrano numerose indagini che

[3] Ci si riferisce, in particolare, al Data Act ed al Data Governance Act, al Digital Markets Act, al Digital Services Act e al più recente Artificial Intelligence Act (vedi capitoli successivi).
[4] Si veda il successivo capitolo per la ricostruzione del percorso dell'Unione europea volto a definire una strategia digitale. In questo contesto, un particolare rilievo lo assume la comunicazione "*A Competiveness Compass for the EU*", con cui la Commissione - sulla base degli studi commissionati a Enrico Letta e Mario Draghi – ha presentato a fine gennaio 2025 la strategia per rafforzare la posizione economica dell'UE e colmare il divario di produttività rispetto ad altre economie globali.
[5] M. Draghi, *The future of European competitiveness*, settembre 2024.
[6] E. Letta, *Much more than a market*, aprile 2024.
[7] Non esiste una definizione consolidata di ecosistema digitale, anche se – generalmente – si intende l'insieme di industrie/settori/soggetti privati e pubblici che intervengono – a diversi livelli – nella produzione di beni e servizi digitali offerti agli utenti finali, alle imprese utilizzatrici, alla pubblica amministrazione. Una espressione affine è quella di filiera digitale. In questo ultimo caso, si assume

ISSN 2038-1662

si concentrano su uno specifico mercato (ad esempio, il cloud, l'high performance computing, l'intelligenza artificiale, nelle sue diverse articolazioni).
In ogni caso, queste analisi – anche quando estese a più settori – forniscono una visione necessariamente parziale della industria digitale dell'Unione europea (UE), e dei singoli paesi che vi fanno parte. In tal senso, risultano solo in parte utili all'impostazione di una strategia di politica industriale per il digitale che abbia una visione di (eco)sistema[8], superando quindi l'approccio fondamentalmente settoriale che ha caratterizzato fino ad ora l'iniziativa dell'UE. In particolare, con riguardo alle politiche per la transizione digitale, che rappresentano uno dei due pilastri del programma della Commissione von der Leyen (sia la precedente che l'attuale).
Tuttavia, qualcosa sta accadendo. Un tentativo interessante di fornire una visione d'assieme dell'economia digitale europea è quello di *Eurostack*, una iniziativa di soggetti privati[9] che propone "*una idea originale per la politica industriale europea…mettendo assieme tecnologia, governance e finanziamento di investimenti focalizzati sull'Europa per costruire ed adottare una suite di infrastrutture digitali: dalla connettività al cloud computing, all'intelligenza artificiale e alle piattaforme digitali*" [10].
Una seconda differenziazione delle analisi sullo stato di salute del digitale *Made in EU* riguarda i risultati conseguiti, dove prevale un tono generalmente pessimistico, anche se – in alcuni casi (ad esempio, per l'industria del supercalcolo) – le valutazioni sono decisamente positive.
Il tono degli interventi e delle analisi migliora, moderatamente, allorché si esaminino le prospettive dell'industria digitale UE, ossia la possibilità di recuperare terreno rispetto ai due paesi che dominano la competizione internazionale: Stati Uniti e Cina.

2.2 Un tentativo di sintesi, con riferimento ai principali mercati/industrie dell'ecosistema digitale

Un'analisi della collocazione dell'industria europea nell'ecosistema digitale a livello internazionale, mediante una accurata ricognizione dei dati resi disponibili da diverse

una visione "verticale", ossia si immagina una sequenza di processi produttivi caratteristici di una serie di industrie. Nel caso dell'ecosistema digitale si esaminano piuttosto le relazioni tra i diversi "protagonisti", che non si limitano alle imprese attive dal lato dell'offerta, ma contemplano anche le imprese utilizzatrici, i consumatori finali, la pubblica amministrazione e le istituzioni che svolgono un ruolo (autorità di governo e Parlamento, autorità amministrative indipendenti, in primo luogo). Per una definizione di ecosistema digitale, si rinvia ai lavori del Laboratorio sull'Ecosistema Digitale, della Fondazione Astrid.

[8] Si veda, P. Guerrieri, G. P. Manzella e F. Onida, *La politica industriale UE nelle sfide dell'autonomia strategica. Proposte e suggerimenti di policy*, 2026, p. 12, Astrid Rassegna, 2026.

[9] L'iniziativa, avviata da una conferenza *Towards European Digital Independence: Building the EuroStack*, nel settembre del 2024, conta ormai oltre trecento aderenti alla Fondazione, istituita nell'ottobre 2025.

[10] Citazione (traduzione propria) dal sito Eurostack.eu.

ISSN 2038-1662

fonti, costituisce un impegno straordinario, che va ben al di là delle finalità di questo contributo, ma anche di ben più attrezzati centri di ricerca, pubblici e privati. Non a caso, il Parlamento europeo - nella risoluzione adottata il 22 gennaio – ha richiesto "*the development of a comprehensive risk assessment framework to monitor and address dependencies across the digital value chain*"[11].

Premesso che, in generale, la dipendenza dell'economia UE da beni, servizi e infrastrutture digitali si colloca oltre l'80% secondo la stessa Commissione europea [12], in questo paragrafo, si forniscono alcune evidenze empiriche relativamente ad una selezione di mercati digitali, per i quali: da un lato, sono disponibili fonti statistiche internazionali affidabili, e, dall'altro lato, la Fondazione Astrid ha maturato una apprezzabile esperienza[13].

I mercati così selezionati assumono carattere complementare rispetto a quelli individuati nel Digital Markets Act (DMA), definiti come di piattaforma di base (*core platform services*)[14]. Questi ultimi, come è noto, sono caratterizzati dalla marcata dominanza delle grandi piattaforme digitali statunitensi, i cosiddetti GAFAM (Google, Amazon, Facebook, Apple, Microsoft)[15], che la regolamentazione unionale intende appunto contrastare.

---

[11] Risoluzione del Parlamento europeo del 22 gennaio 2026 sulla sovranità tecnologica europea e sulle infrastrutture digitali Sovranità tecnologica europea e infrastrutture digitali P10_TA(2026)0022, 2025/2007(INI),

[12] Risoluzione del Parlamento europeo del 22 gennaio 2026 sulla sovranità tecnologica europea e sulle infrastrutture digitali Sovranità tecnologica europea e infrastrutture digitali P10_TA(2026)0022, 2025/2007(INI); Commissione europea, *Relazione sullo stato del decennio digitale 2023 – Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*, COM(2023) 570 final, 27 settembre 2023.

[13] In particolare, dopo una ricerca sul Cloud ed il caso Gaia X, pubblicata nei paper Astrid (n.77), per l'editore Passigli sono usciti quattro volumi (i. *Industria dei cavi sottomarini. Tendenze di mercato e geopolitica*, AA.VV., Passigli Editori, 2022; ii. *Industria dei microchip. La strategia dell'Europa nella competizione internazionale*, AA.VV., Passigli Editori, 2022; iii. *Il calcolo ad alte prestazioni. Italia ed Europa nella competizione mondiale*, AA.VV., Passigli Editori, 2022; iv. *Industria dello spazio. Problemi e opportunità*, AA.VV., Passigli Editori, 2023), che riportano i risultati delle ricerche condotte rispettivamente su cavi sottomarini, microchip, high performance computing ed industria dello spazio. Sui modelli di intelligenza artificiale generativa è appena uscito un volume (*Modelli di intelligenza artificiale generativa e assetti di mercato*, AA.VV., Passigli Editori, 2026), sempre per Passigli, mentre è in corso, una ricerca sull'industria dei data center.

[14] Si tratta dei servizi digitali maggiormente usati da utenti commerciali ed utenti finali, quali: *a*) servizi di intermediazione online, *b*) motori di ricerca online, *c*) social network online, *d*) servizi di piattaforma per la condivisione video, *e*) servizi di comunicazione interpersonale (ad es., messaggistica online), *f*) sistemi operativi, *g*) browser web, *h*) assistenti virtuali, *i*) servizi di cloud computing e *l*) servizi di pubblicità online.

[15] Questa dominanza dei GAFAM si esprime nell'area occidentale del sistema economico internazionale, mentre in Asia, soprattutto nell'Asia dell'est, sono le piattaforme cinesi (Alibaba, Baidu, Tencent, in particolare) ad avere un notevole potere di mercato. L'acronimo GAFAM è quello più correntemente usato per indicare le grandi piattaforme digitali statunitensi, anche se altre imprese – sempre americane – hanno assunto un ruolo importante nell'ecosistema digitale. Accanto ad altri acronimi, che includono ulteriori e diverse imprese/piattaforme digitali (ad esempio, Netflix), si fa

ISSN 2038-1662

Sotto un profilo metodologico/classificatorio, quindi, si può assumere che dell'ecosistema digitale facciano parte sia i mercati delle infrastrutture fisiche, sia i mercati delle infrastrutture logiche (software) e dei contenuti digitali. Nel primo caso, si tratta delle reti di comunicazione elettronica (reti TLC fisse e mobili, reti satellitari, cavi sottomarini, torri di trasmissione), nonché dell'industria dei data center, dei microchip, dei supercalcolatori. Nel secondo caso, avendo a riferimento la tassonomia del DMA prima richiamata, assumono importanza le industrie del cloud, dei software per diversi settori verticali (ad esempio, per le reti di TLC), dei protocolli (le API, *application programming interface*), della cybersecurity, dei motori di ricerca, dei modelli e delle applicazioni di intelligenza artificiale (sia "tradizionale" che generativa – i *large language model* - ed agentica), nonché le varie applicazioni delle piattaforme, sia per la trasmissione di contenuti audiovisivi, sia per le comunicazioni interpersonali. Ciò premesso, di seguito, si rappresenta la situazione della competizione internazionale tra Stati Uniti Cina ed UE, in un numero selezionato di questi mercati, per cui sono possibili comparazioni internazionali, sulla base di dati pubblicamente disponibili[16].
Dall'ampio novero di industrie prima indicate, abbiamo selezionato sei settori, per i quali l'UE ha definito - o sta ridefinendo - una strategia di politica industriale: a) il cloud; ii) i microchip; iii) i supercalcolatori; iv) le reti satellitari; v) i cavi sottomarini; vi) l'intelligenza artificiale, ed in particolare i *large language model*.

Nel mercato del cloud, il dominio degli Stati Uniti, ossia delle sue imprese multinazionali, i cosiddetti hyperscaler, è indiscusso, da diverso tempo a questa parte: i 2/3 del mercato mondiale sono appannaggio di Amazon Web Services, Microsoft Azure, Google Cloud (con Oracle che sta aumentando la propria quota di mercato). Se dal mercato mondiale si passa a quello UE, il dato non cambia: i primi tre *hyperscaler* controllano il 63% del mercato. Anche il mercato asiatico, cinese in particolare, è dominato da poche grandi imprese: Alibaba Cloud (1/3 del mercato), Huawei Cloud (quota del 17% - 18%) e Tencent Cloud (circa il 10% del mercato). Nella UE, vi sono poche imprese di rilievo internazionale, peraltro specializzate in qualche specifico settore del cloud (in Germania, SAP e T-Systems di Deutsche Telekom; in Francia, OVH, Orange Business Services, Atos)[17]. In sintesi, siamo di fronte a mercati del cloud separati in due blocchi (Stati Uniti assieme all'Unione europea, Cina), dove dominano rispettivamente gli hyperscaler statunitensi e cinesi. L'Unione europea, al di là di alcune imprese che esprimono una certa capacità competitiva, è sostanzialmente un mercato dipendente dai fornitori americani. Per emanciparsi da questa preoccupante

ricorso anche ad espressioni quali Big Tech o Tech Giants, oppure hyperscalers, gatekeepers, anche se – in questi ultimi due casi – con riferimento a specifici contesti merceologici o regolamentari.

[16] Ovviamente, dai confronti internazionali sono escluse per definizione le reti TLC, dal momento che ogni paese realizza le proprie infrastrutture sul territorio nazionale e non esiste quindi un "commercio internazionale" di reti TLC.

[17] Per l'Italia, si segnalano TIM Entreprise (in collaborazione con Google ed Amazon) ed Aruba.

ISSN 2038-1662

situazione, la UE sta promuovendo un'infrastruttura cloud sovrana, sicura e indipendente dai colossi tecnologici statunitensi (vedi capitoli successivi).

Nel settore dei microchip, si riscontrano situazioni di dominanza differenziate lungo la catena del valore, ma sempre con un ruolo preponderante di aziende americane e del sud est asiatico.
Nelle attività di automazione e progettazione elettronica, ad alta intensità di R&S, si registra una concentrazione particolarmente elevata, con tre aziende che si aggiudicano da sole i ¾ del mercato: le prime due sono americane [Synopsys (quota di mercato del 31%) e Cadence (quota di mercato del 30%)], la terza è europea, ma con sede negli Stati Uniti [Siemens EDA, quota di mercato del 13%]. Su tale infrastruttura software si innesta la fase di *design/fabless*, assolutamente dominata da aziende statunitensi, in cui operano i principali progettisti globali – NVIDIA[18], AMD, Qualcomm, Broadcom e Intel. La fase di fabbricazione (*foundry*) resta invece sostanzialmente esclusiva delle imprese del sud est asiatico: a metà del 2025, la quota di mercato della multinazionale di Taiwan, TSMC, era intorno al 70%, con Samsung (Corea del Sud) e SMIC (Cina) decisamente distanziate. L'Unione Europea, dal canto suo, rappresenta soprattutto un importante mercato di sbocco, ed esattamente assorbe il 10,6% del totale del mercato mondiale, per un valore di circa 50 miliardi di euro (2023). In questo mercato, l'UE mostra una marcata dipendenza dalle importazioni, cui si accompagna una progressiva riduzione della capacità produttiva[19]. Tuttavia, dal lato dell'offerta, l'UE presidia alcune produzioni che rappresentano snodi tecnologici critici: in particolare, ci si riferisce alla società olandese ASML, leader mondiale nella fornitura di macchine per la litografia ultravioletta estrema.

Per quanto riguarda i supercalcolatori, ossia l'high performance computing, Stati Uniti e Cina continuano a detenere la leadership mondiale, secondo le più importanti e riconosciute classifiche internazionali (come TOP500 o HPCG); tuttavia, l'UE ha una posizione di rilievo ed anche il Giappone è è in buona posizione. Nella classifica per paese TOP500 di novembre 2025, gli Stati Uniti guidano per numerosità (171 sistemi; 34,2%) e per potenza aggregata ($R_{max} \approx 6{,}96\times10^{9}$ GFlops), seguiti dalla Cina, con una base più contenuta (40 sistemi; 8%) e un contributo prestazionale complessivo inferiore ($R_{max} \approx 2{,}05\times10^{8}$ GFlops). L'UE, considerata come somma dei Paesi membri, costituisce un blocco rilevante, anche se ovviamente frammentato: 126 sistemi (25,2%), trainati in particolare da Germania con 40 sistemi e il più alto valore nazionale di Rmax pari a $1{,}4\times10^{9}$ GFlops, seguita da Francia (23 sistemi) e Italia (18 sistemi). Se

[18] Per avere un'idea delle dimensioni che NVIDIA assume in questo mercato, si consideri che nel 2025 è risultata la prima azienda a superare i 100 miliardi di dollari di vendite di semiconduttori, rappresentando il 15,8% dei ricavi globali del comparto.
[19] In tal senso, la strategia industriale europea mira a ridurre le dipendenze e rafforzare le capacità lungo la catena del valore, con l'obiettivo di portare la quota UE al 20% del mercato mondiale, entro il 2030.

ISSN 2038-1662

poi si prende a riferimento la classifica dei dieci sistemi più potenti, quella più nota anche a livello dei media, gli Stati Uniti possono vantare i tre supercomputer più potenti: El Capitan (1,809 PFlop/s), Frontier (1,353 PFlop/s) e Aurora (1,012 PFlop/s), confermando una superiorità sostenuta da infrastrutture e programmi nazionali. L'UE, con quattro sistemi nei top dieci, ha un ruolo di livello. In ordine di potenza, troviamo JUPITER Booster in Germania (1,000 PFlop/s, 4° in classifica), primo sistema exascale europeo, HPC6 dell'ENI in Italia (477,9 PFlop/s, 6° in classifica), LUMI in Finlandia (379,7 PFlop/s, 9° in classifica) e Leonardo del CINECA in Italia (241,2 PFlop/s, 10° in classifica).
In conclusione, nell'industria del supercalcolo (HPC), l'UE è ben posizionata, grazie alle iniziative comunitarie (vari programmi, come illustrato nei successivi capitoli) e degli investimenti pubblici e privati. Dopo le note non proprio positive emerse dai mercati del cloud e dei microchip, registriamo quindi un punto di forza dell'ecosistema digitale europeo.

Per quanto riguarda le reti satellitari, il confronto tra USA, Cina e Unione Europea mostra una frattura ancora più netta tra scala industriale, autonomia strategica e specializzazione di missione delle tre aree.
Se si guarda alla "massa" in orbita, gli Stati Uniti risultano largamente egemoni. Secondo i dati del report dell'European Space Agency (ESA), a metà 2025, la flotta USA era nell'ordine di circa 9.800 satelliti, pari a due terzi dei satelliti operativi a livello globale[20](con una crescita trainata soprattutto dalle costellazioni commerciali in Low Earth Orbit, LEO). La leadership statunitense è sostenuta anche da investimenti federali: la richiesta di budget NASA per il 2025 è stata di circa 25,4 miliardi di dollari, a supporto di programmi scientifici, esplorazione e infrastrutture spaziali che alimentano filiere produttive e innovazione. La Cina segue una traiettoria diversa, in accelerazione. Nel 2025, sono poco meno di mille i satelliti cinesi in orbita, con un mix di applicazioni militari, osservazione della terra e comunicazioni, e con l'avvio/rafforzamento di mega-costellazioni LEO per internet satellitare[21]. L'Unione europea, dal canto suo, si attesta su ordini di grandezza inferiori, anche rispetto alla Cina: circa 500 satelliti, messi in orbita da imprese europee. Tuttavia, l'UE compensa sul versante della "qualità" e della sicurezza, grazie a importanti programmi: Galileo per la navigazione (satelliti Medium Earth Orbit, MEO), con Copernicus/Sentinel (satelliti LEO) per l'osservazione della terra. Inoltre, l'Unione europea può contare su

[20] ESA, Report on the Space Economy 2025, https://space-economy.esa.int/documents/tJMabTj61KkdGVOtF6SKw6wGSxicen6ajUWamCG3.pdf
Altre fonti (Statista/Orbiting Now) forniscono valori più elevati, ma confermano sempre la supremazia degli USA: 8.530 satelliti "in orbita", già a novembre 2024, di cui oltre 7.400 unità di Starlink.
[21] Si veda il programma nazionale "Guowang", che prevede fino a qualche decina di migliaia di satelliti da mandare in orbita.

