

ASTRID FORUM

Rivista Quadrimestrale
di Studi e Ricerche



n.1

Maggio 2026

ISSN: 0000-0000

SOMMARIO

La riforma del governo della politica fiscale in Europa.....	3
<i>di M. Bordignon e G. Pisauro</i>	
A compact for European debt sustainability	49
<i>di P. C. Padoan</i>	
Safe asset europei: contesto macroeconomico, strumenti e prospettive	75
<i>di P. Benigno e E. Reviglio</i>	
Dal coordinamento globale all'imposta europea sulle imprese	103
<i>di V. Ceriani</i>	
Le politiche pubbliche UE per il digitale	147
<i>di A. Manganelli, L. Megale e A. Perrucci</i>	
The transformation of European trade policy in the new global disorder: instruments, objectives and challenges.....	189
<i>di P. Guerrieri</i>	
Environmental sustainability and industrial policy: key items on the European agenda.....	215
<i>di C. De Vincenti</i>	
La difesa dell'Europa	235
<i>di S. Silvestri</i>	
La proposta di riforma elettorale del centrodestra sul finire della XIX legislatura tra rappresentanza territoriale, uguaglianza del voto e forma di governo parlamentare	263
<i>di L. Spadacini</i>	
L'astensionismo involontario: definizioni, caratteristiche, rimedi	289
<i>di P. Feltrin</i>	

Rivista scientifica di studi e ricerche di natura interdisciplinare. Pubblicazione in formato digitale della Fondazione Astrid-ETS

Rivista iscritta in data 14 maggio 2026 al n. 53/2026 del Registro Stampa del Tribunale di Roma

In attesa di ISSN

Numero 1 – Anno 2026

I contributi di questa Rivista sono sottoposti alla valutazione di un revisore in forma anonima (*double blind peer review*), salvo casi opportunamente segnalati in nota.

La Rivista si conforma alle linee guida stabilite dalla *Committee on Publication Ethics* (COPE), nel rispetto del Codice etico consultabile in: <https://www.astrid-online.it/static/upload/codi/codice-etico-astrid-forum.pdf>.

Ogni riflessione e ogni suggerimento sono i benvenuti, nello spirito di una comunità scientifica aperta e partecipata. Per ogni informazione in merito all'invio dei contributi è possibile contattare la Rivista all'indirizzo: redazione.astridforum@astrid-online.it

Direttore responsabile

Stefano Menichini

Direttore scientifico

Franco Bassanini

Comitato di direzione:

Giuseppe Coco, Vincenzo Cerulli Irelli, Giovanna De Minico, Claudio De Vincenti, Filippo Donati, Anna Genovese, Giuseppe Italiano, Amedeo Lepore, Antonio Manganelli, Antonio Perrucci, Cesare Pinelli, Nicoletta Rangone, Aldo Sandulli, Lorenzo Spadacini, Luisa Torchia, Giuseppe Travaglini, Claudia Tubertini, Alberto Zanardi

Comitato scientifico:

Giuliano Amato, Gregorio Arena, Enzo Balboni, Stefania Bariatti, Massimo Bordignon, Marco Buti, Marco Cammelli, Carlo Cambini, Mimmo Carrieri, Vincenzo Cerulli Irelli, Enzo Cheli, Giuseppe Coco, Paolo Costa, Marco D'Alberti, Gianfranco D'Alessio, Gaetano D'Auria, Gian Candido De Martin, Maurizio Dècina, Paolo Feltrin, Alfonso Fuggetta, Franco Gallo, Piero Giarda, Giuseppe Italiano, Marco Leonardi, Mario Libertini, Massimo Luciani, Alfredo Macchiati, Andrea Manzella, Oreste Massari, Bernardo Giorgio Mattarella, Mario Rosario Mazzola, Francesco Merloni, Marcello Messori, Giulio Napolitano, Alessandro Natalini, Fabrizio Onida, Pier Carlo Padoan, Alessandro Pajno, Stefano Passigli, Cesare Pinelli, Giuseppe Pisauro, Franco Pizzetti, Alberto Quadrio Curzio, Pippo Ranci, Cesare Salvi, Domenico Sorace, Gian Luigi Tosato, Tiziano Treu, Adriana Vigneri, Massimo Villone

Capo della Redazione

Lorenzo Spadacini

Comitato di redazione

Alessandro Augurio, Marzia Gandiglio, Luca Megale, Gordon A. Mensah, Alessandra Miraglia, Loredana Parpaglion, Andrea Ramazzotti, Lorenzo Spadacini



A S T R I D

Ente di ricerca del Terzo Settore

Corso Vittorio Emanuele II, 00186 Roma – tel. 39066810261 – redazione.astridforum@astrid-online.it – www.astrid.eu

Roma, Maggio 2026

Le politiche pubbliche UE per il digitale

A. Manganelli*, L. Megale** e A. Perrucci***

ABSTRACT (IN ITALIANO): *Il contributo illustra il percorso regolamentare avviato dall'Unione europea per governare la trasformazione digitale, combinando regolazione settoriale e normativa orizzontale. L'analisi esamina lo stato dell'industria digitale europea, le dipendenze tecnologiche da operatori extra-UE e le politiche pubbliche adottate, dal Digital Markets Act all'AI Act. Il lavoro evidenzia la necessità di integrare regolazione e politica industriale per rafforzare la sovranità digitale europea.*

TITOLO IN INGLESE: *EUROPEAN PUBLIC POLICIES FOR THE DIGITAL SECTOR*

ABSTRACT (IN INGLESE): *This paper examines the regulatory path undertaken by the European Union to govern digital transformation, combining sectoral regulation with horizontal legislation. The analysis reviews the state of Europe's digital industry, technological dependencies on non-EU operators, and adopted public policies from the Digital Markets Act to the AI Act. The work highlights the need to integrate regulation and industrial policy to strengthen European digital sovereignty.*

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 Bresnahan e Trajtenberg, trent'anni fa¹.

Di conseguenza, alla tradizionale regolazione settoriale dei mercati primariamente interessati dalla trasformazione digitale (comunicazioni elettroniche, audiovisivo, servizi postali), l'UE ha progressivamente affiancato una serie di regolamenti – di

* *Professore straordinario presso l'Università di Siena e Research fellow presso il Centre on Regulation in Europe (CERRE).*

** *Assegnista di ricerca in Diritto amministrativo, Università LUMSA di Roma.*

*** *Direttore del Laboratorio sull'ecosistema digitale della Fondazione Astrid.*

¹ T.F. Bresnahan e M. Trajtenberg, *General Purpose Technologies “Engines of Growth”?*, in *Journal of Econometrics*, 65, 1995, pp. 83-108. In sintesi, si tratta di tecnologie applicabili ai più vari settori e contesti, in continua evoluzione e in grado di dar luogo a complementarità nell'innovazione e, quindi, di favorire l'innovazione anche nei settori che la utilizzano.

carattere orizzontale – che riguardano i servizi digitali, l’intelligenza artificiale e i *big data*².

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. Viene delineato lo stato dell’industria europea, con specifico riferimento ad alcuni settori dell’ecosistema digitale (par. 2). Successivamente, si ricostruisce il quadro normativo e di *policy* europeo sul digitale (par. 3), articolato in otto *cluster* tematici. Si analizza quindi il passaggio dalla regolazione alla politica industriale (par. 4), evidenziando i limiti strutturali dell’approccio regolatorio nel promuovere capacità produttive e scala competitiva. Si approfondisce poi l’evoluzione della politica industriale verso gli obiettivi di “sovrani  digitale” e “autonomia strategica”, distinguendo tra misure abilitanti e misure restrittive (par. 5), arrivando ad esaminare alcune criticit  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* (par. 6). In conclusione, si formulano alcune prime considerazioni sulle azioni necessarie a rafforzare la sovranit  digitale europea (par. 7).

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

2.1 Le analisi sulla competizione internazionale nei mercati digitali: limiti e differenze

Le analisi sullo stato dell’industria digitale europea sono ormai numerose, sia di fonte istituzionale (Unione europea³, Rapporto Draghi⁴, Rapporto Letta⁵), sia svolte da centri studi, societ  di consulenza ed esperti.