ISSN 2038-1662

OneWeb/Eutelsat, una costellazione da 648 satelliti per broadband professionale (marittimo, aeronautico, governi, backhaul). Infine, vi sono importanti iniziative in corso, in particolare: i) il programma Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), una costellazione multi-orbita da 290 satelliti (LEO+MEO) progettata per portare connettività sicura e resiliente a istituzioni e infrastrutture critiche europee, affiancando (non sostituendo) l'offerta commerciale; ii) l'iniziativa GOVSATCOM per le comunicazioni satellitari governative, in sinergia con IRIS², per garantire comunicazioni sicure alle autorità dell'UE[22]. In conclusione, gli Stati Uniti restano il paese leader per numero di satelliti e capacità di generare fatturato, soprattutto con i satelliti LEO dei suoi operatori privati, mentre la Cina, sia pure in crescita rapida sotto la regia statale, resta per ora alquanto distanziata in termini di numerosità e di specializzazione. L'Unione europea risulta focalizzata su servizi critici (navigazione, osservazione della terra) e su nuove architetture (IRIS²) per accrescere la propria autonomia nel settore (vedi capitoli successivi).

Nel settore dei cavi sottomarini, il confronto tra Stati Uniti, Cina e Unione Europea evidenzia differenze tra modelli industriali, specializzazione tecnologica e posizionamento internazionale. Nel 2025, la mappa dei collegamenti "attivi o in costruzione" a livello globale censisce 597 sistemi di cavo e 1.712 punti di approdo (landings), a testimonianza di un ecosistema già molto presente a livello mondiale ed in continua espansione. In questo quadro, l'Europa si differenzia per il modello proprietario, in primo luogo rispetto agli Stati Uniti dove dominano i grandi hyperscaler (Google, Meta, Microsoft, AWS), mentre nel vecchio continente esistono molteplici operatori generalmente specializzati su singole rotte e su particolari mercati (cavi elettrici, cavi per le TLC ed Internet). In questo contesto, si segnalano due "presidi" europei: da un lato, il ruolo di snodo di approdi tra Atlantico, Mediterraneo e rotte verso Medio Oriente/Asia; dall'altro lato, una leadership nei cavi elettrici sottomarini, dove i collegamenti diventano asset della transizione energetica e dell'integrazione dei mercati[23]. Quindi, nello specifico segmento dei cavi elettrici, i paesi dell'UE sembrano ancora competitivi. Sul versante dei cavi per i settori TLC ed Internet, la partita è invece più sbilanciata: gli Stati Uniti emergono come baricentro del modello "private backbone", con gli hyperscaler (Google, Meta, Microsoft, AWS) sempre più coinvolti nel deployment di nuovi sistemi che si segnalano per capacità, resilienza e controllo delle rotte. L'Unione europea, in risposta, rafforza - comunque - corridoi alternativi e mediterranei: BlueMed (Italia–Francia–Grecia e hub nel

[22] European Commission, IRIS²: the new EU Secure Satellite Constellation Infrastructure for Resilience, Interconnectivity and Security by Satellite, https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

[23] Emblematici sono i grandi interconnettori nel Mare del Nord: North Sea Link (Norvegia–Regno Unito, 720 km) e NordLink (Norvegia–Germania, ~623 km), a cui si aggiunge Viking Link (Regno Unito–Danimarca, ~765 km, completato nel 2023), che consolida la traiettoria europea verso "supercavi" per lo scambio di energie rinnovabili su scala regionale.

ISSN 2038-1662

Mediterraneo) e il più ampio Blue & Raman puntano a portare connettività dati ad alta capacità dall'Europa fino all'India (via Israele e Medio Oriente), riducendo latenza e diversificando i passaggi rispetto ai colli di bottiglia tradizionali; in parallelo Medusa (finanziamento anche UE/CEF) costruisce un ponte digitale Euro–Nord Africa nel Mediterraneo con fasi di deployment che nel 2025 sono entrati nella dimensione operativa/di avanzamento dei landing. La Cina, infine, cresce soprattutto come investitore/fornitore e promotore di corridoi Asia–Africa–Europa: sistemi come PEACE (Pakistan–East Africa–Connecting Europe) rappresentano un esempio di espansione lungo l'asse indo-mediterraneo con tecnologia in fibra ottica e obiettivi di capacità/rotta "diretta" per traffico dati, mentre fonti ufficiali cinesi indicano che, a fine 2024, imprese cinesi risultavano coinvolte in 17 sistemi internazionali in servizio (oltre a progetti in corso), segnalando una strategia di presenza crescente, ma meno centrata sulla proprietà da parte di hyperscaler (cinesi) e più su partnership. In conclusione, l'industria statunitense (grazie agli hyperscaler) conferma la propria posizione di forza nei diversi segmenti del mercato dei cavi, mentre la Cina si va caratterizzando come attore industriale e geopolitico delle dorsali intercontinentali. L'UE resta competitiva come hub di rotte e landing e, soprattutto, come laboratorio di interconnessioni energetiche HVDC e di nuovi corridoi dati mediterranei. In ogni caso, l'UE sta ridefinendo (vedi capitoli successivi) la propria strategia per questo settore strategico, anche dal punto di vista della difesa, oltre che dell'autonomia produttiva.

I large language model, ossia i modelli di intelligenza artificiale generativa, rappresentano il passaggio dell'intelligenza artificiale alla dimensione del mass market. Questo processo è riconducibile al novembre 2022, quando Open AI ha reso disponibile a tutti e gratuitamente una versione del suo modello ChatGPT, raggiungendo cento milioni di utenti nell'arco di soli due mesi. Nel confronto internazionale, il dominio delle imprese statunitensi è evidente, in termini di modelli rilasciati: 174, nel biennio 2023-2024. Segue la Cina, con 53 modelli rilasciati nello stesso periodo e quindi l'UE assieme al Regno Unito, con 44 modelli rilasciati. Se si considerano i modelli rilasciati per impresa, torna – ancora una volta – la regola (empirica) dei 2/3: nel periodo 2019-2024, il 66% dei foundation model sul mercato (206) erano di proprietà di Google, Open AI, Microsoft e Meta. Il primo modello europeo – Mistral – si collocava al settimo posto (con otto modelli, quasi il 4% del totale), mentre si segnalavano la Germania, soprattutto con Aleph Alpha, e l'Italia, con Velvet di Almawave e Miia di Fastweb. In questo mercato, la Cina si è messa in evidenza soprattutto per il modello lanciato dalla start up DeepSeek, caratterizzato da costi di sviluppo assai contenuti rispetto a quelli sostenuti dalle imprese statunitensi. Anche le grandi imprese digitali cinesi sono tuttavia presenti con i propri modelli: questo è il caso di Alibaba, Baidu e ByteDance. Tuttavia, i dati sul mercato cinese (investimenti, utenti) non sembrano pienamente affidabili, per cui i confronti con questo paese devono essere prudenti nel pervenire a conclusioni affidabili. In

ISSN 2038-1662

conclusione, al momento la supremazia degli USA, ossia delle big tech americane, appare assai difficile da contrastare da parte di imprese europee: le dimensioni di investimento per lo sviluppo di modelli di intelligenza artificiale generativa sono al di fuori della loro portata, anche se esistono opportunità per produrre modelli di medie dimensioni, più vicine alle esigenze degli utilizzatori finali (imprese e pubbliche amministrazioni), che sono peraltro proprietari di dati fondamentali per addestramento e sviluppo dei modelli.

3. Il quadro normativo e di policy sul digitale

L'analisi del capitolo che precede ha già dato modo di comprendere come la trasformazione digitale abbia rappresentato uno dei processi più complessi e ambiziosi della storia dell'integrazione europea contemporanea, in parallelo con un progressivo indebolimento della sovranità degli Stati che ha gradualmente condizionato l'esercizio e l'universale condivisione dei valori alla base dell'Unione[24]. Si parla, a tal riguardo, di crisi della sovranità popolare[25] e, almeno dal 2013, di obiettivo di "autonomia strategica" dell'Unione[26].

Già nel quadro della strategia di Lisbona del 2000, il Consiglio europeo aveva fissato l'obiettivo di trasformare l'Unione europea in un'economia basata sulla conoscenza più competitiva e dinamica del mondo entro il 2010: "una società dell'informazione per tutti"[27]. A sostegno di tale ambizione, la Commissione europea ha avviato una serie di iniziative volte a promuovere la diffusione delle infrastrutture digitali e dei servizi online, tra cui i piani d'azione eEurope 2002[28], eEurope 2005[29] e la strategia i2010[30], con particolare attenzione allo sviluppo dell'e-government, dell'e-business e all'incremento degli investimenti in ricerca e innovazione nel settore delle tecnologie

[24] S. Cassese, *Democrazie e poteri (privati) globali*, in *Rivista dello Stato Digitale*, 1, 2025, p. 19 e E. Falletti*, Sovranità digitale, tutela della sicurezza nazionale e libertà di manifestazione del pensiero: i faticosi equilibri della sentenza TikTok v. Garland*, in *Diritto dell'informazione e dell'informatica*, 1, 2025, pp. 81 ss.

[25] J. P. Beetz, *Saving popular sovereignty from a slow death in the European union*, in *Journal of Common Market Studies*, 26(2), 2024, pp. 508 – 524.

[26] Si veda D. Martire, *Pluralità degli ordinamenti giuridici e Costituzione repubblicana. Spunti di riflessione alla luce dell'esperienza costituzionale*, in *Diritto pubblico*, 3, 2017, pp. 872 ss., secondo il quale, peraltro, "sovranità" è in contrapposizione con "autonomia".

[27] Consiglio europeo, *Conclusioni della Presidenza*, Lisbona, 23-24 marzo 2000.

[28] Comunicazione della Commissione al Consiglio ed al Parlamento europeo, eEurope 2002: Impatto e priorità – Comunicazione al Consiglio europeo di primavera Stoccolma 23-24 marzo 2001, COM(2001) 140 def., 13 marzo 2001

[29] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, eEurope 2005: una società dell'informazione per tutti – Piano d'azione da presentare per il Consiglio europeo di Siviglia 21 e 22 giugno 2002, COM(2002) 263 def.

[30] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 1° giugno 2005, intitolata "i2010 – Una società europea dell'informazione per la crescita e l'occupazione". COM(2005) 229 def.

ISSN 2038-1662

dell'informazione e della comunicazione. Le politiche digitali sono state successivamente integrate nelle iniziative faro della strategia Europa 2020[31], culminando nel 2010 con l'istituzione dell'Agenda digitale europea[32], sino alla strategia del mercato unico digitale del 2015[33]. Lo schema regolatorio europeo si è indubbiamente posto il fine di recuperare terreno rispetto al crescente potere economico delle potenze straniere, in termini di protezione degli operatori economici e consumatori europei[34].
Nel mentre, la già affrontata Comunicazione della Commissione "2030 Digital Compass: the European way for the Digital Decade", pubblicata all'inizio del 2021, ha sottolineato come la pandemia abbia esposto le vulnerabilità del nostro spazio digitale e le sue dipendenze dalle tecnologie non europee, stabilendo obiettivi concreti come la copertura 5G universale, l'80% degli adulti con competenze digitali di base e 20 milioni di specialisti ICT entro il 2030[35].

La produzione normativa in materia digitale, sebbene recente, è estremamente vasta e una mappatura completa richiederebbe di considerare anche la regolamentazione settoriale, data la capacità pervasiva del digitale di interessare qualsiasi ambito. Nel presente paragrafo non si può pertanto mirare a una ricostruzione esaustiva, ma si tenterà di fornire una panoramica – suddivisa in raggruppamenti omogenei – delle principali iniziative dell'Unione Europea, al fine di evidenziare l'approccio Unionale al tema della sovranità digitale e trarne alcune riflessioni, anche rispetto ad un potenziale e recente cambio di paradigma che – come si vedrà – ha interessato le ultime iniziative Unionali.

Il cuore pulsante della strategia si può rinvenire nel programma strategico per il decennio digitale 2030[36], che stabilisce obiettivi vincolanti e crea un framework di governance per coordinare l'azione degli Stati membri, una visione che è stata ulteriormente rafforzata e ridefinita dal già citato *Competitiveness Compass* e dalla

[31] Comunicazione della Commissione, Europa2020 – Una strategia per una crescita intelligente, sostenibile e inclusiva, COM(2010) 2020 def., 3 marzo 2020.
[32] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, Un'agenda digitale europea, COM(2010) 245 def., 19 maggio 2010.
[33] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa, COM(2015) 192 def., del 6 maggio 2015.
[34] M. Granieri, *Problema e sistema dei dati non personali nel diritto euro-unitario*, in Aa. Vv. *Annali italiani del diritto d'autore – AIDA*, Milano, Giuffrè, 2023, p. 199.
[35] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni su "Bussola digitale 2030: il modello europeo per il decennio digitale"*, COM(2021) 118 final, 9.03.2021.
[36] Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030, *GUUE* L 323, 19 dicembre 2022.

ISSN 2038-1662

strategia *Single Market*[37].
L'architettura normativa che ne risulta si articola in otto grandi cluster tematici che rappresentano altrettante dimensioni della sovranità digitale europea, ciascuna con la propria logica interna ma – in teoria – interconnessa con le altre in un sistema complesso di governance multilivello.

Il primo cluster riguarda i diritti digitali fondamentali e la protezione dei dati, dove il Regolamento generale sulla protezione dei dati[38] ha costituito la pietra angolare che ha stabilito uno standard globale per la protezione dei dati personali. Questo è stato affiancato alla Direttiva ePrivacy[39] che protegge specificamente le comunicazioni elettroniche e dalla Direttiva sulla protezione dei dati nel *law enforcement*[40] che regola il trattamento dei dati personali da parte delle autorità di polizia. Il sistema è completato dal Regolamento (UE) 2018/1725 che applica gli stessi principi alle istituzioni europee stesse. La governance di questo cluster è affidata all*'European Data Protection Board* (EDPB) che coordina le autorità nazionali di protezione dati, all'European Data Protection Supervisor (EDPS) che supervisiona le istituzioni europee, e alle singole autorità nazionali che mantengono ampi poteri di enforcement. Il framework sui diritti digitali fondamentali non è un elemento accessorio della strategia europea ma ne costituisce il DNA distintivo e ha permesso all'Europa di posizionarsi come modello di esportazione (il cd *Brussels effect*[41]).

Il secondo cluster comprende la governance dell'intelligenza artificiale, dove il Regolamento sull'intelligenza artificiale[42] ha rappresentato la prima regolamentazione

[37] COM(2025)500 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - The Single Market: our European home market in an uncertain world.
[38] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – GDPR), *GUUE* L 119, 4 maggio 2016.
[39] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche – Direttiva ePrivacy), *GUCE* L 201, 31 luglio 2002.
[40] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI, *GUUE* L 119, 4 maggio 2016.
[41] A. Bradford, *The Brussels Effect*, in 107 *Nw. U. L. Rev. 1*, 2012.
[42] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale – AI Act), *GUUE* L, 12 luglio 2024.

ISSN 2038-1662

comprensiva sull'AI a livello mondiale che introduce un sistema di classificazione del rischio (sebbene con problemi di effettività[43]) con obblighi proporzionati che vanno dalla proibizione per pratiche considerate inaccettabili, attraverso valutazioni di conformità rigorose per sistemi ad alto rischio utilizzati in ambiti critici, fino a semplici obblighi di trasparenza per sistemi a rischio minimo. Il regolamento include anche regole specifiche per i modelli a scopi generali (l'IA generativa è trattata in tale contesto) che devono rispettare obblighi di trasparenza sulle fonti dei dati di training, gestione del rischio sistemico per i modelli più potenti, e cooperazione con le autorità di regolamentazione, tentando anche qui un precedente globale su come governare questa tecnologia trasformativa. La governance è affidata all'Ufficio europeo per l'IA presso la Commissione Europea, ai fini di supervisione generale e specificamente per i modelli GPAI, all'*European Artificial Intelligence Board* che coordina l'implementazione tra gli Stati membri, e a una rete di autorità nazionali competenti che supervisionano i sistemi AI ad alto rischio nei rispettivi territori[44].

Nel contesto dell'IA, la strategia *Apply AI* lanciata dalla Commissione mira esplicitamente ad accelerare l'adozione dell'AI attraverso l'industria europea con particolare focus su dieci settori industriali chiave (manifattura, energia, trasporti, salute, finanza, agricoltura, pubbliche amministrazioni, educazione, media, retail)[45]. Questa è supportata da investimenti settoriali, dalla creazione di una rete di AI Factories che utilizzano l'infrastruttura di supercalcolo europea EuroHPC per sviluppare modelli AI avanzati, da programmi specifici per formare e attrarre talento europeo nell'AI attraverso iniziative di "*shaping and strengthening European AI talent*"[46], dal *Memorandum of Understanding sulle AI Gigafactories* che cerca di creare infrastrutture specifiche per lo sviluppo di modelli AI di frontiera[47], e dall'*AI Pact* che coinvolge le aziende su base volontaria nell'implementazione anticipata dei principi del Regolamento sull'intelligenza artificiale prima che entri pienamente in vigore[48]. Il regolamento *EuroHPC* è stato, inoltre, recentemente modificato per rafforzare le capacità europee in AI e quantum computing, riconoscendo che l'infrastruttura computazionale rappresenta un prerequisito fondamentale per qualsiasi ambizione di

[43] *Ex multis*, T. Karathanasis, *The AI Act: balancing implementation challenges and the EU's simplification agenda*, in *ssrn.com*, 2025. Per un caso pratico, si veda anche L. Megale e N. Rangone, *Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making*, in *European Journal of Risk Regualtion*, 16, 2025, pp. 1082 – 1097.

[44] Art. 64, Regolamento (UE) 2024/1689.

[45] Commissione europea, *Comunicazione della Commissione al Parlamento europeo e al Consiglio – Apply AI Strategy*, COM(2025) 723 final, Bruxelles, 8 ottobre 2025.