Nel novero di queste analisi,   importante una distinzione di carattere metodologico, per i riflessi che pu  avere sull’impostazione delle politiche per il digitale europeo (e italiano). Accanto a un numero – limitato – di studi che considerano pi  settori tra quelli che compongono l’ecosistema digitale⁶, si registrano numerose indagini che si

² Ci si riferisce, in particolare, al *Data Act* e al *Data Governance Act*, al *Digital Markets Act*, al *Digital Services Act* e al pi  recente *Artificial Intelligence Act*.

³ Si veda il successivo paragrafo per la ricostruzione del percorso dell’Unione europea volto a definire una strategia digitale. In questo contesto, particolare rilievo 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 produttivit  rispetto ad altre economie globali.

⁴ M. Draghi, *The future of European competitiveness*, settembre 2024.

⁵ E. Letta, *Much more than a market*, aprile 2024.

⁶ 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

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. Per questo motivo, risultano solo in parte utili all'impostazione di una strategia di politica industriale per il digitale che abbia una visione di (eco)sistema⁷, superando quindi l'approccio fondamentalmente settoriale che ha caratterizzato fino ad ora l'iniziativa dell'UE.

Tuttavia, qualcosa sta accadendo. Un tentativo interessante di fornire una visione d'insieme dell'economia digitale europea è quello di *Eurostack*, una iniziativa di soggetti privati⁸ 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»⁹. Parallelamente, le iniziative di *policy* più recenti della Commissione, descritte nel prossimo paragrafo, sembrano essere caratterizzate da una più estesa visione di insieme, almeno negli intenti di promuovere una maggiore “competitività” dell'industria europea.

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.

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 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).

⁷ 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*, p. 12.

⁸ 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.

⁹ Citazione (traduzione propria) dal sito Eurostack.eu.

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

Dell'ecosistema digitale fanno parte sia i mercati delle infrastrutture fisiche, sia 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 delle infrastrutture per il *cloud* e l'*edge computing*, i *data center*, dei *microchip*, dei supercalcolatori. Nel secondo caso, assumono importanza le industrie dei software per diversi settori verticali (ad esempio, per le reti di TLC), dei protocolli (le API, *application programming interfaces*), della *cybersecurity*, dei motori di ricerca, dei modelli e delle applicazioni di intelligenza artificiale (sia "tradizionale" che generativa – i *large language model* – e agentica), nonché le varie applicazioni delle piattaforme, sia per la trasmissione di contenuti audiovisivi, sia per le comunicazioni interpersonali.

Premesso che – in generale – la dipendenza dell'economia UE da beni e servizi e infrastrutture digitali, si colloca oltre l'80%, come indicano recenti documenti di *policy* dell'UE¹⁰, l'analisi dei mercati digitali non può che prendere il via da quei mercati e servizi che, singolarmente e nel loro complesso, risultano soggetti al predominio economico e informativo di un gruppo di poche piattaforme digitali di dimensioni globali, i cosiddetti GAFAM (Google, Amazon, Meta, Apple, Microsoft)¹¹. Questi mercati sono quelli in prima istanza individuati dal *Digital Markets Act* (DMA)¹², definiti come servizi di piattaforma di base (*core platform services*)¹³, in cui rendimenti

¹⁰ 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.

¹¹ 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 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.

¹² 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.

¹³ Si tratta dei servizi digitali maggiormente usati da utenti commerciali e 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.,

di scala crescenti, economie di varietà, esternalità di rete indirette e dirette hanno determinato un progressivo aumento del livello di concentrazione e una “cattura”/dipendenza informativa degli utenti. Il punto di partenza della regolazione introdotto dal DMA è, infatti, che un numero limitato di grandissime piattaforme online sono diventate *gatekeepers*, ossia controllori di accesso ai mercati digitali per migliaia di piccole imprese: un vero e proprio punto di ingresso per raggiungere centinaia di milioni di consumatori nel mercato unico europeo¹⁴.