[46] Si veda https://digital-strategy.ec.europa.eu/en/library/shaping-and-strengthening-european-ai-talent.

[47] Commissione europea, *Commission Decision C(2025) 6977 – MoU AI Gigafactories*, 4 dicembre 2025. Disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/it/library/memorandum-understanding-ai-gigafactories

[48] Si veda https://digital-strategy.ec.europa.eu/it/policies/ai-pact.

ISSN 2038-1662

sovranità nell'AI[49].

Il terzo cluster investe il tema della regolamentazione delle piattaforme digitali e dei contenuti online, ove il Regolamento sui servizi digitali[50] stabilisce le fondamenta per la regolamentazione delle piattaforme online con obblighi di due diligence proporzionali alle dimensioni e all'impatto delle piattaforme, sistemi di *notice-and-action* per contenuti illegali, trasparenza algoritmica, gestione del rischio sistemico per le piattaforme che devono condurre valutazioni annuali sulle attività che le hanno interessate.
Il DSA è completato dal Regolamento sui mercati digitali[51] che affronta specificamente il potere di mercato concentrato nelle mani di poche piattaforme digitali globali designate come "gatekeeper" sulla base di criteri quantitativi (fatturato, capitalizzazione, numero di utenti) e qualitativi (posizione di intermediario tra consumatori e fornitori di servizi), imponendo obblighi ex-ante come l'interoperabilità dei servizi di messaggistica, il divieto di auto-preferenza nei risultati di ricerca o negli app store, l'obbligo di permettere agli utenti di disinstallare app preinstallate, la portabilità dei dati, e il divieto di combinare dati personali provenienti da servizi diversi senza consenso esplicito, con l'obiettivo di consentire l'ingresso competitivo nel mercato e salvaguardare equità e innovazione.
Riconosciuta la complessità del contesto normativa, la Commissione ha analizzato l'interazione del DSA con altre normative europee attraverso il *Report on the application of Article 33 of the DSA and its interaction with other legal instruments*[52], che riconosce esplicitamente le tensioni e sovrapposizioni con la Direttiva sul diritto d'autore nel mercato unico digitale[53]. Questa modernizza le regole sul diritto d'autore introducendo responsabilità delle piattaforme per contenuti caricati dagli utenti e nuovi diritti per autori e editori (sebbene rimangano questioni irrisolte sull'utilizzo di contenuti protetti per il training di modelli AI). Vi sono poi il Regolamento sulla trasparenza e il targeting della pubblicità politica che introduce trasparenza per gli

[49] Regolamento (UE) 2026/150 del Consiglio, del 16 gennaio 2026, che modifica il regolamento (UE) 2021/1173 che istituisce l'impresa comune europea per il calcolo ad alte prestazioni (EuroHPC), *GUUE* L, 19 gennaio 2026.
[50] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali – Digital Services Act, DSA), *GUUE* L 277, 27 ottobre 2022.
[51] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali – Digital Markets Act, DMA), *GUUE* L 265, 12 ottobre 2022.
[52] Commissione europea, *Relazione sull'applicazione dell'articolo 33 del regolamento (UE) 2022/2065 (DSA) e sull'interazione di tale regolamento con altri atti giuridici*, COM(2025) 708 final, Bruxelles, 17 novembre 2025.
[53] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (Direttiva sul diritto d'autore nel mercato unico digitale), *GUUE* L 130, 17 maggio 2019.

ISSN 2038-1662

annunci politici online con obblighi di etichettatura chiara, repository pubblici di annunci politici, e limitazioni al targeting comportamentale salvaguardando i processi democratici nell'era digitale[54]; il Regolamento sulla libertà dei media europei[55] che protegge il pluralismo mediatico e l'indipendenza editoriale rispondendo alle crescenti preoccupazioni su influenza statale e disinformazione attraverso regole sulla trasparenza della proprietà dei media, indipendenza dei regolatori nazionali, e protezione delle fonti giornalistiche, e la Direttiva sui servizi di media audiovisivi[56] che regola i servizi audiovisivi tradizionali e on-demand con quote di contenuti europei e regole sulla pubblicità. Il Regolamento sui contenuti terroristici online[57] impone poi la rimozione rapida di contenuti terroristici entro un'ora dalla notifica delle autorità, mentre le proposte su *combating violence against women*[58] e contrasto agli abusi sessuali sui minori[59] affrontano minacce specifiche che si manifestano attraverso le piattaforme digitali. La governance di tale cluster è affidata al coordinamento tra la Commissione Europea che supervisiona direttamente le piattaforme designate sotto il DSA e i gatekeeper sotto il DMA, l'*European Board for Digital Services* che coordina le autorità nazionali competenti (*Digital Services Coordinators*), il *High-Level Group on DMA*, e l'*European Board for Media Services per l'EMFA*, con il supporto di meccanismi di enforcement. La proposta di *Digital Fairness Act* promette di aggiungere ulteriori tutele per i consumatori digitali affrontando pratiche commerciali problematiche specifiche dell'ambiente online, mentre la questione della soglia di designazione del DSA (attualmente 45 milioni di utenti attivi mensili nell'UE) è oggetto di valutazione per determinare se sia appropriata o debba essere rivista.

[54] Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio, del 13 marzo 2024, relativo alla trasparenza e al targeting della pubblicità politica, *GUUE* L, 20 marzo 2024.
[55] Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (Regolamento europeo per la libertà dei media – European Media Freedom Act, EMFA), *GUUE* L, 17 aprile 2024.
[56] Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (Direttiva sui servizi di media audiovisivi – Direttiva AVMS), *GUUE* L 95, 15 aprile 2010.
[57] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online (Regolamento TCO), *GUUE* L 172, 17 maggio 2021.
[58] Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio, del 14 maggio 2024, relativa alla lotta contro gli abusi sessuali sui minori e lo sfruttamento sessuale dei minori e il materiale pedopornografico, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio, *GUUE* L, 24 maggio 2024.
[59] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori (CSAM), COM/2022/209 final, procedura 2022/0155(COD) – attualmente in fase di negoziazione legislativa.

ISSN 2038-1662

Il quarto cluster riguarda l'economia dei dati e gli spazi dati settoriali, dove il Regolamento sui dati[60] sblocca i dati industriali e dell'Internet of Things (IoT) per un uso più ampio attraverso diritti di accesso ai dati generati da prodotti connessi e servizi correlati, regole sulla condivisione dei dati tra imprese (B2B data sharing), meccanismi per rendere disponibili dati del settore privato alla pubblica amministrazione in situazioni di emergenza o per svolgere compiti di interesse pubblico, e disposizioni per mitigare gli effetti di lock-in dei fornitori cloud facilitando il switching tra provider e la portabilità dei dati, ponendosi al centro della strategia europea per l'economia dei dati e la competitività digitale. Il Regolamento sulla governance dei dati[61] introduce invece nuovi framework di condivisione dati e intermediari affidabili (*data intermediaries*) che facilitano la condivisione volontaria di dati tra imprese o tra individui e imprese, regole sul riutilizzo di determinate categorie di dati del settore pubblico che sono soggetti a diritti di terzi, e un framework per l'altruismo dei dati dove individui o imprese rendono disponibili i propri dati per finalità di interesse generale senza compenso, complementando il Regolamento sui dati e supportando gli spazi dati europei settoriali. Lo Spazio europeo dei dati sanitari (EHDS) costituisce il primo "*data space*" settoriale pienamente regolamentato a livello europeo, imponendo a un'ampia gamma di fornitori sanitari di catturare dati chiave in formato elettronico strutturato secondo standard comuni[62]. La Direttiva sui dati aperti[63] completa questo quadro regolando il riutilizzo delle informazioni del settore pubblico, mentre la strategia European Data Union mira esplicitamente a sbloccare i dati per l'AI creando un'economia basata sui dati che rispetti la privacy attraverso la creazione di molteplici spazi dati settoriali oltre alla sanità (energia, mobilità, agricoltura, manifattura, finanza, competenze) basati su governance, architetture tecniche e modelli di business comuni definiti dal Regolamento sui dati e Regolamento sulla governance dei dati. La governance è coordinata dall'European Data Innovation Board (EDIB) che riunisce rappresentanti degli Stati membri per garantire applicazione coerente del Regolamento sui dati e Regolamento sulla governance dei dati, dall'European Health Data Space Board (EHDS Board) specificamente per il settore sanitario, e dall'Interoperable Europe Board che garantisce l'interoperabilità tecnica e semantica dei sistemi pubblici

[60] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (Regolamento sui dati – Data Act), *GUUE* L, 22 dicembre 2023.

[61] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati – Data Governance Act), *GUUE* L 152, 3 giugno 2022.

[62] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (Direttiva Open Data), *GUUE* L 172, 26 giugno 2019.

[63] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (Direttiva Open Data), *GUUE* L 172, 26 giugno 2019.

ISSN 2038-1662

attraverso il Regolamento sull'interoperabilità europea (Regolamento (UE) 2024/903), mentre la raccolta dati per affitti a breve termine (Regolamento (UE) 2024/1028) e l'EU Digital Travel application (2024/0670(COD)) dimostrano come la logica degli spazi dati si applichi progressivamente a nuovi settori. Questa architettura normativa riflette la convinzione europea che i dati rappresentino una risorsa strategica che deve essere governata secondo principi di equità, accessibilità e protezione della privacy, cercando di creare un terzo modello tra il capitalismo dei dati americano dove le piattaforme accumulano e monetizzano dati con limitati vincoli e il modello cinese di controllo statale centralizzato dei dati, un modello europeo basato su condivisione volontaria facilitata da intermediari fiduciari, accesso regolamentato per finalità specifiche di interesse pubblico, e empowerment individuale attraverso diritti di accesso e portabilità.

Il quinto cluster riguarda la cybersicurezza e la resilienza digitale, dove il Regolamento sulla cibersicurezza[64] conferisce all'European Union Agency for Cybersecurity (ENISA) un ruolo permanente con mandato rafforzato e crea il framework europeo di certificazione cybersecurity che permette di sviluppare schemi di certificazione armonizzati per prodotti ICT, servizi e processi garantendo che soddisfino requisiti di sicurezza verificati da organismi indipendenti, costituendo la fondazione per fiducia e sicurezza. La Direttiva NIS 2 espande drasticamente le regole baseline di cybersicurezza coprendo molti più settori rispetto alla direttiva precedente (18 settori ad alta criticità tra cui energia, trasporti, banche, infrastrutture digitali, spazio, e 11 settori critici aggiuntivi tra cui servizi postali, gestione rifiuti, produzione chimica, alimentare), imponendo obblighi di gestione del rischio cyber, reporting di incidenti significativi entro tempistiche strette, e misure organizzative appropriate, con meccanismi di supervisione rafforzata da parte delle autorità nazionali competenti coordinate attraverso il *NIS cooperation group* a livello europeo[65].
Il Regolamento sulla resilienza cibernetica[66] rappresenta una normativa rivoluzionaria per i prodotti connessi (hardware e software) richiedendo security-by-design durante

[64] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (Regolamento sulla cibersicurezza – Cybersecurity Act), *GUUE* L 151, 7 giugno 2019.
[65] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972, e che abroga la direttiva (UE) 2016/1148 (Direttiva NIS 2), *GUUE* L 333, 27 dicembre 2022.
[66] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (Regolamento sulla ciberresilienza – Cyber Resilience Act, CRA), *GUUE* L, 20 novembre 2024.

ISSN 2038-1662

tutto il ciclo di vita del prodotto, gestione attiva delle vulnerabilità con obbligo di fornire aggiornamenti di sicurezza per un periodo definito, reporting di vulnerabilità e incidenti alle autorità, e marcatura CE che attesta conformità ai requisiti essenziali di cybersicurezza, colmando lacune critiche nella cybersicurezza delle supply chain hardware e software che hanno permesso la proliferazione di dispositivi IoT insicuri. Il Regolamento sulla solidarietà cibernetica[67] rafforza invece la resilienza e le capacità di cybersicurezza europee attraverso meccanismi di coordinamento come l'*European Cyber Shield* che aggrega capacità distribuite per identificare minacce emergenti, il sistema di allerta europea per la cybersicurezza (*European Cybersecurity Alert System*) che dissemina rapidamente informazioni su minacce e vulnerabilità, e la riserva europea per la cybersicurezza (*EU Cybersecurity Reserve*) che pre-posiziona capacità di risposta agli incidenti che possono essere mobilitate rapidamente in caso di crisi cyber su richiesta degli Stati membri. Il Regolamento sulla resilienza operativa digitale (DORA) applica questi principi specificamente al settore finanziario imponendo una robusta gestione del rischio ICT per banche, assicurazioni, investimenti e i loro fornitori tecnologici terzi (inclusi provider di cloud, analytics, data centers) con requisiti dettagliati su test di resilienza, gestione del rischio di terze parti, condivisione di informazioni su minacce, e governance ICT[68]. La Commissione ha, inoltre, proposto un nuovo pacchetto sulla cybersicurezza per rafforzare ulteriormente la resilienza e le capacità dell'UE in materia di sicurezza informatica. La proposta di revisione del Cybersecurity Act fa parte di questo pacchetto[69]. L'obiettivo è aumentare le capacità e la resilienza in materia di cybersicurezza e prevenire la frammentazione nel mercato unico digitale dell'UE. Inoltre, mira a rafforzare la sicurezza delle catene di approvvigionamento delle tecnologie dell'informazione e della comunicazione (ICT) dell'UE. La governance di questo cluster coinvolge ENISA come hub tecnico centrale con responsabilità per certificazione, capacity building, esercitazioni, e supporto tecnico agli Stati membri, l'*European Cybersecurity Competence Centre* (ECCC) che coordina la ricerca e l'innovazione in cybersicurezza finanziando progetti e costruendo una rete di centri di competenza nazionali, CERT-EU che fornisce servizi di risposta agli incidenti per le istituzioni europee, l'*Interinstitutional Cybersecurity Board* (IICB) che coordina la sicurezza informatica tra le istituzioni, il *Cyber Crises Liaison*

[67] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (Regolamento sulla cibersolidarietà – Cyber Solidarity Act), *GUUE* L, 15 gennaio 2025.

[68] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (Regolamento sulla resilienza operativa digitale – Digital Operational Resilience Act, DORA), *GUUE* L 333, 27 dicembre 2022.

[69] Si vedano https://www.europarl.europa.eu/news/it/agenda/plenary-news/2026-01-19/8/le-nuove-proposte-sulla-cibersicurezza-dell-ue.

ISSN 2038-1662

Organisation Network (EU CyCLONe) che facilita la gestione coordinata di crisi cyber su larga scala, la rete CSIRTs che connette i computer security incident response team nazionali, il *NIS cooperation* group che coordina l'implementazione della Direttiva NIS 2, la *European Cyber Shield* che aggrega capacità di *detection*, e la EU Cybersecurity Reserve che pre-posiziona capacità di risposta. Si è così di fronta ad un ecosistema di governance multilivello che riflette la natura transnazionale delle minacce cyber, ma che solleva anche questioni di coordinamento e tempestività della risposta in situazioni di crisi dove ogni minuto conta.

Il sesto cluster interessa le tecnologie strategiche e l'autonomia industriale, dove il Regolamento europeo sui semiconduttori[70] cerca di costruire la capacità europea nei semiconduttori attraverso un approccio integrato. Peraltro, quest'ultima normativa menziona esplicitamente il rafforzamento della sovranità digitale come uno dei suoi obiettivi cardine, intesa come indipendenza tecnologica[71]. Il Regolamento si collega alla ricerca avanzata attraverso il *Chips Joint Undertaking*[72] che mobilita risorse pubbliche e private per R&D, supporto alla costruzione di nuove fabbriche attraverso meccanismi di finanziamento facilitati per progetti di prima e seconda generazione che soddisfano criteri di rilevanza europea (, creazione di una rete europea di centri di competenza in semiconduttori che condividono conoscenze e infrastrutture di test, e gestione delle crisi attraverso un meccanismo di monitoraggio delle supply chain e coordinamento. Il tutto governato dall'*European Semiconductor Board* che riunisce Stati membri e industria, attualmente oggetto di una consultazione pubblica per valutarne l'efficacia e le eventuali revisioni necessarie dopo i primi anni di implementazione[73]. Il prossimo Quantum Act dovrebbe invece focalizzarsi di applicare una logica simile al quantum computing creando un framework per investimenti coordinati, condivisione di infrastrutture di ricerca costose, sviluppo di competenze, e eventualmente meccanismi di procurement pubblico coordinato per creare massa critica di domanda, riconoscendo che il quantum computing rappresenta una tecnologia potenzialmente disruptive dove l'Europa rischia di rimanere indietro rispetto a USA e Cina senza intervento coordinato. Il Regolamento sull'industria a zero emissioni nette[74]

[70] Regolamento (UE) 2023/1781 del Parlamento europeo e del Consiglio, del 13 settembre 2023, che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il regolamento (UE) 2021/694 (Regolamento sui chip – European Chips Act), *GUUE* L 229, 18 settembre 2023.

[71] Commissione europea, *Chips Act – Relazione illustrativa*, COM(2022) 46 final, p. 4.

[72] Si veda https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/chips-joint-undertaking_en.

[73] Si veda https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3932.

[74] Regolamento (UE) 2024/1735 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che istituisce un quadro di misure per rafforzare l'ecosistema europeo di fabbricazione di prodotti a

ISSN 2038-1662

e il Regolamento sulle materie prime critiche[75] rafforzano l'indipendenza europea nelle tecnologie verdi e nelle materie prime critiche attraverso obiettivi quantitativi (produrre in Europa almeno il 40% del fabbisogno di tecnologie net-zero, estrarre almeno il 10% e processare almeno il 40% del fabbisogno di materie prime critiche entro il 2030), fast-tracking dei permessi per progetti strategici, coordinamento attraverso la *Net-zero Europe Platform* e l'*European Critical Raw Materials Board*, e meccanismi di monitoraggio delle supply chain per identificare vulnerabilità, riconoscendo che la transizione verde richiede sicurezza di approvvigionamento in tecnologie e materiali dove l'Europa è attualmente fortemente dipendente da fornitori extraeuropei concentrati.

Il prossimo EU Space Act si pone invece l'obiettivo a rafforzare l'autonomia europea nelle tecnologie e servizi spaziali[76], settore dove l'UE ha già capacità significative attraverso programmi come Galileo (navigazione satellitare), Copernicus (osservazione della Terra), e EGNOS (navigazione regionale) gestiti dall'European Union Agency for the Space Programme (EUSPA) e supportati dal Programma per una connettività sicura dell'Unione[77] che include partnership con l'European Space Agency (ESA) per garantire connettività sicura e sovrana attraverso infrastrutture spaziali europee.