Di fatto, poi, le *Big Tech* hanno espanso, oltre la scala, sempre più la varietà delle loro attività: una strategia di mercato denominata *platform envelopment* (inviluppo), realizzata attraverso una continua espansione di servizi, forniti in mercati distinti, anche sviluppando alcune delle infrastrutture digitali necessarie a livello globale (ad esempio, i cavi sottomarini), divenendo così orchestratori di interi ecosistemi digitali. È questo contesto di concentrazione del potere di mercato da parte di un ristretto nucleo di grandi piattaforme digitali che caratterizza ormai le dinamiche economiche e industriali dell’ecosistema digitale.

Di seguito, si forniscono alcuni dati relativamente al posizionamento dell’industria UE per una selezione¹⁵ di mercati dell’ecosistema digitale, per cui sono possibili comparazioni internazionali, sulla base di dati pubblicamente disponibili¹⁶. Dall’ampio novero di industrie prima indicate, sono stati selezionati sei settori, per i quali l’UE ha definito – o sta ridefinendo – una strategia di politica industriale: a) il *cloud*; ii) i

messaggistica online), f) sistemi operativi, g) *browser web*, h) assistenti virtuali, i) servizi di *cloud computing* e l) servizi di pubblicità online.

¹⁴ Fra i molti, si veda F. Chirico e A. Manganelli, *Mercati e Servizi Digitali*, in *Economia e diritto della Regolazione. Reti, piattaforme e servizi di pubblica utilità*, a cura di C. Cambini, A. Manganelli, G. Napolitano e A. Nicita, *Economia e diritto della Regolazione. Reti, piattaforme e servizi di pubblica utilità*, Bologna, Il Mulino, 2024; A. Manganelli e A. Nicita, *Regulating Digital Markets. The EU Approach*, Londra, Palgrave MacMillan, 2022.

¹⁵ La selezione operata riguarda mercati digitali, prevalentemente di natura industriale, per i quali la Fondazione Astrid ha acquisito, nel corso del tempo, una maggiore conoscenza, attraverso l’operato del Laboratorio sull’Ecosistema Digitale e, più di recente, dell’Osservatorio sulle dinamiche dell’intelligenza artificiale.

¹⁶ Un’analisi della collocazione dell’industria europea nell’ecosistema digitale a livello internazionale, mediante una accurata ricognizione dei dati resi disponibili da diverse fonti, costituisce un impegno straordinario, che va ben al di là delle finalità di questo contributo. Non a caso, il Parlamento europeo – nella risoluzione adottata il 22 gennaio scorso – ha richiesto “*the development of a comprehensive risk assessment framework to monitor and address dependencies across the digital value chain*”. Cfr. *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).

microchip; iii) i supercalcolatori; iv) le reti satellitari; v) i cavi sottomarini; vi) l'intelligenza artificiale, e 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 situazione, la UE sta promuovendo un'infrastruttura *cloud* sovrana, sicura e indipendente dai colossi tecnologici statunitensi (vedi oltre).

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 3/4 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 – NVIDIA¹⁸, AMD, Qualcomm, Broadcom e Intel. La fase di fabbricazione (*foundry*) resta invece sostanziale 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

¹⁷ Per l'Italia, si segnalano TIM Enterprise (in collaborazione con Google e Amazon) e Aruba.

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.

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 produttiva¹⁹. 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 e anche il Giappone 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 ($R_{max} \approx 6,96 \times 10^9$ GFlops), seguiti dalla Cina, con una base più contenuta (40 sistemi; 8%) e un contributo prestazionale complessivo inferiore ($R_{max} \approx 2,05 \times 10^8$ 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 R_{max} pari a $1,4 \times 10^9$ GFlops, seguita da Francia (23 sistemi) e Italia (18 sistemi). Se poi si passa alla 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 livello²⁰. In conclusione, nell'industria del supercalcolo (HPC), l'UE è ben posizionata, grazie alle iniziative comunitarie (vari programmi, come illustrato oltre) e degli investimenti pubblici e privati.

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

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.

²⁰ 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).

a due terzi dei satelliti operativi a livello globale²¹ (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, dal canto suo, 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 satellitare²². L'Unione europea 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 OneWeb/Eutelsat, una costellazione da 648 satelliti per broadband professionale (marittimo, aeronautico, dedicato ai 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'UE²³. 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.

²¹ 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.

²² Si veda il programma nazionale "*Guowang*", che prevede fino a qualche decina di migliaia di satelliti da mandare in orbita.

²³ 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.

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 e 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 e 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 mercati²⁴. Quindi, nello specifico segmento dei cavi elettrici, i paesi dell’UE sembrano ancora competitivi. Sul versante dei cavi per i settori TLC e 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 mediterranei²⁵. 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

²⁴ 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.

²⁵ In questo contesto, BlueMed (Italia-Francia-Grecia e *hub* nel 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*.

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 e, comunque, sta ridefinendo (vedi oltre) 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 mercato di massa. 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 delle imprese statunitensi: 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 Almax 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 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 paragrafo 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'Unione²⁶. Si parla, a tal riguardo, di crisi della sovranità popolare²⁷ e, almeno dal 2013, di obiettivo di “autonomia strategica” dell'Unione²⁸.

Già nel quadro della strategia di Lisbona del 2000, il Consiglio europeo aveva fissato l'obiettivo di trasformare l'UE in un'economia basata sulla conoscenza più competitiva e dinamica del mondo²⁹. 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 eEurope³⁰ e la strategia i2010³¹. Le politiche digitali sono state successivamente integrate nelle iniziative faro della strategia Europa 2020³², culminando con l'Agenda digitale europea³³ e la strategia del mercato unico digitale del 2015³⁴. Lo schema regolatorio europeo si è posto il fine di recuperare terreno rispetto al crescente potere economico delle potenze straniere³⁵. La Comunicazione della Commissione “2030 Digital Compass” ha poi sottolineato come

²⁶ S. Cassese, *Democrazie e poteri (privati) globali*, «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*, «Diritto dell'informazione e dell'informatica», 1, 2025, pp. 81 ss.

²⁷ J.P. Beetz, *Saving popular sovereignty from a slow death in the European union*, «Journal of Common Market Studies», 26(2), 2024, pp. 508-524.

²⁸ Si veda D. Martire, *Pluralità degli ordinamenti giuridici e Costituzione repubblicana. Spunti di riflessione alla luce dell'esperienza costituzionale*, «Diritto pubblico», 3, 2017, pp. 872 ss., secondo il quale, peraltro, “sovranità” è in contrapposizione con “autonomia”.

²⁹ Consiglio europeo, *Conclusioni della Presidenza*, Lisbona, 23-24 marzo 2000.

³⁰ Comunicazione della Commissione al Consiglio e 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; 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.

³¹ 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.

³² Comunicazione della Commissione, *Europa2020 – Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM(2010) 2020, def., 3 marzo 2020.

³³ 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.

³⁴ 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.

³⁵ M. Granieri, *Problema e sistema dei dati non personali nel diritto euro-unitario*, in *Annali italiani del diritto d'autore – AIDA*, a cura di AA. VV., Milano, 2023, p. 199.

la pandemia abbia esposto le vulnerabilità dello spazio digitale europeo 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 2030³⁶.

La produzione normativa in materia digitale, sebbene recente, è estremamente vasta e una mappatura completa richiederebbe di considerare anche la regolamentazione settoriale. Nel presente paragrafo si tenterà di fornire una panoramica – suddivisa in raggruppamenti omogenei che, tuttavia, sarà influenzata prossimamente dalle proposte di Omnibus digitale³⁷ e Omnibus sull'IA³⁸ – delle principali iniziative dell'Unione Europea, al fine di evidenziare l'approccio Unionale al tema della sovranità digitale.