L'EU Cloud and AI Development Act[78] e l'Advanced Materials Act[79] promettono invece di completare questo quadro di autonomia strategica nelle tecnologie critiche, mentre la Piattaforma per le tecnologie strategiche per l'Europa (STEP)[80] crea un ombrello finanziario che mobilita risorse attraverso vari strumenti esistenti (InvestEU, Horizon Europe, coesione) per tecnologie strategiche identificate. La governance

---

tecnologia zero emissioni nette e che modifica la direttiva (UE) 2018/2001 (Regolamento per l'industria a zero emissioni nette – Net-Zero Industry Act, NZIA), *GUUE* L, 28 giugno 2024.

[75] Regolamento (UE) 2024/1252 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro atto a garantire un approvvigionamento sicuro e sostenibile di materie prime critiche e che modifica i regolamenti (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1724 e (UE) 2019/1020 (Regolamento sulle materie prime critiche – Critical Raw Materials Act, CRMA), *GUUE* L, 3 maggio 2024. Si veda anche Si veda, in questo volume, P. Guerrieri, G. P. Manzella e F. Onida, *La politica industriale UE nelle sfide dell'autonomia strategica. Proposte e suggerimenti di policy*, 2026, p. 21.

[76] Si veda https://defence-industry-space.ec.europa.eu/eu-space-act_en.

[77] Regolamento (UE) 2023/588 del Parlamento europeo e del Consiglio, del 15 marzo 2023, che istituisce il programma dell'Unione per una connettività sicura per il periodo 2023-2027 (programma IRIS²), *GUUE* L 79, 17 marzo 2023.

[78] Si veda https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-cloud-and-ai-development-act.

[79] Si veda https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/chemicals-and-advanced-materials/towards-advanced-materials-act_en.

[80] Regolamento (UE) 2024/795 del Parlamento europeo e del Consiglio, del 29 febbraio 2024, che istituisce la piattaforma per le tecnologie strategiche per l'Europa (STEP) e che modifica la direttiva 2003/87/CE e i regolamenti (UE) 2021/1058, (UE) 2021/1056, (UE) 2021/1057, (UE) n. 1303/2013, (UE) n. 223/2014, (UE) 2021/1060, (UE) 2021/523, (UE) 2021/695, (UE) 2021/697 e (UE) 2021/241, *GUUE* L, 29 febbraio 2024.

ISSN 2038-1662

coinvolge molteplici *Joint Undertakings* (EuroHPC per high-performance computing con capacità AI e quantum, Chips JU per semiconduttori, Smart Networks and Services JU per telecomunicazioni 5G/6G), board settoriali (European Semiconductor Board, European Critical Raw Materials Board, Net-zero Europe Platform), e agenzie specializzate (EUSPA per spazio, European Defence Agency per tecnologie dual-use), coordinati attraverso meccanismi come l'European Chips Infrastructure Consortium (ECIC)[81] e l'European Digital Infrastructure Consortium (EDIC)[82] che creano infrastrutture condivise riducendo duplicazioni e creando economie di scala.
Sempre nell'ambito del sesto cluster, un ruolo crescente – si presume – spetterà all'*Industrial Accelerator Act*[83] (IAA), proposta legislativa della Commissione europea in attesa di presentazione nell'ambito del *Clean Industrial Deal*. Rinominato dalla denominazione originaria di "Industrial Decarbonisation Accelerator Act" su impulso della Presidente von der Leyen, l'IAA si propone di accelerare la transizione e l'innovazione delle industrie europee ad alta intensità energetica – con priorità per acciaio e cemento – attraverso tre assi principali: la semplificazione e accelerazione dei procedimenti autorizzativi per la modernizzazione industriale; la creazione di mercati di sbocco (*lead markets*) per prodotti industriali a bassa emissione di carbonio, inclusa l'introduzione di un'etichetta *low-carbon* per i prodotti industriali europei; e il rafforzamento delle catene di approvvigionamento pulite attraverso criteri "clean, resilient, circular, cybersecure" negli appalti pubblici. Sebbene il focus principale dell'IAA sia la decarbonizzazione industriale, esso introduce criteri di resilienza e sicurezza informatica che si intrecciano con le priorità digitali dell'UE, riconoscendo il nesso tra competitività industriale, autonomia strategica e transizione tecnologica. La proposta è stata preceduta da un intenso dibattito sui requisiti di contenuto locale ("Made in EU") in settori come trasporti e costruzioni, riflettendo la tensione tra protezione delle catene del valore europee e rispetto degli accordi di libero scambio[84].
Inoltre, anche il settore del *defence tech* ha assunto un'importanza crescente nell'agenda europea di autonomia strategica, con ricadute dirette sull'ecosistema digitale. Il *Fondo europeo per la difesa*[85] (EDF), con un bilancio complessivo di circa 7,3 miliardi di euro per il periodo 2021–2027, sta investendo oltre 4 miliardi di euro in ricerca e sviluppo per tecnologie di difesa critiche, identificando come priorità strategiche l'intelligenza artificiale applicata alle operazioni militari (superiorità

[81] Art. 7, *European Chips Act*.
[82] Si veda https://digital-strategy.ec.europa.eu/en/policies/edic.
[83] Commissione europea, *Industrial Accelerator Act*, proposta legislativa presentata il 25 febbraio 2026 nell'ambito del Clean Industrial Deal. Cfr. anche Parlamento europeo, Legislative Train Schedule, scheda aggiornata sull'IAA.
[84] Si veda ECCO Climate, *What is the European Industrial Accelerator Act, what does it involve and why is it needed?*, febbraio 2026; CAN Europe, *The Industrial Accelerator Act: Unlocking EU Industrial Transformation with Targeted Demand Measures*, febbraio 2026.
[85] Commissione europea, DG Defence Industry and Space, *From AI to Quantum: How the European Defence Fund shapes the future of EU Defence Technologies*, 15 dicembre 2025.

ISSN 2038-1662

informativa, consapevolezza situazionale, interoperabilità), le tecnologie quantistiche (comunicazioni ultra-sicure, sensing avanzato, crittografia post-quantistica), la cyber difesa con soluzioni di cloud militare sicuro e protezione delle infrastrutture critiche, e i sistemi autonomi inclusi droni e sistemi anti-drone. Con il Programma di lavoro 2025 da 1,065 miliardi di euro, i nuovi progetti avviati vedono la partecipazione di oltre 600 soggetti giuridici tra PMI, università, centri di ricerca e grandi industrie di difesa. Questi sviluppi sono coerenti con il *White Paper for European Defence* e con la *Defence Readiness Roadmap 2030*, che identificano la superiorità tecnologica come pilastro della deterrenza europea. Sul versante della protezione dei dati di difesa, l'UE sta sviluppando una piattaforma federata per la condivisione sicura e sovrana di dati di interesse per la difesa (DAIDS – Defence AI and Data Space), concepita per operare senza dipendenza da tecnologie statunitensi, insieme a un cloud militare sovrano che il Commissario per la Difesa Andrius Kubilius ha esplicitamente invitato gli Stati membri a costruire[86]. Sul versante degli investimenti privati, il 2025 ha segnato un anno record per il venture capital nel settore europeo del defence tech: le startup europee attive nella difesa, sicurezza e resilienza hanno raccolto 8,7 miliardi di dollari, con una crescita del 55% rispetto all'anno precedente, trainata da round di investimento di taglia crescente in società attive nell'IA militare (Helsing, con 600 milioni di euro), nei sistemi autonomi (droni e counter-drone), nelle tecnologie spaziali e nella crittografia post-quantistica[87]. La *Defence tech* è diventata la categoria a più rapida crescita nel venture capital europeo (6,2% del totale degli investimenti nell'UE), con tecnologie a duplice uso (*dual-use*) che fondono applicazioni civili e militari – quantum computing, semiconduttori, cybersecurity, spazio – e che rappresentano al contempo asset strategici per la resilienza economica e per la prontezza militare. L'EDF supporta questo ecosistema anche tramite lo *EU Defence Innovation Scheme* (EUDIS), che abbassa le barriere di accesso per startup e PMI innovative, e si coordina con il *NATO Innovation Fund* (1 miliardo di euro) e con DIANA (Defence Innovation Accelerator for the North Atlantic).

Il settimo cluster riguarda la connettività, le infrastrutture digitali e i servizi fiduciari, dove il Codice europeo delle comunicazioni elettroniche (EECC)[88] fornisce un primo framework armonizzato per la regolamentazione dei servizi di rete fissa e mobile con principi di neutralità tecnologica, gestione efficiente dello spettro radio attraverso la

[86] Euractiv, *Exclusive: EU wants defence data secured without US tech*, 2026; cfr. anche Commissione europea, *Cloud Sovereignty Framework*, versione 1.2.1, ottobre 2025.
[87] Dealroom e NATO Innovation Fund, *European Defence, Security & Resilience Startups Smash Record with $8.7B Raised in 2025*, febbraio 2026; Resilience Media/Dealroom, *State of Defence Tech 2025*, settembre 2025.
[88] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche e che modifica la direttiva (UE) 2016/1148, *GUUE* L 321, 17 dicembre 2018.

ISSN 2038-1662

Decisione sullo spettro radio[89] e la Direttiva sulle bande di frequenza[90] che armonizzano bande per servizi paneuropei, separazione funzionale degli operatori con significativo potere di mercato per garantire accesso *wholesale* non discriminatorio, protezione dei consumatori attraverso contratti trasparenti e neutralità della rete attraverso il Regolamento sull'accesso a Internet aperto[91]. Si aggiungono le note regole sul roaming attraverso il Regolamento sul roaming[92] che ha progressivamente eliminato le tariffe di roaming all'interno dell'UE, creando un vero mercato unico delle telecomunicazioni dove i cittadini possono utilizzare i propri piani nazionali in tutta l'UE senza costi aggiuntivi. Il Regolamento sulle infrastrutture gigabit mira ad accellearare lo sviluppo di reti ad altissima capacità riducendo i costi di installazione attraverso diritto di accesso a infrastrutture fisiche esistenti di operatori di rete in settori diversi (energia, trasporti, acqua, fognature), semplificazione e armonizzazione delle procedure di permesso, e coordinamento dei lavori civili per minimizzare disruption, con l'obiettivo di raggiungere gli obiettivi del Digital Decade di connettività gigabit per tutti e copertura 5G lungo i corridoi di trasporto principali entro il 2030[93]. L'ormai prossimo Digital Networks Act (DNA) mira a sostituire il citato Codice europeo delle comunicazioni elettroniche con regole più semplici e armonizzate che riducono frammentazione normativa tra Stati membri, facilitano investimenti in reti attraverso certezza regolatoria e riduzione di compliance costs, e adattano il framework alla convergenza tra telecomunicazioni, media e servizi digitali che rende obsolete distinzioni tradizionali tra questi settori[94]. La Direttiva sulla compatibilità

[89] Decisione 676/2002/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa ad un quadro normativo per la politica in materia di spettro radio nella Comunità europea (Decisione sullo spettro radio), *GUCE* L 108, 24 aprile 2002.

[90] Direttiva 87/372/CEE del Consiglio, del 25 giugno 1987, relativa alle bande di frequenza da assegnare per l'introduzione coordinata del servizio pubblico paneuropeo di comunicazioni mobili cellulari digitali terrestri nella Comunità (Direttiva GSM), *GUCE* L 196, 17 luglio 1987.

[91] Regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio, del 25 novembre 2015, che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione (Regolamento sulla neutralità della rete), *GUUE* L 310, 26 novembre 2015.

[92] Regolamento (UE) 2022/612 del Parlamento europeo e del Consiglio, del 6 aprile 2022, relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione (Regolamento sul roaming), *GUUE* L 115, 13 aprile 2022.

[93] Regolamento (UE) 2024/1309 del Parlamento europeo e del Consiglio, del 29 aprile 2024, che stabilisce misure volte a ridurre i costi di realizzazione di reti di comunicazione elettronica Gigabit e che abroga la direttiva 2014/61/UE (Regolamento sulle infrastrutture Gigabit – Gigabit Infrastructure Act, GIA), *GUUE* L, 8 maggio 2024.

[94] M. Manganelli, *Il Digital Netoworks Act, fra nuove tecnologie, nuove dinamiche di mercato e vecchi principi regolatori*, in *Rivista della Regolazione dei mercati*, 2, 2025.

ISSN 2038-1662

elettromagnetica[95] e la Direttiva sulle apparecchiature radio[96] garantiscono che apparecchiature elettroniche non causino interferenze e utilizzino lo spettro radio efficacemente, mentre il Regolamento (UE) 2019/517 governa il dominio europeo coordinato dal *Multistakeholder Advisory Group*. Il Regolamento eIDAS[97] recentemente aggiornato dall'eIDAS 2.0[98] abilita identità digitale sicura e servizi fiduciari (firme elettroniche, sigilli elettronici, time stamping, electronic registered delivery), attraverso l'UE correggendo i gravi problemi di interoperabilità transfrontaliera del sistema precedente attraverso l'introduzione del European Digital Identity Wallet che tutti gli Stati membri dovranno fornire ai propri cittadini e residenti, permettendo identificazione e autenticazione per servizi pubblici e privati online con mutuo riconoscimento transfrontaliero garantito, conservazione sicura di attributi verificati (patente, diplomi, prescrizioni mediche) che possono essere selettivamente condivisi, e firma di documenti con pieno valore legale. La governance è coordinata dalla *Body of European Regulators for Electronic Communications* (BEREC) che raggruppa i regolatori nazionali delle telecomunicazioni, dal Communications Committee (COCOM) che assiste la Commissione nell'implementazione, e dal Gateway coordination group per il Regolamento eIDAS che garantisce l'interoperabilità tecnica dei sistemi di identità digitale nazionali, mentre il Regolamento sull'interoperabilità europea garantisce più in generale l'interoperabilità dei sistemi informativi pubblici attraverso standard comuni, architetture di riferimento, e meccanismi di condivisione di soluzioni riusabili coordinati dall'Interoperable Europe Board.

L'ottavo e ultimo cluster riguarda il mercato unico digitale, la concorrenza e la protezione dei consumatori, dove il Regolamento sui mercati digitali impone obblighi ex-ante sui "gatekeeper" per prevenire abusi di posizione dominante prima che si verifichino, a rafforzare l'esistente normativa antitrust. Sul fronte della protezione dei consumatori, la Direttiva sui diritti dei consumatori[99] garantisce diritti di recesso per

[95] Direttiva 2014/30/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla compatibilità elettromagnetica (Direttiva CEM), *GUUE* L 96, 29 marzo 2014.

[96] Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (Direttiva RED), *GUUE* L 153, 22 maggio 2014.

[97] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (Regolamento eIDAS), *GUUE* L 257, 28 agosto 2014.

[98] Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (Regolamento eIDAS 2 – European Digital Identity Wallet), *GUUE* L, 30 aprile 2024.

[99] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE

ISSN 2038-1662

acquisti online e a distanza, informazioni pre-contrattuali standardizzate, e protezioni contro pratiche commerciali sleali, completata dalla Direttiva sulle pratiche commerciali sleali[100] che proibisce pratiche ingannevoli o aggressive, dalla Direttiva sulle clausole abusive nei contratti[101] che invalida clausole vessatorie nei contratti con consumatori, dalla Direttiva sull'indicazione dei prezzi[102] che richiede trasparenza sui prezzi, e dalle direttive su Digital content[103] e Digital contracts for goods[104] che adattano le garanzie di conformità e i rimedi per prodotti digitali e beni con elementi digitali. Il Regolamento sulla sicurezza generale dei prodotti[105] riforma completamente la sicurezza dei prodotti per l'era digitale rafforzando tracciabilità attraverso identificatori unici, obblighi per marketplace online di verificare che i venditori rispettino le regole e rimuovere rapidamente prodotti pericolosi, coordinamento di richiami transfrontalieri, e poteri di enforcement rafforzati per le autorità di sorveglianza del mercato, mentre la Direttiva sulla responsabilità da prodotto difettoso[106] aggiorna le regole sulla responsabilità del produttore per l'era digitale coprendo esplicitamente software difettoso inclusi aggiornamenti che introducono difetti, prodotti con elementi digitali dove i difetti possono essere sia hardware che

---

del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio (Direttiva sui diritti dei consumatori), *GUUE* L 304, 22 novembre 2011.

[100] Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio (Direttiva sulle pratiche commerciali sleali), *GUUE* L 149, 11 giugno 2005.

[101] Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori, *GUCE* L 95, 21 aprile 1993.

[102] Direttiva 98/6/CE del Parlamento europeo e del Consiglio, del 16 febbraio 1998, relativa alla protezione dei consumatori in materia di indicazione dei prezzi dei prodotti offerti ai consumatori, *GUCE* L 80, 18 marzo 1998.

[103] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (Direttiva sui contenuti e servizi digitali), *GUUE* L 136, 22 maggio 2019.

[104] Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE e che abroga la direttiva 1999/44/CE (Direttiva sulla vendita di beni), *GUUE* L 136, 22 maggio 2019.

[105] Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 e la direttiva (UE) 2020/1828, e che abroga la direttiva 2001/95/CE e la direttiva 87/357/CEE del Consiglio (Regolamento sulla sicurezza generale dei prodotti – General Product Safety Regulation, GPSR), *GUUE* L 135, 23 maggio 2023.

[106] Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi e che abroga la direttiva 85/374/CEE del Consiglio (Direttiva sulla responsabilità da prodotto – Product Liability Directive), *GUUE* L, 18 novembre 2024.

ISSN 2038-1662

software, e sistemi AI sotto responsabilità oggettiva dove il danneggiato non deve provare colpa ma solo difetto, danno e nesso causale. La Direttiva sul diritto alla riparazione[107] promuove la riparabilità dei prodotti in chiave di economia circolare obbligando i produttori a rendere disponibili pezzi di ricambio e informazioni tecniche a riparatori indipendenti per un periodo definito, mentre il Regolamento sulla progettazione ecocompatibile[108] impone standard di sostenibilità ambientale con requisiti di efficienza energetica, durabilità, riparabilità, riciclabilità per categorie crescenti di prodotti inclusi sempre più prodotti digitali, il tutto sviluppato attraverso consultazione tecnica nell'Ecodesign Forum. La governance di questo cluster coinvolge la DG Competition per enforcement antitrust, l'*European Competition Network* (ECN) che coordina le autorità nazionali di concorrenza, gli *Advisory Committee on Restrictive Practices and Dominant Positions e on Concentrations* che assistono la Commissione, l'*High-Level Group on DMA* per il Regolamento sui mercati digitali, la *DG JUST* (Unit B.3) per l'enforcement dei diritti dei consumatori.