Il cuore pulsante della strategia si può rinvenire nel programma strategico per il decennio digitale 2030³⁹ (si prevede per giugno 2026 la revisione del *digital decade policy programme*⁴⁰), il quale rappresenta il salto di qualità nella capacità, a livello istituzionale, di governare le strategie nazionali e Unionali, poiché per la prima volta queste vengono inserite in modo organico all'interno di un quadro coordinato in cui si includono linee guida, un monitoraggio e una valutazione, prevedendo anche eventuali revisioni. Si stabiliscono così obiettivi vincolanti e si crea un *framework* di *governance* per coordinare l'azione degli Stati membri, una visione ulteriormente rafforzata dal *Competitiveness Compass* e dalla strategia *Single Market*⁴¹. 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

³⁶ 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.

³⁷ Commissione Europea, *Proposta di regolamento che modifica il Regolamento (UE) 2016/679 (GDPR), la Direttiva 2002/58/CE (ePrivacy), la Direttiva (UE) 2022/2555 (NIS2) e il Regolamento (UE) 2023/2854 (Data Act) per la semplificazione del quadro normativo digitale*, COM(2025) 837 final.

³⁸ Commissione Europea, *Proposta di regolamento che modifica i Regolamenti (UE) 2024/1689 (AI Act) e (UE) 2018/1139 per la semplificazione dell'attuazione delle norme armonizzate sull'intelligenza artificiale*, COM(2025) 836 final.

³⁹ 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.

⁴⁰ Si veda <https://digital-strategy.ec.europa.eu/en/consultations/survey-opens-future-digital-decade-policy-programme>.

⁴¹ 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*.

– 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 dati⁴² ha costituito la pietra angolare che ha stabilito uno standard globale per la protezione dei dati personali. Questo è stato affiancato dalla Direttiva ePrivacy⁴³ che protegge le comunicazioni elettroniche e dalla Direttiva sulla protezione dei dati nel *law enforcement*⁴⁴. La *governance* è affidata all'*European Data Protection Board* (EDPB) che coordina le autorità nazionali e all'*European Data Protection Supervisor* (EDPS). Il *framework* sui diritti digitali fondamentali ha permesso all'Europa di posizionarsi come modello di esportazione normativa (il cd *Brussels effect*⁴⁵).

Il secondo *cluster* comprende la *governance* dell'intelligenza artificiale, dove il Regolamento sull'IA⁴⁶ ha rappresentato la prima regolamentazione sistematica a livello mondiale, introducendo un sistema di classificazione del rischio (sebbene con problemi di effettività⁴⁷) con obblighi proporzionati che vanno dalla proibizione per pratiche inaccettabili, attraverso valutazioni di conformità per sistemi ad alto rischio, fino a obblighi di trasparenza per sistemi a rischio minimo. Il regolamento include regole specifiche per i modelli a scopi generali. La *governance* è affidata all'Ufficio

⁴² 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.

⁴³ 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.

⁴⁴ 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.

⁴⁵ A. Bradford, *The Brussels Effect*, «Nw. U. L. Rev.», 107, 1, 2012.

⁴⁶ 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.

⁴⁷ *Ex multis*, T. Karathanasis, *The AI Act: balancing implementation challenges and the EU's simplification agenda*, «SSRN» 2025, <https://ssrn.com/abstract=5332512>. 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*, «European Journal of Risk Regulation», 16, 2025, pp. 1082-1097.

europeo per l'IA e all'*European Artificial Intelligence Board*⁴⁸. Nel contesto dell'IA, la strategia *Apply AI* mira ad accelerare l'adozione dell'IA in dieci settori industriali chiave⁴⁹, supportata da investimenti settoriali, dalla rete di *AI Factories* sull'infrastruttura EuroHPC per sviluppare modelli AI avanzati, da programmi per formare e attrarre talento europeo⁵⁰, dal *Memorandum of Understanding sulle AI Gigafactories*⁵¹ e dall'*AI Pact*⁵². Il regolamento EuroHPC è stato 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 sovranità nell'AI⁵³.