La sopra delineata normativa a otto cluster rappresenta un tentativo estremo di governance democratica della trasformazione tecnologica. L'obiettivo di tale approccio è tentare du dimostrare come sia possibile costruire un'economia digitale competitiva e innovativa che rispetti simultaneamente diritti fondamentali, protegga l'ambiente[109], garantisca sicurezza e promuova equità sociale. La tensione tra questi obiettivi potenzialmente contrastanti – regolare per proteggere diritti e creare un contesto competitivo per le imprese – costituisce la sfida politica ed economica centrale che l'UE dovrà affrontare nei prossimi anni, con la risposta che non può essere semplicemente "più regolamentazione" o "meno regolamentazione". Il *Digital Fitness Check* è un tentativo di affrontare questa sfida attraverso una valutazione sistematica dell'impatto cumulativo delle regole digitali europee che riconosce esplicitamente le preoccupazioni su oneri di compliance, sovrapposizioni normative, incoerenze tra strumenti diversi, e potenziali effetti negativi su innovazione e competitività[110].

---

[107] Direttiva (UE) 2024/1799 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che modifica le direttive 2005/29/CE e 2011/83/UE per quanto riguarda la responsabilizzazione dei consumatori per la transizione verde mediante il miglioramento della tutela dalle pratiche sleali e dell'informazione (Direttiva sul greenwashing e sull'obsolescenza programmata), *GUUE* L, 26 giugno 2024.

[108] Regolamento (UE) 2024/1781 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che istituisce un quadro per la definizione delle specifiche di progettazione ecocompatibile dei prodotti sostenibili, che modifica la direttiva (UE) 2020/1828 e il regolamento (UE) 2023/1542 e che abroga la direttiva 2009/125/CE (Regolamento sulla progettazione ecocompatibile dei prodotti sostenibili – Ecodesign for Sustainable Products Regulation, ESPR), *GUUE* L, 28 giugno 2024.

[109] Sui problemi dell'AI Act rispetto alla tutela dell'ambiente, si veda N. Rangone, *Intelligenza artificiale, tutela dell'ambiente e regolazione europea*, in *Biolaw Journal - Rivista di biodiritto*, 1, 2025.

[110] Si veda https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules_en.

ISSN 2038-1662

4. Dalla regolazione alla politica industriale

Lo sviluppo dell'industria digitale europea ed i relativi assetti di mercato, descritti in precedenza, evidenziano alcune "luci", ad esempio, nel supercalcolo e in alcune filiere della *space economy*, e diverse "ombre", come nel cloud, microchip, *large language model*, e tutti i servizi di piattaforma base).

Questa base chiaro-scura è quella su cui si innestano gli atti normativi e le politiche europee sul digitale, descritte nella sezione 2, che testimoniano un generale cambio di paradigma nell'intervento pubblico europeo: lo spostamento progressivo da un'impostazione prevalentemente regolatoria, nel senso classico di disciplina del mercato e tutela di diritti dei consumatori, verso un'impostazione che incorpora esplicitamente strumenti di politica economica ed industriale.

Oscillazioni del pendolo che definisce il "rapporto mobile"[111] fra regolazione e politica industriale, in generale, non sono tuttavia una novità. Il paradigma della regolazione economica sviluppatosi nei processi di liberalizzazioni delle *public utilities* (telecomunicazioni, energia, trasporti a rete, servizi postali) nasce infatti in un contesto molto specifico di monopolio legale pubblico.

In tale ambito, la regolazione pro-concorrenziale ha riconosciuto che le primarie "infrastrutture" dei servizi di pubblica utilità – reti di accesso, reti di trasmissione, infrastrutture di smistamento, ecc. - tipicamente realizzate e/o consolidate con risorse pubbliche o in regime di concessione esclusiva – sono essenziali e/o difficilmente duplicabile. Si è introdotta quindi un'asimmetria regolatoria, imponendo obblighi e costi sull'incumbent/ex-monopolista - in primis l'accesso alle infrastrutture essenziali a condizioni eque, trasparenti e non discriminatorie. Questa architettura regolatoria ha reso chiaro un elemento cruciale per il confronto col digitale: la regolazione settoriale "storica" ha inciso direttamente sulla struttura dell'industria: l'accesso regolato all'*essential facility* ha prodotto, in tempi relativamente brevi, ingresso e consolidamento di concorrenti[112].

La regolazione dei mercati digitali nasce, invece, con fatica[113], in un contesto completamente diverso. Un contesto di mercato aperto in cui lo scopo principale era

---

[111] L. Torchia, *I mercati e la loro disciplina: il bilancio di un decennio*, in *Rivista della regolazione dei mercati*, 2, 2024.

[112] In altri termini, così come la creazione di monopoli per le industrie, reti e servizi pubblici è stata politica industriale, similarmente lo è stata la loro liberalizzazione e la regolazione pro-concorrenziale, cui si lega indissolubilmente in quanto liberalizzazione "sostanziale", che ha ridefinito i mercati e le imprese in essi attive.

[113] Il processo di sviluppo delle politiche pubbliche di regolazione delle piattaforme digitali non è stato né semplice né lineare: inizialmente, i mercati digitali sono stati oggetto di un approccio prudenziale, volto a evitare interventi eccessivi che potessero ostacolare l'innovazione e a coltivare l'idea di un web come spazio di libertà individuale poco soggetto a regolazione pubblica, visione oggi ampiamente superata. Con la centralizzazione strutturale del web nelle mani di poche piattaforme globali, il dibattito si è spostato dalla scelta fra regolazione e non-regolazione a quella tra regolazione pubblica e regolazione privata, mentre la teoria economica continuava a sostenere che, grazie alla

ISSN 2038-1662

quello di creare le precondizioni e gli incentivi alla fornitura e l'adozione dei servizi (direttiva e-commerce), con obiettivi primari di tutela del cittadino/consumatore, per creare fiducia nell'ambiente digitale: privacy, trasparenza, correttezza delle pratiche commerciali, sicurezza degli utenti, integrità dello spazio informativo.
La scelta naturale è stata quasi sempre quella di una regolazione simmetrica, applicabile cioè a tutti i soggetti che trattano dati, offrono servizi digitali o operano come intermediari. In questa traiettoria si collocano, con logiche diverse, il GDPR, i più recenti interventi sul governo/uso dei dati (ad es. Data Act), la modernizzazione della tutela consumeristica (direttiva "Omnibus") e parti importanti della disciplina sui servizi digitali (DSA), dove la finalità primaria è ridurre asimmetrie informative, rischi e danni per utenti e consumatori, e rafforzare accountability e trasparenza.
Mentre nel paradigma delle liberalizzazioni la regolazione ha scaricato intenzionalmente buona parte dell'onere sull'*incumbent* (regolazione asimmetrica), nel digitale la regolazione "dei diritti" tende inevitabilmente a distribuire l'onere su un insieme ampio di attori. Questa impostazione è tuttavia risultata sempre più ambivalente sul versante industriale, in quanto l'applicazione simmetrica si è trasformata – nei fatti – in un costo fisso di *compliance* che, con il crearsi di asimmetrie enormi fra i vari player, è andata a pesare relativamente molto di più sugli operatori piccoli e sui nuovi entranti, che non hanno la possibilità di spalmare tali costi su basi utenti/ricavi comparabili a quelle dei grandi operatori.
Ne consegue che, proprio nei contesti in cui l'Europa presenta un tessuto produttivo più frammentato (startup, PMI innovative, operatori specializzati), una regolazione simmetrica molto esigente rischia di produrre un effetto collaterale: non tanto "meno innovazione" in astratto, quanto un innalzamento della soglia minima per stare sul mercato (soglia legale, organizzativa e tecnologica).[114]

---

forte concorrenza potenziale e ai bassi costi di transazione, il potere di mercato restasse temporaneo e contestabile, senza che fenomeni di "tipping" risultassero inevitabili o irreversibili. In questo quadro, la mancanza di un quadro regolatorio efficace è stata anche dovuta a una "limitata capacità regolatoria", legata da un lato a una marcata asimmetria informativa tra policy maker e piattaforme, dovuta alla rapida innovazione tecnologica, e dall'altro a un processo decisionale pubblico ancora prevalentemente nazionale, che fatica a interagire con l'orizzonte globale delle piattaforme e a disegnare regole efficaci e coerenti. Cfr Manganelli (2021) La proposta di regolamento Eu per i mercati digitali: ratio, criticità e prospettive di evoluzione, in Mercato concorrenza regole / a. XXIII, n. 3, dicembre 2021

[114] In questa stessa direzione, il Rapporto Draghi sottolinea che, in un quadro in cui coesistono regole nazionali eterogenee (anche per fenomeni di *gold-plating*) e obblighi "precauzionali" ex ante, l'effetto può diventare paradossale: la regolazione finisce per essere sostenibile soprattutto per operatori di grande dimensione (spesso extra-UE), mentre i nuovi entranti rinunciano a scalare o persino a operare nel mercato europeo. Da qui l'enfasi su una correzione di rotta "pro-competitività": riduzione e semplificazione degli adempimenti dove possibile, valutazioni d'impatto mirate sui costi di compliance, maggiore armonizzazione nell'implementazione/enforcement (ad es. del GDPR) e riduzione di sovrapposizioni e incoerenze fra regimi (in particolare rispetto alla regolazione dell'AI), così da evitare che la regolazione simmetrica dei "diritti" alzi la soglia minima per competere proprio

ISSN 2038-1662

Peraltro, come descritto nella sezione 1, anche nei mercati digitali si sono progressivamente creati assetti estremamente concentrati, fino a forme di quasi-monopolio o oligopolio ristretto. Tuttavia, la genesi di queste posizioni dominanti è diversa da quella delle utilities, poi liberalizzate: non deriva (in via principale) da barriere giuridiche alla concorrenza (monopoli legali o concessioni esclusive), ma da dinamiche di mercato e innovazione in contesti globali.

I noti meccanismi sono molteplici e cumulativi: economie di scala e di scopo (spesso con costi marginali bassissimi), effetti di rete diretti e indiretti, *lock-in* e *switching costs*, vantaggi informativi e di apprendimento legati ai dati, integrazione verticale e conglomerale tra servizi complementari, standard *de facto* e interfacce proprietarie, controllo dei canali di distribuzione (app store, sistemi operativi, marketplace), fino a dinamiche *winner-takes-all/most*.[115]

Nei mercati e nell'industria digitale non esiste quindi né un percorso politico-normativo da invertire, redistribuendo risorse, asset e rendite createsi in regime di monopolio; né tantomeno un singolo "interruttore" economico-regolatorio analogo a quello delle utilities, ossia aprire l'accesso all'infrastruttura pubblica/monopolistica; nei vari mercati dell'industria digitale le barriere economiche sono principalmente tecnologiche e di ecosistema che si auto-rafforzano nel tempo. In altri termini, rispetto alla regolazione delle utilities, in cui il "fattore produttivo scarso" era l'accesso alla rete, nel digitale, il "fattore scarso" è un insieme di risorse (capitale, conoscenza, utenti, dati, standard) che di per sé non sono scarse, ma lo è il loro uso complementare, che la regolazione non riesce così facilmente a disciplinare e ristrutturare.

L'azione regolatoria pro-concorrenziale incontra, quindi, limiti strutturali nell'ecosistema digitale, in quanto una disciplina che vieti ex-ante pratiche (potenzialmente) escludenti e agevoli un *level playing field* concorrenziale può non essere sufficiente a creare le condizioni economiche perché un entrante raggiunga massa critica; inoltre, le dinamiche competitive e tecnologiche sono così rapide che quando l'equilibrio di mercato si consolida, gli interventi ex post antitrust sono tardivi ma anche interventi ex ante, se non accompagnati da leve di scala e investimento, rischiano di migliorare la "correttezza" del gioco senza cambiarne il risultato industriale.

Il Digital Markets Act (DMA) rappresenta il tentativo più evoluto di adattamento dell'economia digitale al paradigma regolatorio pro-concorrenziale "asimmetrico": individua soggetti qualificati come *gatekeeper* e impone obblighi e divieti ex ante, con l'obiettivo di correggere squilibri strutturali nei mercati dei *core platform services*. Tuttavia, proprio il diverso contesto di mercato ha condizionato la definizione dei suoi

nei segmenti più dinamici dell'innovazione. M. Draghi, *The future of European Competitiveness*, 2024.

[115] F. Chirico e A. Manganelli, Mercati e servizi digitali, in C. Cambini, G. Napolitano e A. Nicita (a cura di), *Economia e Diritto della Regolazione. Reti, piattaforme e servizi di pubblica utilità*, Bologna, 2024.

ISSN 2038-1662

obiettivi: la contendibilità, tesa a creare spazi di potenziali concorrenza - e l'equità, tesa a limitare pratiche di sfruttamento e riequilibrare i rapporti tra piattaforme e imprese utenti/complementors.
Il perseguimento ed anche il raggiungimento di questi obiettivi può rendere il mercato "più aperto", attraverso obblighi di portabilità e interoperabilità, ed alla fine più "contendibile" senza che ciò, tuttavia, comporti l'emersione di nuovi soggetti industriali europei capaci di competere nelle stesse filiere industriali estese e sugli stessi mercati globali.
È in questo contesto che si comprende il passaggio verso la politica industriale: non come abbandono della regolazione, ma come riconoscimento che la regolazione – persino nella sua forma più "ambiziosa" e asimmetrica – non produce automaticamente capacità produttive, filiere, investimenti e scala, tendendo a ribilanciare le quote di mercato, soprattutto quando i mercati di riferimento sono globali e i concorrenti sono in posizione di mercato preminente.
L'evoluzione del contesto geo-politico ha quindi contribuito a spostare la giustificazione dell'intervento pubblico: non solo (o non tanto) correggere inefficienze statiche, come rimedio puntuale al potere e ai fallimenti di mercato, ma rafforzare la capacità competitiva in mercati globali, aumentando autonomia e resilienza verso crisi o rischi che impattano sulla capacità produttiva, commerciale ed infine anche "politica", nel senso pieno del termine[116].
Nell'ecosistema digitale, questo quadro ha portato le politiche pubbliche verso nuovi paradigmi di intervento pubblico:

1. La politica industriale digitale deve agire sui colli di bottiglia della capacità europea, che oggi non sono (solo) normativi ma di scala di investimento, accesso a risorse computazionali, disponibilità di infrastrutture cloud e dati, attrazione di talenti, standard e interoperabilità, procurement e domanda aggregata.
2. La regolazione resta necessaria per rendere/mantenere aperto l'ecosistema, ma non può assumersi l'obiettivo di "fare industria". Il rischio, altrimenti, è duplice: da un lato, aspettative irrealistiche sugli effetti industriali di strumenti nati per obiettivi diversi (tutela di diritti, correttezza dei mercati); dall'altro, tentazioni di piegare il diritto della concorrenza e la regolazione pro-mercato a finalità di protezione dei campioni europei, con effetti potenzialmente distorsivi[117].
3. È necessaria una coerenza tra regole e investimenti. Se l'UE intende ridurre dipendenze (ad es. nel cloud, nei microchip, nelle piattaforme e nell'IA), occorre un disegno in cui le regole abilitino interoperabilità e riducano lock-in, mentre la politica industriale costruisce alternative credibili (infrastrutture, piattaforme, standard, progetti comuni e domanda pubblica).

[116] C. Scarpa, *Cosa c'è di nuovo nella "nuova" politica industriale europea?*, in *Rivista della regolazione dei mercati*, 2, 2024.
[117] M. Grillo, *Concorrenza e politica industriale: cosa cambia con la globalizzazione*, in *Rivista della regolazione dei mercati*, 2, 2024.

ISSN 2038-1662

4. Infine, un elemento spesso sottovalutato nel dibattito pubblico europeo è che l'intervento pubblico, può incidere sulla traiettoria industriale anche attraverso la domanda pubblica, commesse e programmi *mission-oriented*. La letteratura di politica dell'innovazione (e il filone che insiste sul ruolo dello Stato come co-produttore di mercati e tecnologie) ha mostrato come, in diversi settori high-tech, la domanda pubblica e gli investimenti pubblici abbiano svolto un ruolo abilitante nel ridurre l'incertezza e accelerare la scalabilità delle soluzioni[118].

In sintesi, il passaggio dalla regolazione alla politica industriale, nel digitale, va letto come passaggio da una logica centrata sulla correzione del mercato (e sulla tutela di diritti) a una logica che include la ricostruzione del mercato: costruzione di capacità, resilienza ed indipendenza/autonomia strategiche ed infine competitività

Questa spinta verso la competitività è tanto forte da includere in questo percorso anche le industrie a rete tradizionali [119]. Non sembra infatti (più) realistico per il *policy maker* europeo concepire la regolazione economica come un mero strumento di riequilibrio degli svantaggi competitivi legati alla disponibilità di infrastrutture, quando tali infrastrutture sono soggette a intensi cicli di innovazione e, al tempo stesso, costituiscono fattori abilitanti di tecnologie complementari, generando esternalità positive diffuse in tutto l'ecosistema digitale e nell'economia nel suo complesso. Ossia, quando e se le infrastrutture "tradizionali" divengono variabili di competitività geopolitica, si assiste ad una "ripresa della politica industriale" [120].

5. La Politica industriale verso la "sovranità digitale" e la "autonomia strategica"

Come evidenziato dai report Draghi e Letta, l'Unione è dinnanzi ad una sfida esistenziale: colmare il divario di produttività con Stati Uniti e Cina, decarbonizzare l'economia e ridurre le dipendenze strategiche da paesi terzi, con una risposta che si articola attraverso tre pilastri interconnessi: semplificazione regolamentare, completamento del mercato unico e creazione di un clima favorevole agli investimenti.

---

[118] M. Mazzucato e C. Perez, *Redirecting growth: inclusive, sustainable and innovation-led,* in E. S. Reinert e I. H. Kvangraven (a cura di), *A Modern Guide to Uneven Economic Development,* Cheltenham*,* 2023. Un esempio discusso spesso è quello delle infrastrutture e applicazioni della *space economy*, dove anche servizi poi "commerciali" possono aver beneficiato in origine di committenza e programmi pubblici Spesso il caso Starlink è frequentemente richiamato in questa chiave. A. Manganelli e A. Perrucci, *La "nuova" economia dello spazio e il "caso Starlink". Profili economico-giuridici e di policy*, in *Rivista della regolazione dei mercati*, 1, 2025.

[119] Si veda le comunicazioni elettroniche e la recente proposta di Digital Network Act.. A. Manganelli, *Il Digital Networks Act, fra nuove tecnologie, nuove dinamiche di mercato e vecchi principi regolatori*, in *Rivista della regolazione dei mercati*, 2, 2025.

[120] L. Ammannati, *Per una politica industriale comune. Scelte di governance dell'Unione europea*, in *Rivista della regolazione dei mercati*, 2, 2024.

ISSN 2038-1662

È nel contesto sopra delineato che il concetto di sovranità digitale[121] è emerso sempre più, catalizzato dalla pandemia COVID-19 che ha esposto drammaticamente le vulnerabilità e le dipendenze dell'Europa[122] (sebbene il termine risalga già ai tempi del programma Galileo, nel 2000[123]).
Oggi l'UE dipende dai paesi stranieri per oltre l'80% dei suoi prodotti, servizi e infrastrutture digitali[124]. Tale situazione sta rappresentando il principale *trigger* delle recenti azioni di politica economica nell'industrie digitali.
Il presidente francese Macron ha richiamato la necessità di garantire la sovranità digitale a livello europeo, affermando che spetta all'Europa definire il quadro normativo che impone a sé stessa, in quanto ciò implica sia la protezione delle libertà individuali sia dei dati economici delle sue imprese - elementi al centro della sua sovranità e della sua capacità operativa concreta di agire in modo autonomo[125]. La Germania si è soffermata invece sull'obiettivo di rafforzare i fornitori nazionali, con investimenti mirati nella competitività e la salvaguardia dalle distorsioni della concorrenza, superando il concetto generale di autosufficienza digitale[126].

Da ultimo, nella dichiarazione di Vienna per la sovranità digitale europea, gli Stati membri firmatari hanno definito la sovranità digitale come "capacità dell'UE e dei suoi Stati membri di agire in modo autonomo e di scegliere liberamente le proprie soluzioni, pur beneficiando, quando possibile, della collaborazione con partner globali"[127]. È un

---

[121] P. Bellanger, *De la souveraineté en général et de la souveraineté numérique en particulier*, in *Les Echos*, 30.08.2011, disponibile qui: http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm; F. Gueham, *Digital Sovereignty – Steps towards a new system of Internet Governance, Fondation pour l'innovation politique*, gennaio 2017, pp. 9 e 11. Più recentemente. O. Pollicino, *Potere digitale*, in M. Cartabia, M. Ruotolo (diretto da), *Enciclopedia del diritto. Potere e Costituzione*, Milano, 2023, p. 411, quale forma di legittimazione e controllo del potere pubblico nel contesto digitale su dati, software, standards, servizi e infrastrutture. A tal riguardo, si vedano anche H. Roberts, J. Cowls, F. Casolari, J. Morley, M. Taddeo e L. Floridi, *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, in *Internet Policy Review*, 2021, p. 3.
[122] P. Zuddas, *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio AIC*, 3/2020, p. 83.
[123] C. Hobbs, *L'Europa alla ricerca di una sovranità digitale: sfide e interessi in gioco*, in *Agenda Digitale*, 8 ottobre 2020.
[124] Commissione europea (2023), *Relazione sullo stato del decennio digitale 2023*, COM(2023) 570 final, 27 settembre 2023.
[125] Si veda https://www.elysee.fr/en/emmanuel-macron/2025/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe. Si veda anche, nel 2020, E. Macron, "*Discours du Président Emmanuel Macron sur la stratégie de défense et de dissuasion devant les stagiaires de la 27ème promotion de l'école de guerre*" (7 febbraio 2020).
[126] Si veda https://www.bundesregierung.de/breg-en/news/digital-sovereignty-2394992.
[127] Nella dichiarazione di Vienna – A livello più "tecnico", la sovranità europea è descritta come "*la capacità di costruire capacità, resilienza e sicurezza riducendo le dipendenze strategiche, prevenendo la dipendenza da attori stranieri e da singoli fornitori di servizi, e salvaguardando tecnologie e infrastrutture critiche; invita allo sviluppo di un quadro completo di valutazione dei rischi per*

ISSN 2038-1662

riscontro tardivo alla percezione di una perdita di autonomia, competitività e sicurezza nello spazio digitale[128].

Il concetto di sovranità digitale, pur essendo diventato centrale nel discorso politico europeo, rimane caratterizzato da una certa ambiguità definitoria e sovrapposizione tra i termini "sovranità", "automomia digitale"[129] e "autonomia strategica"[130], e con un significato più politico che giuridico[131].
Il concetto di "autonomia strategica"[132] - inizialmente definito significativamente come autonomia strategica "aperta" - evidenzia la capacità dell'Unione europea di agire in modo indipendente in settori chiave, mantenendo al contempo partnership globali costruttive. Esso implica la capacità di decidere quando e come esercitare tale indipendenza, rafforzando una visione di "interdipendenza" - piuttosto che di indipendenza - sostenuta da alternative credibili che riducono la vulnerabilità alle dipendenze critiche.
Ai nostri fini, è utile vedere – in primo luogo – come la Commissione si è mossa e si sta muovendo, rispetto alle difficoltà legate al ruolo del potere privato nella sfera pubblica digitale, alle interferenze da parte di attori stranieri, alla crisi dello Stato di diritto, al rischio di una governance digitale non adeguata e alla carenza di alfabetizzazione digitale[133].
In questo contesto, si inserisce la Bussola della competitività dell'UE, che mira a colmare il divario di innovazione (primo pilastro) ed a ridurre le dipendenze strategiche (terzo pilastro). Entrambi questi i pilastri mirano in ultima analisi a rafforzare

monitorare e affrontare le dipendenze lungo l'intera catena del valore digitale; sottolinea che tale quadro dovrebbe costituire la base per garantire la preparazione e la resilienza dell'UE, rafforzando la politica industriale europea e potenziando le capacità interne di ricerca e sviluppo e di produzione nelle tecnologie strategiche" *(.....)*

[128] L. von Ditfurth, *The European Union's Pursuit of Digital Sovereignty Through Legislation*, in *JIPITEC*, 16, 2025, pp. 286 ss.

[129] Per un'analisi che parte dal caso Costa v ENEL, si veda N. A. Smuha, *Digital Sovereignty in the European Union: five challenges from a normative perspective*, in G. Barrett et al. (a cura di), *European Sovereigtny: the legal dimension*, New York, 2024.

[130] T. Breton, *European Commission, Europe: Keys to sovereignty*, comunicato stampa, 11.09.2020, disponibile qui: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en; European Parliamentary Research Service, *EPRS Ideas Paper | Towards a more resilient EU, Digital sovereignty for Europe*, luglio 2020, pp.1-12. Si veda anche M. Merler, *Il ruolo della Commissione europea nella realizzazione dello spazio digitale europeo*, in *Rivista trimestrale di diritto pubblico*, 4, 2024, p. 1121. Sul tema è opportuno menzionare anche L. Floridi, *The fight for digital sovereignty: what it is, and why it matters, especially for the EU*, in 33 *Philosophy & Technology*, 2020, pp. 369 ss.

[131] G. Finocchiaro, *La sovranità digitale*, in *Diritto Pubblico*, 2022, pp. 809 e ss.

[132] C. Cagnin et al., *Shaping and securing the EU`s Open Strategic Autonomy by 2040 and beyond*, JRC paper, 2021; H. Kroll, *Assessing Open Strategic Autonomy*, JRC paper, 2021.

[133] N. A. Smuha, *Digital Sovereignty in the European Union: five challenges from a normative perspective, cit.*

ISSN 2038-1662

l'"autonomia strategica" dell'UE, ma lo fanno da angolazioni diverse e con tempistiche distinte.
Questo obiettivo può essere perseguito attraverso azioni di policy che rientrano sostanzialmente in due tipi di azioni: (i) misure volte a promuovere catene di approvvigionamento alternative basate sull'UE ("abilitanti"); (ii) misure volte a limitare o restringere la presenza di fornitori non UE ("restrittive").
Sebbene i confini tra le due non siano sempre netti e possano non essere mutuamente esclusivi, la distinzione è importante dal punto di vista analitico e normativo. L'approccio restrittivo richiede infatti un'attenta valutazione, in particolare se sviluppato e portato a compimento nel breve periodo. Qualsiasi dipendenza ha alla base un "bisogno" industriale o economico, che in questo caso è direttamente correlato con la competitività dell'Europa e degli stati membri. La digitalizzazione, ossia l'adozione e l'uso efficace di tecnologie e servizi digitali, ha infatti un chiaro impatto specifico sulla produttività e sulla competitività.[134]
La ricerca di una maggiore indipendenza comporta, quindi, nel breve termine potenziali rischi, tra cui un possibile rallentamento della diffusione digitale, una minore qualità dei servizi e una riduzione della scelta dei consumatori. Tali *trade-off* evidenziano la complessità dell'attuale contesto di policy, in cui trovare un efficiente equilibrio non è così semplice, ma è essenziale per garantire che gli sforzi volti a diminuire le dipendenze non ostacolino inavvertitamente il ciclo di innovazione che lo stessa Bussola per la Competitività mira ad accelerare. [135]
Diviene quindi cruciale la questione dell'esistenza di fornitori europei alternativi che siano in grado di fornire la stessa quantità, varietà e qualità di servizi. Tale assetto, come accennato, non è banale e dipende in larga misura dal settore e dal servizio specifici che stiamo considerando. E, in ogni caso, rende pivotale la definizione di politiche "abilitanti" e conferisce loro anche una priorità economica e logico-temporale – anche in ragione del tempo necessario affinché queste producano un risultato tangibile nel mercato in termini di promozione attiva dello sviluppo dell'industria europea.
Un approccio abilitante eurounitario può consentire progressivamente alle imprese europee di competere in modo più efficace, sia nei mercati privati che negli appalti pubblici. Tuttavia, dovrebbe essere progettato con attenzione poiché le politiche abilitanti possono incontrare due vincoli: (i) effetti soglia - un sostegno insufficiente non riesce a superare gli svantaggi strutturali, generando costi senza vantaggi competitivi; e (ii) effetti di dipendenza - un sostegno eccessivo o prolungato può creare dipendenza dall'intervento pubblico piuttosto – che presumibilmente non può essere permanente, che costruire una capacità reale.
Una ulteriore dimensione delle politiche orientate all'autonomia strategica si riferisce all'ambito di applicazione, ossia la distinzione fra misure rivolte ai privati (consumatori

[134] Draghi, 2024, cit.
[135] Z. Mayers, *A framework for understanding EU competitiveness*, CERRE issue paper, 2024.

ISSN 2038-1662

e imprese) e misure rivolte ai i governi e altre amministrazioni pubbliche ("privato" vs "pubblico").[136]

Le opzioni di policy rivolte ai servizi per gli enti pubblici non implicano necessariamente minori trade-off economici; tuttavia, il quadro analitico può essere soggetto a una rivalutazione quando entra in gioco la sicurezza nazionale. In questi ambiti, un approccio maggiormente fondato sul principio di precauzione - rispetto a quello basato sul principio di proporzionalità che anima gran parte della regolazione e delle politiche a fine di efficienza nella UE - potrebbe essere considerato più giustificato.

Il fine è quello di dare priorità alla protezione contro rischi a bassa probabilità ma ad alto impatto (sorveglianza straniera, interruzione delle infrastrutture, leva coercitiva), anche quando tali rischi non possono essere quantificati con precisione. Tuttavia, una certa proporzionalità d'azione sembra comunque necessaria. Pertanto, invocare la sicurezza per giustificare misure precauzionali non può essere esteso indiscriminatamente, ma dovrebbe essere valutato e mirato con precisione.

Infine, sembra importante notare come obiettivi abilitati dal lato dell'offerta, e.g., reti digitali, cloud, e altre infrastrutture digitali, si giustificano sotto un profilo economico sul fatto che i guadagni di produttività derivanti dalle tecnologie general-purpose (GPT)[137] spesso si manifestano con un ritardo temporale.[138] Ciò avviene perché l'adozione e le capacità complementari tendono a seguire il dispiegamento infrastrutturale solo dopo un periodo di aggiustamento. Ne consegue che un investimento precoce in infrastrutture può essere economicamente giustificato, in aree ad alto potenziale in cui si possano raggiungere un punto di svolta (*tipping point*) e un adeguato ritorno sull'investimento. Inoltre, l'inerzia infrastrutturale, gli elevati costi fissi e i "colli di bottiglia regolatori" rendono impraticabile un dispiegamento completamente "reattivo" o comunque non facilmente e rapidamente adattabile alla domanda di mercato.[139]

---

[136] Questa distinzione è generalmente più chiara della dicotomia abilitante/restrittiva, poiché la categoria degli utenti finali è più facilmente identificabile, anche se permangono zone grigie nei partenariati pubblico-privati, nelle infrastrutture critiche e nelle tecnologie a duplice uso.

[137] Le GPT condividono tre caratteristiche distintive: (i) sono pervasivi nelle loro applicazioni, (ii) migliorabili nel tempo e (iii) in grado di catalizzare innovazioni complementari che ampliano il loro impatto trasformativo. Sono quindi in genere caratterizzate da un'ampia applicabilità e dalla capacità di generare esternalità positive pervasive, aumenti di produttività e una crescita economica diffusa.

[138] E. Brynjolfsson, *The productivity paradox of information technology*, in Communications of the ACM, 36 (12), 1993, pp. 66–77; E. Brynjolfsson, D. Rock, C. Syverson, *The Productivity J-Curve: How Intangibles Complement General Purpose Technologies*, in *American Economic Journal: Macroeconomics*, 13 (1), 2021, pp. 333–72.

[139] Questo argomento è particolarmente forte per le cosiddette "infrastrutture trasformative", ossia tecnologie che abilitano servizi del tutto nuovi, anziché limitarsi a migliorare la qualità di quelli esistenti tramite aggiornamenti incrementali. Queste ultime, infatti, possono essere più facilmente guidate dalla domanda corrente.

ISSN 2038-1662

Detto ciò, tuttavia, gli obiettivi dal lato dell'offerta devono essere valutati rispetto alla domanda attuale e prevista, ossia perché l'"investimento anticipatorio" sia efficace, deve comunque riflettere effetti di produttività differenziati, esternalità e capacità di assorbimento. Nel caso dei *data centre* e delle *AI factories*, le tendenze della domanda e della disponibilità a pagare sono strettamente legate all'aumento dei carichi di lavoro legati all'IA, che richiedono una notevole capacità di archiviazione ed elaborazione dei dati.

Box 1. La progressiva definizione di una politica industriale per il cloud

Un settore paradigmatico dell'evoluzione della regolazione e della politica industriale europea è quello del cloud. Come evidenziato nella sezione 1, nonostante l'espansione dei fornitori di servizi cloud dell'UE, gli hyperscaler statunitensi rappresentano ancora circa il 70% del mercato dell'infrastruttura come servizio (IaaS) e del cloud privato.

Si prevede che questa tendenza persisterà a causa delle caratteristiche economiche del settore, nonostante i diversi atti di regolazione pro-concorrenziali in materia di cloud adottate dall'UE:[140] sia di regolazione asimmetriche (il cloud è un dei servizi di piattaforma basa definiti dal DMA) sia simmetriche (penetranti disposizioni a tutela del consumatore nello switching e terminazione dei contratti sono definite dal Data Act)[141]

Questo è uno dei settori in cui si segnala una forte dipendenza strategica sia un deficit di investimenti che l'Europa (fondi privati e/o pubblici) deve colmare per soddisfare tale esigenza (o parte di essa) in modi alternativi. Tale dipendenza è alla base di una molteplice vulnerabilità: il cloud è alla base di moltissimi servizi digitali, compreso l'addestramento e l'inferenza dei sistemi di intelligenza artificiale, ma è anche l'infrastruttura in cui sono ospitati dati, personali, non personali, sensibili o strategici.

In questo contesto il report Draghi sostiene che, sebbene sia troppo tardi per l'UE cercare di sviluppare concorrenti sistemici ai principali fornitori di servizi cloud statunitensi (gli investimenti necessari sono troppo ingenti e distoglierebbero risorse da settori e aziende in cui le prospettive innovative dell'UE sono migliori), l'UE dovrebbe garantire di disporre di un'industria nazionale competitiva in grado di soddisfare la domanda di soluzioni di 'cloud sovrano'.

Una delle principali azioni di policy dell'UE, che rappresenta un pilastro legislativo centrale della bussola della competitività, è la proposta di

[140] In particolare, il capitolo VI e VIII del Data Act (Regolamento 2023/2854), recentemente entrato in vigore e applicabile, e il Digital and Markets Act (Regolamento 2022/1925), che è stato caratterizzato da sfide concettuali e di applicazione per quanto riguarda i servizi cloud. A. Manganelli, *La composita regolazione europea dei servizi Cloud*, in *Mercato Concorrenza Regole*, 3, 2024.

[141] A. Manganelli e D. Schnurr, Competition and Regulation of Cloud Computing Services, CERRE Report, 2024.

ISSN 2038-1662

regolamento, in corso di elaborazione, sullo sviluppo del cloud e dell'intelligenza artificiale (CAIDA). La proposta legislativa CAIDA, prevista per il primo trimestre del 2026, dovrebbe essere strutturata attorno a tre pilastri principali: (i) ricerca e sviluppo, (ii) autonomia, che mira a creare un'infrastruttura cloud sicura con sede nell'UE, progettata per supportare casi d'uso strettamente definiti e altamente critici, in particolare quelli che richiedono livelli elevati di sicurezza dei dati, come nel settore pubblico; e (iii) implementazione, che sarà attuato attraverso l'adozione di obiettivi quantitativi concreti, in particolare concernenti la capacità di elaborazione dei dati dell'UE, che dovrebbe essere triplicata nei prossimi cinque-sette anni attraverso sviluppo di centri dati altamente sostenibili. Quest'ultimo obiettivo infrastrutturale è coerente con gli obiettivi del programma politico per il decennio digitale (DDPP) e li rafforza in modo sostanziale. Attualmente, infatti, l'UE ospita solo circa un terzo dei *data centre* degli Stati Uniti, il che limita notevolmente la sua capacità di supportare l'archiviazione di dati su larga scala e l'elaborazione relativa all'IA. [142]

Il CAIDA si concentra principalmente su misure promozionali "abilitanti" volte a rafforzare le industrie nazionali dell'UE nel settore del cloud e dell'IA; tuttavia, alcune disposizioni relative all'"autonomia" potrebbero funzionare come misure "restrittive", limitando l'accesso al mercato per i fornitori non UE. Queste andranno a complementare la revisione della direttiva *sul public procurement*, che la UE sta rivedendo, con l'obiettivo di introdurre criteri che valorizzino sovranità, sostenibilità e resilienza delle catene di valore, anche attraverso logiche di tipo "*buy European*" nei settori strategici.[143]

In questo contesto, sono emerse le soluzioni commerciali di "cloud sovrano" sviluppate dai principali hyperscaler, innescando un dibattito in corso su ciò che costituisce veramente la sovranità nel dominio cloud: se sia sufficiente la semplice localizzazione dell'infrastruttura all'interno dell'UE o se la vera sovranità richieda che i fornitori di servizi cloud siano di proprietà e gestione europea. In alternativa, le partnership transatlantiche, se adeguatamente regolamentate e conformi agli standard di protezione e sicurezza dei dati dell'UE, potrebbero anche allinearsi agli obiettivi di sovranità dell'UE?[144]

[142] Savills Research, *European Data Centres Navigating the new data-centric frontiers*, 2024, disponible a: https://pdf.euro.savills.co.uk/european/european-commercial-markets/spotlight-european-data-centres---may-2024.pdf

[143] Le norme attuali restano fondate sul terzetto di direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sugli appalti pubblici e sulle concessioni, destinate però a essere aggiornate da una nuova proposta legislativa attesa nel 2026.

[144] Le aziende possono rimanere soggette alle leggi delle loro giurisdizioni di origine, anche quando i dati o le operazioni si trovano fisicamente all'estero. In particolare, i fornitori di servizi cloud statunitensi rimangono soggetti alla legge americana indipendentemente dal luogo in cui gestiscono la loro infrastruttura, quindi al Clarifying Lawful Overseas Use of Data Act ("Cloud Act"), che consente alle autorità statunitensi di obbligare le aziende a fornire dati indipendentemente dalla loro ubicazione

ISSN 2038-1662

Recentemente, la definizione di un *Cloud Sovereignty Framework* (CSF) [145] si è collocata come strumento operativo non vincolante per gli Stati membri, ma vincolante per i fornitori che partecipano a un tender interno alla Commissione.[146]. Il CSF traduce la politica di sovranità digitale in criteri oggettivi – tramite obiettivi di sovranità, *Sovereignty Effective Assurance Levels* e *Sovereignty Score* – che operano come requisiti di ammissibilità e criteri di aggiudicazione nel bando UE, rendendo la sovranità valutabile e premiante. Anche se questo non è un atto normativo diretto sui Paesi membri, il CSF esercita un'importante influenza di fatto: fornisce un modello comune di valutazione della sovranità del cloud che molte amministrazioni nazionali possono adottare o ispirare nei propri bandi, agendo di fatto come soft law / punto focale di coordinamento e riferimento per standard di "cloud sovrano" e orienta la progettazione delle offerte da parte dei fornitori globali, rinforzando così, sul terreno, la politica UE di "buy European" e di autonomia strategica nel digitale.

6. Alcune criticità dell'evoluzione delle policy UE

La proliferazione legislativa – descritta in precedenza – ha dato l'idea, sino ai tempi recenti, di una direzione chiara: da una visione principalmente economico-regolatoria del mercato unico digitale a una concezione più ampia di politica industriale che integra preoccupazioni di sicurezza nazionale, autonomia, resilienza delle infrastrutture critiche e valori fondamentali europei volti ad affermare la propria sovranità[147]. Tuttavia, tra le varie, due macro-criticità si inseriscono di fronte al successo Unionale in termini di sovranità: i) la fase di implementazione della normativa da parte degli Stati membri, ii) un recente cambio di rotta verso una semplificazione che sembra "opaca. Questi temi saranno affrontati – a titolo di esempio, senza poterli realisticamente declinare in tutti i profili del digitale – in relazione alla regolazione dell'intelligenza artificiale.

Il primo aspetto è di sovente sottovalutato. Mentre l'UE promuove un quadro normativo ambizioso per affermare la propria autonomia strategica nel settore digitale, gli Stati membri, particolarmente quelli dell'Europa centro-orientale, ma non solo, mostrano

fisica, e alla "FISA Section 702", che consente la sorveglianza dei dati di cittadini non statunitensi conservati da aziende americane al di fuori degli Stati Uniti. Naturalmente, tutte queste procedure sono soggette a limitazioni giuridiche sostanziali e procedurali e non sono molto diverse, in termini di impatto sui diritti degli utenti, da leggi simili in vigore negli Stati membri dell'UE.

[145] *Cloud Sovereignty Framework* (CSF) 1.2.1, ottobre 2025, adottato dalla Direzione Generale per i Servizi digitali.

[146] Cloud III DPS, valore 180 milioni di euro.

[147] B. Marchetti, *L'esecuzione della regolazione digitale dell'Unione europea e il ruolo della Commissione*, in *Rivista trimestrale di diritto pubblico*, 4, 2024, p. 1096.

ISSN 2038-1662

resistenze significative legate alla preservazione della sovranità nazionale[148]. Questa tensione non è semplicemente una questione tecnica, ma riflette divergenze profonde su cosa significhi esercitare il potere nell'era digitale e su chi debba avere l'autorità di regolare uno spazio che per sua natura trascende i confini nazionali.
Si è visto che il concetto di sovranità digitale sviluppato dall'Unione negli ultimi anni è articolato e multidimensionale. Non si tratta semplicemente di erigere barriere protezionistiche contro i giganti tecnologici americani o cinesi, ma di costruire un'industria europea che anche internalizzi un modello alternativo di governance digitale che rifletta i valori europei. Come è noto, gli Stati membri dell'Unione presentano livelli estremamente diversi di sviluppo economico, priorità politiche e capacità regolatorie. Questa eterogeneità è particolarmente pronunciata nei Paesi più piccoli come Ungheria, Slovacchia e Repubblica Ceca, dove lo sviluppo delle infrastrutture digitali e la capacità di applicare efficacemente le normative dipendono in larga misura dai finanziamenti europei[149]. Questi Stati hanno risorse limitate per monitorare e- se del caso - sanzionare efficacemente le grandi piattaforme e le differenze interpretative tra Paesi determinano una disomogeneità applicativa che mina l'efficacia complessiva del regolamento. L'Ungheria, la Slovacchia, la Repubblica Ceca e la Polonia hanno, ad esempio, elaborato strategie che riflettono le loro specifiche situazioni economiche, politiche e culturali, ma tutte condividono una preoccupazione per il mantenimento di spazi di autonomia decisionale nazionale all'interno del quadro europeo[150]. Senza dover guardare alle difficoltà di tali particolari Paesi, applicare il concetto di sovranità digitale all'Unione europea solleva anche la questione del se e come l'UE possa essere considerata essa stessa sovrana. Ad esempio, la Corte costituzionale tedesca nega l'esistenza di una sovranità dell'UE, sostenendo che essa rimane integralmente in capo agli Stati membri[151]. Si tratta dello storico problema Unionale della crisi di legittimazione dell'ordinamento sovranazionale[152].
Si pensi anche alla già menzionata iniziativa Gaia-X, la quale rappresenta un tentativo concreto di tradurre l'ambizione di sovranità tecnologica in un progetto tangibile[153]. Questo ecosistema di servizi cloud interoperabili e sicuri, operante secondo standard e valori europei, mirava – sia pure in maniera non del tutto esplicita e diretta – ad offrire un'alternativa ai servizi cloud dominati da fornitori non europei. L'importanza di Gaia-

[148] G. Hulko, J. Kalman e A. Lapsanszky, *The politics of digital soverignty and the European Union's legislation: navigating crises*, in *Frontiers in Political Science*, 7, 2025.
[149] *Ibid*.
[150] *Ibid*.
[151] Bundesverfassungsgericht [Corte costituzionale federale], 30 giugno 2009, 123 BVerfGE 267, 380 – 406.
[152] *Ex multis*, S. Dellavalle, *Il potere dell'Unione europea*, in *Teoria politica. Nuova Serie*, Annali VI, 2016, pp. 193-223 e G. De Burca, *The Quest for Legitimacy in the European Union*, in *The Modern Law Review*, 59:3, 1996, p. 349.
[153] Un'analisi del progetto Gaia-X è offerta da M. Dècina, A. Fuggetta e A. Perrucci, *L'industria del cloud e il ruolo dell'Italia nell'ambito del progetto Gaia-X*, Paper di Astrid, 77, 2021.

ISSN 2038-1662

X è non solo nel rafforzamento dell'indipendenza tecnologica, ma anche nel supporto all'innovazione e all'imprenditorialità europea. Il progetto ha, tuttavia, incontrato rilevanti difficoltà significative nel decollare, riflettendo la sfida di coordinare attori diversi con priorità e capacità differenti e di competere con ecosistemi tecnologici già consolidati, nonché l'irrisolta incapacità di limitare la dipendenza dai grandi cloud provider esterni[154].
La sfida per l'Unione Europea passa quindi per un consenso interno che deve essere sufficientemente solido da garantire un'implementazione efficace delle normative. È quanto richiede anche la già citata dichiarazione di Vienna, là dove si specifica che l'obiettivo della sovranità richiede un approccio europeo comune che rinforzi l'abilità di agire liberamente, ma sempre con apertura verso il mercato e i partner globali[155].
Le nuove "politiche abilitanti" devono quindi anche andare a compensare le lacune strutturali e di coordinamento di lunga data nella politica industriale dell'UE. Come ha recentemente sottolineato Mario Draghi, in un contesto geopolitico in evoluzione in cui tutte le grandi potenze stanno cercando di ridurre le dipendenze esterne e di riconquistare l'autonomia strategica, l'UE deve articolare una politica industriale coerente, coordinata a livello centrale e guidata strategicamente.
Sebbene gli Stati membri abbiano iniziato a adeguare le loro strategie con politiche industriali e strategiche più assertive, questi sforzi a livello dell'UE sono spesso scoordinati e frammentati, diluendo il loro impatto collettivo.[156] La sfida del coordinamento è duplice: (i) tra gli Stati membri: gli interventi a livello nazionale spesso portano a duplicazioni degli sforzi, standard divergenti e esternalità transfrontaliere trascurate, indebolendo l'efficacia dell'azione a livello europeo; e (ii) tra i diversi settori politici: nelle principali economie globali come gli Stati Uniti e la Cina, la politica industriale è sempre più multidimensionale e collega incentivi fiscali, applicazione delle norme commerciali e strumenti economici esteri in strategie nazionali integrate, mentre replicare questo approccio nel contesto dell'UE richiede un forte allineamento tra le priorità nazionali e la governance a livello dell'UE.

Il secondo profilo, non meno rilevante, riguarda il recentissimo approccio dell'UE incentrato sulla semplificazione, con un pacchetto legislativo di semplificazione che già viene descritto come un fattore di maggiore incertezza e complicazione[157]. È un percorso che vede già alla sua base la Bussola per la competitività (trattata nel paragrafo che precede), la quale prende le mosse dai rapporti Letta e Draghi e delinea

[154] A. Baur, *European ambitions captures by american clouds: digital sovereignty through Gaia-X*?, in Information, Communication & Society, 2025, pp. 1-18.
[155] Vienna
[156]Letta E. (2024) Much more than a market
[157] M. Macchia, *La funzione europea di regolazione*, cit. L'Autore richiama S. Cassese e una descrizione del comportamento dei regolatori che sembra ancora attuale: "prigionieri del circolo vizioso regolatorio, per cui più regolano, più rilevano scostamenti e deviazioni, più tornano a regolare controllare", in S. Cassese, *Regolazione e concorrenza*, in G. Tesauro, M. D'Alberti (a cura di), *Regolazione e concorrenza*, Bologna, 2000, p. 23.

ISSN 2038-1662

la necessità di ripensare il modello di competitività europea, là dove la semplificazione è intesa come un pilastro della nuova competitività europea, della sovranità, sicurezza economica e influenza globale dell'UE.
L'esempio più lampante di tale approccio è il crescente uso dell'"Omnibus" quale tecnica legislativa di semplificazione del panorama regolatorio e che non riguarda solo il tema del digitale. Si ritiene opportuno affrontare il tema in due dimensioni: la prima, focalizzata sull'omnibus come strumento legislativo; la seconda, sul caso specifico del digitale. Il fine è duplice: rappresentare il cambio di paradigma già menzionato e le criticità di come tale approccio di semplificazione è messo in atto.

L'omnibus si è trasformato da strumento occasionale in vera e propria tecnica legislativa per attuare rapidamente un'agenda de-regolatoria di ampia portata. Tale evoluzione solleva problemi costituzionali rilevanti, perché concentra riforme profonde in un unico pacchetto, accelera drasticamente i tempi decisionali e comprime passaggi fondamentali del processo legislativo, come le valutazioni d'impatto, le consultazioni pubbliche e l'analisi delle alternative. Dal punto di vista giuridico, l'omnibus non è illegittimo in sé, ma ogni atto dell'Unione deve rispettare il principio di proporzionalità, che impone che le misure siano adeguate agli obiettivi perseguiti, necessarie e fondate su un solido impianto fattuale[158]. La strada intrapresa sembra andare, per altro, contro la risoluzione del Parlamento europeo sulla sovranità digitale europea e l'infrastruttura digitale, là dove si sottolinea:

"*94. la necessità che le nuove proposte legislative siano* ***allineate ai principi del*** **better regulation***, garantendo che qualsiasi nuova misura di politica digitale che incida sulla competitività sia accompagnata da una valutazione d'impatto, comprensiva di una verifica sulla competitività, sulle PMI e sulle piccole imprese a media capitalizzazione, che valuti se un determinato strumento legislativo sia necessario e proporzionato e non crei oneri inutili per le imprese, in particolare per le PMI, e quindi i suoi effetti sulla competitività, sulle prospettive di investimento e sul benessere dei consumatori; 95. la semplificazione della legislazione dell'UE non deve mettere in pericolo alcuno dei diritti fondamentali dei cittadini e delle imprese, compromettendo così la certezza del diritto; ritiene* ***che qualsiasi proposta di semplificazione non debba essere affrettata né presentata senza un'adeguata valutazione, consultazione e analisi d'impatto***"[159].

L'uso attuale dell'omnibus mostra invece un modello ricorrente caratterizzato da carenza di evidenze empiriche, assenza di analisi comparative, consultazioni ristrette

[158] *Ibid*.
[159] Risoluzione del Parlamento europeo del 22 gennaio 2026 sulla sovranità tecnologica europea e sulle infrastrutture digitali Sovranità tecnologica europea e infrastrutture digitali P10_TA(2026)0022, 2025/2007(INI), enfasi aggiunta.

ISSN 2038-1662

soprattutto agli operatori economici e mancanza di una valutazione strutturata degli effetti. La giurisprudenza più recente ha, peraltro, richiesto alle istituzioni di dimostrare di aver realmente esercitato la propria discrezionalità sulla base di dati, valutazioni e comparazioni tra opzioni diverse[160].

Il crescente approccio deregolatorio rende difficile dimostrare che le misure adottate siano davvero necessarie o che non esistano soluzioni meno restrittive per raggiungere gli stessi obiettivi. La tecnica dell'omnibus produce inoltre un effetto di opacità: mescolando interventi tecnici con scelte politiche controverse, rende più difficile per il Parlamento, per la società civile e per l'opinione pubblica comprendere la reale portata dei cambiamenti e valutare singolarmente le diverse opzioni. Ne risulta un impoverimento del dibattito democratico, perché si è costretti ad accettare o respingere pacchetti indivisibili. Il rischio più ampio è quello di creare un precedente strutturale: invocare urgenza e competitività per aggirare le normali garanzie procedurali, trasformando l'eccezione in regola. Il crescente approccio rischia di minare tre pilastri del modello europeo: la legislazione basata su evidenze, la partecipazione democratica e la proporzionalità dell'azione pubblica[161]. La direzione scelta rischia di andare contro ai valori alla base della strategia Unionale e la semplificazione non può tradursi – nel percorso di ricerca della propria indipendenza - in scorciatoia procedurale: efficienza e garanzie costituzionali non sono alternative, ma condizioni complementari di una buona legislazione.

Box 2. Le criticità della proposta OMNIBUS per l'IA

La proposta di regolamento Omnibus per l'IA[162] presenta diverse criticità, riconducibili a un approccio orientato al mero alleggerimento degli oneri di *compliance* piuttosto che al miglioramento strutturale della competitività[163]. Una delle criticità più evidenti è il rinvio dell'applicazione delle norme sui sistemi ad alto rischio: l'Omnibus posticipa l'entrata in vigore delle relative disposizioni, subordinandola a una decisione della Commissione sulla disponibilità di misure di supporto alla conformità, con scadenze massime fissate al 2 dicembre 2027 (Allegato III) e al 2 agosto 2028 (Allegato I). La giustificazione addotta — ritardi nella designazione delle autorità nazionali, mancanza di standard armonizzati e di strumenti di conformità — non ha evitato le preoccupazioni dell'EDPB e dell'EDPS circa l'impatto sulla protezione dei diritti fondamentali[164]. A ciò si

[160] Corte di Giustizia UE, *Repubblica Ceca v Parlamento e Consiglio*, C-482/17, EU:C:2019:1035, dicembre 2019.
[161] *Ibid*.
[162] COM/2025/836 final.
[163] Federation of European Data and Marketing, *Position paper on Digital & AI Omnibus Proposal*, 4 febbraio 2026.
[164] EDPB-EDPS Joint opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).

ISSN 2038-1662

aggiunge l'ampliamento della clausola di *grandfathering* (art. 111, par. 2, AI Act), che allunga il periodo in cui sistemi potenzialmente problematici, già immessi sul mercato, possono operare al di fuori del nuovo quadro regolatorio, a meno di modifiche significative nella progettazione[165].
L'eliminazione dell'obbligo di registrazione per determinati sistemi IA solleva ulteriori preoccupazioni in termini di trasparenza e *accountability*, rischiando di creare asimmetrie informative a danno di consumatori e operatori in buona fede[166]. Sul piano del trattamento dei dati, la proposta introduce un nuovo art. 4a che estende la possibilità di trattare categorie particolari di dati personali — originariamente limitata ai fornitori di sistemi ad alto rischio (art. 10, par. 5, AI Act) — a tutti i sistemi e modelli IA e anche ai *deployer*[167]. Inoltre, il testo introduce un approccio soggettivo alla definizione di "dati personali", stabilendo che le informazioni non sono considerate tali qualora l'entità non possa ragionevolmente identificare la persona, e attribuisce alla Commissione il potere di definire tramite atti di esecuzione cosa non costituisce dato personale, con il rischio di escludere interi settori dall'ambito del GDPR[168].
Lette congiuntamente, le modifiche rivelano uno spostamento strutturale più profondo: da un modello centrato sui diritti e sulla governance a uno *pro-industria*. Il restringimento delle regole di accesso nell'interesse pubblico, l'ampliamento dei motivi per rifiutare la condivisione dei dati e le esenzioni dagli obblighi di *cloud switching* segnalano una prioritizzazione della politica industriale rispetto ai diritti fondamentali. Privilegiando il controllo dei risultati invece di investire nei fattori strutturali della competitività — capitale, potenza di calcolo, dati di qualità e competenze — l'Unione europea rischia di compromettere la propria "sovranità cognitiva", favorendo l'adozione acritica di tecnologie sviluppate altrove, con effetti profondi su cultura, immaginario collettivo e processi democratici[169]. Modificare le norme a ridosso della loro applicazione mina inoltre la certezza del diritto e le aspettative legittime degli operatori; l'uso di procedure rapide senza adeguata consultazione pubblica solleva dubbi sulla trasparenza democratica, come evidenziato anche dall'Ombudsman europeo[170].
Lo studio del Parlamento europeo sul pacchetto Digital Omnibus conferma queste preoccupazioni, concentrandosi sulla capacità della semplificazione di

[165] *Ibid.*
[166] N. Rangone, *The Paradoxes of the European Union's AI Regulation*, in *The Regulatory Review*, in corso di pubblicazione.
[167] *Ibid.*
[168] B. Lazarotto, *The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite*, in *MediaLaws*, 19 dicembre 2025.
[169] N. Rangone, *The Paradoxes of the European Union's AI Regulation*, *cit.*
[170] Si veda https://www.ombudsman.europa.eu/en/press-release/it/215989.

ISSN 2038-1662

migliorare effettivamente l'usabilità senza indebolire la protezione uniforme, l'applicabilità e la certezza del diritto. Lo studio osserva che diverse modifiche possono ridurre l'eccesso di conformità in alcuni ambiti, ma potrebbero anche generare maggiore incertezza giuridica e controversie interpretative[171]. In particolare, l'approccio condizionale ai tempi di applicazione delle norme sull'IA ad alto rischio — che subordina l'entrata in vigore alla disponibilità di standard armonizzati e linee guida — introduce una dinamica di "stop-and-start" che complica la pianificazione degli investimenti per le imprese e crea incertezza per i regolatori su quando e come intensificare l'attività di *enforcement*. Sul piano dei dati sensibili, l'ampliamento delle condizioni per il trattamento di categorie particolari di dati personali a fini di rilevazione e correzione dei *bias* — esteso dai soli sistemi ad alto rischio a tutti i sistemi e modelli IA — rischia di sfumare il confine tra test di equità e addestramento, creando incertezza sulla base giuridica e sulle garanzie applicabili quando sono coinvolti dati sensibili. L'analisi rileva anche che la trasformazione dell'obbligo di *AI literacy* da vincolante a incoraggiato rappresenta un indebolimento sostanziale dell'architettura di governance dell'AI Act, privando lavoratori e rappresentanti di una chiara base giuridica per esigere formazione e sviluppo di competenze dai datori di lavoro.

In sede parlamentare, il dibattito si sta orientando verso la fissazione di scadenze certe per le norme sull'IA ad alto rischio (2 dicembre 2027 per i sistemi di cui all'Allegato III e 2 agosto 2028 per quelli dell'Allegato I), il ripristino dell'obbligo di registrazione nella banca dati UE e l'introduzione dello standard di "stretta necessità" per il trattamento di categorie particolari di dati personali, come proposto dal testo di compromesso della Presidenza cipriota del Consiglio[172]. Le reazioni degli stakeholder restano tuttavia profondamente divise: se i gruppi industriali accolgono favorevolmente il pacchetto come passo necessario per la competitività, le organizzazioni della società civile e i sindacati lo qualificano come il più significativo arretramento dei diritti digitali nella storia dell'UE, mentre l'EDPB e l'EDPS, pur sostenendo l'obiettivo generale, chiedono limiti rigorosi al trattamento dei dati sensibili e si oppongono all'eliminazione degli obblighi di registrazione e alle modifiche alla literacy sull'IA.

Infine, l'efficacia dell'AI Act dipenderà in larga misura dall'attuazione negli Stati membri. La regolamentazione si svolge in un contesto complesso, dove le regole europee devono essere applicate dai singoli Paesi, con il rischio di *gold-plating* (regole nazionali più rigide che innalzano i costi di *compliance*),

[171] G. Skiotytė, A. Sadauskaitė, *A Digital Omnibus: Identifying Interlinks and Possible Overlaps Between Different Legal Acts in the Field of Digital Legislation to Streamline Tech Rules*, European Parliament, Policy Department for Economy and Growth, PE 772.641, febbraio 2026.

[172] M. Niestadt, *Digital Omnibus on AI*, EPRS, European Parliamentary Research Service, PE 782.651, febbraio 2026.

ISSN 2038-1662

divergenze interpretative che frammentano il mercato unico e frammentazione istituzionale, con Paesi che hanno scelto autorità di controllo eterogenee per mandato e grado di indipendenza, il che può portare a interpretazioni diverse della stessa legge, come già accaduto con il GDPR[173].

Quanto sopra delineato sembra, peraltro, andare contro all'obiettivo di rafforzare l'innovazione europea e la competitività attraverso un quadro normativo chiaro, prevedibile e favorevole agli investimenti, come riportato nella recente Dichiarazione per la sovranità digitale europea[174]. La dichiarazione si focalizza, peraltro, anche sull'importanza di un panorama regolatorio chiaro, prevedibile ed equo[175] – descrizione che sembra non in linea con il corrente approccio.

Il quadro appare dunque incerto anche da un punto di vista dell'approccio dell'UE e della protezione dei valori fondanti l'Unione, ma si può ancora affermare che la lettura del concetto di sovranità interessa l'intera catena di approvvigionamento dell'IA, dai dati all'hardware e al software[176]. Tale impostazione si scontra però con una realtà difficile: come si è visto nel par. 1, permane una forte dipendenza da imprese informatiche con sede fuori dall'Unione. Questo limita la leadership e l'autonomia strategica dell'UE nel mondo digitale e, di conseguenza, ne frena il potenziale di crescita economica[177]. Su quali aspetti dovrebbe dunque concentrarsi l'UE?

[173] Si veda https://digital-strategy.ec.europa.eu/it/policies/market-surveillance-authorities-under-ai-act.
[174] Dichiarazione per la sovranità digitale europea, 17 novembre 2025, TELECOM 425, accessibile qui: https://data.consilium.europa.eu/doc/document/ST-15781-2025-INIT/en/pdf.
[175] *Ibid*.
[176] B. C. Larsen, *The Geopolitics of AI and the Rise of Digital Sovereignty*, Brookings, 8 dicembre 2022.
[177] Opinion of the European Economic and Social Committee on Digital Sovereignty: a crucial pillar for EU's digitalisation and growth 2023 (2023/C 75/02).

ISSN 2038-1662

7. Quali azioni per la sovranità digitale? Alcune prime considerazioni

L'analisi svolta consente alcune prime conclusioni.

Al di là di una situazione complessiva di difficoltà dell'industria UE a competere con Stati Uniti e Cina nei mercati dell'ecosistema digitale (a livello di specifici settori/mercati, con ritardi di competitività che in taluni casi appaiono difficilmente colmabili), vi sono situazioni in cui la performance del *Made in EU* è decisamente migliore (*High Performance Computing*) o comunque positiva (alcuni segmenti dell'industria dello spazio e dei cavi sottomarini).

Il contesto della divisione internazionale del lavoro nei mercati digitali resta – in ogni caso – segnato dalla presenza di oligopoli, sia sul versante occidentale, con la indiscutibile leadership delle Big Tech USA, sia nell'emisfero asiatico, dove dominano aziende di stato cinesi e alcune multinazionali coreane o taiwanesi.

L'UE sta reagendo – finalmente con un approccio a più ampio spettro - a questa situazione di difficoltà, aumentando sia il numero di settori digitali che di strumenti con cui intervenire a sostegno delle produzioni europee, agendo tanto sul fronte della ricerca, quanto su quello della promozione di campioni europei, start up, scale up[178]. In tal senso, bisognerà seguire l'evoluzione di alcuni (menzionati) programmi a sostegno della R&S e degli investimenti, nonché di iniziative legislative in corso, quali l'Industrial Acceleration Act, il Digital Networks Act e la revisione del Cybersecurity Act.

Purtroppo, fino ad ora, gli interventi a sostegno della competitività delle industrie europee sono spesso frammentari, di modeste dimensioni economiche/finanziarie, non sempre coordinati, e talora sovrapponibili alle iniziative su scala nazionale (si pensi al cloud o ai large language models). In estrema sintesi, pochi programmi hanno prodotto risultati importanti, quale ad esempio è stato il caso dei progetti per il supercalcolo.

Inoltre, dopo la fase in cui l'UE ha affiancato alle politiche per la promozione e tutela della concorrenza e dell'utente una impostazione a sostegno della competitività, e quindi avviato programmi di R&S e di promozione degli investimenti, stiamo vivendo una ulteriore evoluzione, in cui, accanto a questi obiettivi, se ne pongono altri legati ai

[178] In realtà, la politica dell'UE in materia di digitale ha una storia pluridecennale di iniziative: non solo con riguardo ai profili regolamentari, che pure rimangono terreno d'elezione dell'intervento unionale, ma anche per quanto riguarda le misure a sostegno della competitività dell'industria europea. L'Agenda digitale europea è del 2010, ma già nei primi anni di questo secolo l'UE si preoccupava delle sfide competitive poste dalla (nuova) società dell'informazione. Tuttavia, le azioni intraprese sono spesso risultate inefficaci per risolvere il gap di competitività del Made in Europe, per i motivi che verranno richiamati.

ISSN 2038-1662

temi della difesa e della sicurezza, per tenere conto della dimensione geopolitica che sempre più stanno assumendo tecnologie e mercati digitali.

Da questo scenario, derivano alcune considerazioni in merito all'impostazione di una rinnovata strategia UE per i mercati digitali, a partire dalle iniziative già in essere e dalle iniziative legislative in corso.

Sul versante regolamentare, bisogna innanzitutto tenere conto della particolarità della regolazione del digitale, che ha limitate affinità con la regolazione – tipicamente simmetrica - delle industrie a rete (utilities) caratterizzate – in Europa - dal monopolio dello Stato (TLC, energia, trasporti). Nei mercati digitali, non siamo in presenza di settori da ricondurre ad assetti concorrenziali, ma, rispetto al mondo delle utilities in cui il fattore scarso è rappresentato dall'accesso alla infrastruttura, in questi casi gli asset strategici riguardano l'accesso ad altri fattori produttivi: capitali, talenti, dati, tecnologie (ed alla capacità di combinarli tra loro). Ne deriva la necessità di un nuovo paradigma che, al momento, è quello delineato nel Digital Markets Act (DMA), che – correttamente a nostro avviso – riprende una impostazione asimmetrica, individuando alcuni soggetti (gatekeepers) cui imporre obblighi e divieti ex ante[179].

Inoltre, la semplificazione della normativa in materia di digitale, invero assai articolata e complessa, è senz'altro un percorso da affiancare agli interventi di politica industriale per il digitale, al fine di accrescerne l'efficacia e non ostacolarne lo sviluppo. Tuttavia, bisogna fare attenzione a che la tecnica legislativa utilizzata – l'Omnibus – sia coerente con requisiti alla base della legislazione unionale: proporzionalità, adeguata valutazione, consultazione, analisi d'impatto, *better regulation*.

Sul versante industriale, per quanto sia difficile, è importante promuovere un approccio di ecosistema, ad evitare di dover poi razionalizzare le diverse misure specifiche per singole tecnologie/produzioni. L'invito del Parlamento europeo va in questa direzione, anche se la velocità del cambiamento tecnologico (e di mercato) non consente di procedere in sequenza (analisi e poi intervento), per cui occorre agire in parallelo: continuare l'analisi, senza fermare le iniziative in essere o previste, ma con un continuo monitoraggio e valutazione di queste ultime, alla luce dei risultati conseguiti e dell'analisi svolta.

[179] L'efficacia del DMA verrà valutata nel corso della sua applicazione, dal momento che siamo ancora ad alcuni primi interventi nei confronti delle grandi piattaforme digitali. Intanto, però, è chiaro che, accanto ad un nuovo paradigma regolamentare per i mercati digitali, necessita quella politica industriale di sistema, cui si è fatto cenno prima.

ISSN 2038-1662

In secondo luogo, è necessario accrescere ulteriormente la dimensione unionale dei programmi di intervento, dando una concreta declinazione al concetto di sovranità digitale europea, e contrastando quindi la tentazione alle vie nazionali al digitale, che pure alcuni stati membri continuano a perseguire.

Un orientamento strategico verso la sovranità digitale dovrebbe tradursi in interventi strutturali, ma allo stesso tempo non può focalizzarsi realisticamente su tutti i layer della catena del valore digitale. Occorre concretizzare una reale capacità europea di innovare, gestire e controllare i livelli più critici e permettere, per gli ambiti su cui si è meno avanzati, di poter comunque operare al di fuori delle influenze esterne. In altri termini, per alcuni dei settori/mercati della filiera digitale, l'industria europea può rafforzare la propria capacità di competere a livello internazionale, mentre – per altri settori/mercati – la via più razionale sembra quella di agire dal lato della domanda (pubblica, in primo luogo), differenziando le fonti di approvvigionamento, ad evitare – per quanto possibile – situazioni di lock in[180].

In questa prospettiva, i sistemi di intelligenza artificiale addestrati su dati e domini specifici (la c.d. "vertical AI") rappresentano un ambito in cui l'Europa può capitalizzare sui propri punti di forza: l'eccellenza in settori ad alta intensità di conoscenza come il manifatturiero avanzato, la sanità, la finanza e l'agricoltura di precisione[181]. Questa logica di specializzazione settoriale consente all'Europa di competere non sulla scala di calcolo dei modelli o sul volume di dati utilizzati, ambiti in cui gli Stati Uniti e la Cina mantengono vantaggi significativi, ma sulla precisione, l'affidabilità e la conformità normativa di sistemi di intelligenza artificiale progettati per contesti ad alta complessità e regolamentazione stringente.

Inoltre, nell'ecosistema digitale, un ruolo cruciale è assunto dall'edge computing, da identificare come tecnologia abilitante per applicazioni ad alta intensità di dati come

[180] In tale direzione, si segnala il paper del Tony Blair Institute for Global Change "Sovereignty in the Age of AI: Strategic Choises, Structural Dependencies and the Long Game Ahead, 2026.

[181] Iniziative come il progetto OpenEuroLLM, che mira a sviluppare modelli linguistici open source multilingue specificamente orientati ad applicazioni verticali (finanza, sanità, telecomunicazioni), dimostrano questa consapevolezza, anche se le risorse assegnate sono davvero ridotte. Il programma AI Matters, una delle quattro Testing and Experimentation Facilities europee, offre alle imprese manifatturiere l'accesso a servizi altamente sovvenzionati (fino al 100% per le micro e piccole imprese) per testare e validare soluzioni di intelligenza artificiale settoriali in condizioni operative reali, focalizzandosi su ottimizzazione produttiva, interazione uomo-robot ed economia circolare. La strategia della Data Union, pubblicata nel novembre 2025, enfatizza proprio la necessità di dataset multilingue settoriali di alta qualità come condizione essenziale per l'innovazione nell'ecosistema europeo dell'intelligenza artificiale generativa, proponendo il potenziamento degli spazi comuni europei di dati settoriali e la creazione di "Data Labs" per connettere gli spazi dati con gli sviluppatori di intelligenza artificiale.

ISSN 2038-1662

l'Internet of Things industriale, la guida autonoma, la sanità digitale e l'agricoltura intelligente. L'edge computing rappresenta per l'Europa un'opportunità di riposizionamento strategico: mentre la competizione nel cloud computing centralizzato vede una concentrazione di mercato elevatissima, l'elaborazione distribuita ai margini della rete permette alle imprese europee di presidiare nodi critici senza necessariamente replicare l'intero stack tecnologico dei grandi fornitori. In tale contesto, sarà cruciale la fase di implementazione del *Cloud and AI Development Act*.

Un'ulteriore direttrice della politica digitale UE riguarda lo sviluppo di standard aperti, tecnologie interoperabili e comunità open source, che consentono di ridurre/superare la dipendenza da fornitori proprietari e di rendere verificabili e modificabili i componenti fondamentali del software europeo. Questo approccio non solo rafforza la sicurezza dei sistemi, ma stimola anche innovazione e competitività su scala globale, facendo leva sulle competenze locali e su modelli tecnologici trasparenti.

Infine, non può mancare un focus sulle competenze: la costruzione di una effettiva sovranità digitale passa anche attraverso programmi di formazione avanzata, scuole specialistiche e centri di eccellenza, per colmare il gap di talenti e sviluppare un ecosistema europeo capace di sostenere la propria evoluzione tecnologica.

In conclusione, la strategia industriale europea per il digitale non può fondarsi sulla ricerca di una autosufficienza tecnologica integrale, obiettivo irrealistico e controproducente, ma nella capacità di selezionare i settori/mercati digitali per cui promuovere il made in Europe, attraverso programmi di R&S ed industriali, riducendo al contempo il grado di dipendenza da singoli fornitori in quei settori/mercati digitali dove il ritardo rispetto alle imprese USA e cinesi non appare recuperabile nel breve-medio periodo.

ISSN 2038-1662