Il terzo *cluster* investe la regolamentazione delle piattaforme digitali e dei contenuti online. Il Regolamento sui servizi digitali (*Digital Services Act, DSA*)⁵⁴ stabilisce obblighi di due *diligence* proporzionali, sistemi di *notice-and-action* per contenuti illegali, trasparenza algoritmica e gestione del rischio sistemico. Il DSA è completato dal Regolamento sui mercati digitali (*Digital Markets Act, DMA*) che – come descritto – affronta il potere dei *gatekeeper* designati sulla base di criteri quantitativi e qualitativi, imponendo obblighi *ex-ante* come l'interoperabilità dei servizi di messaggistica, il divieto di auto-preferenza, la portabilità dei dati e il divieto di combinare dati personali senza consenso esplicito. La Commissione ha analizzato l'interazione del DSA con altre normative europee⁵⁵, riconoscendo le “tensioni” con la Direttiva sul diritto d'autore nel mercato unico digitale⁵⁶. Vi sono poi il Regolamento

⁴⁸ Art. 64, Regolamento (UE) 2024/1689.

⁴⁹ Commissione europea, *Comunicazione della Commissione al Parlamento europeo e al Consiglio – Apply AI Strategy*, COM(2025) 723 final, Bruxelles, 8 ottobre 2025.

⁵⁰ Si veda <https://digital-strategy.ec.europa.eu/en/library/shaping-and-strengthening-european-ai-talent>.

⁵¹ 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>.

⁵² Si veda <https://digital-strategy.ec.europa.eu/it/policies/ai-pact>.

⁵³ 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.

⁵⁴ 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.

⁵⁵ 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.

⁵⁶ 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.

sulla trasparenza della pubblicità politica⁵⁷, il Regolamento sulla libertà dei media europei⁵⁸, la Direttiva sui servizi media audiovisivi⁵⁹, il Regolamento sui contenuti terroristici online⁶⁰ e le proposte su *combating violence against women*⁶¹ e contrasto agli abusi sessuali sui minori⁶². La *governance* 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*), l'*High-Level Group on DMA* e l'*European Board for Media Services* per l'EMFA. La proposta di *Digital Fairness Act* promette di aggiungere ulteriori tutele per i consumatori digitali, 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.

Il quarto *cluster* riguarda l'economia dei dati e gli spazi dati settoriali. Il Regolamento sui dati⁶³ sblocca i dati industriali e dell'IoT con diritti di accesso ai dati generati da prodotti connessi, regole sulla condivisione B2B, meccanismi per rendere disponibili dati privati alla pubblica amministrazione in emergenza e disposizioni per mitigare il

⁵⁷ 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.

⁵⁸ 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.

⁵⁹ 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.

⁶⁰ 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.

⁶¹ 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.

⁶² 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.

⁶³ 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.

lock-in dei fornitori *cloud*. Il Regolamento sulla *governance* dei dati⁶⁴ introduce intermediari affidabili che facilitano la condivisione volontaria e un *framework* per l'altruismo dei dati. Lo Spazio europeo dei dati sanitari (EHDS)⁶⁵ costituisce il primo *data space* settoriale pienamente regolamentato. La Direttiva sui dati aperti⁶⁶ completa il quadro, mentre la strategia *European Data Union* mira a creare spazi dati settoriali (energia, mobilità, agricoltura, manifattura, finanza), proponendo un modello europeo basato su condivisione volontaria facilitata da intermediari fiduciari, accesso regolamentato per finalità di interesse pubblico ed *empowerment* individuale. La *governance* è coordinata dall'*European Data Innovation Board* (EDIB), dall'*European Health Data Space Board* specificamente per il settore sanitario e dall'*Interoperable Europe Board* che garantisce l'interoperabilità tecnica e semantica dei sistemi pubblici.

Il quinto *cluster* riguarda la cybersicurezza e la resilienza digitale. Il Regolamento sulla *cybersicurezza*⁶⁷ conferisce a ENISA (*European Network and Information Security Agency*), un ruolo permanente con mandato rafforzato e fornisce il *framework* europeo di certificazione *cybersecurity*. La Direttiva NIS 2⁶⁸ espande le regole di base, coprendo 18 settori ad alta criticità (energia, trasporti, banche, infrastrutture digitali, spazio) con obblighi di gestione del rischio *cyber* e *reporting* di incidenti. Il Regolamento sulla resilienza cibernetica⁶⁹ rappresenta una normativa rivoluzionaria per i prodotti connessi richiedendo *security-by-design* durante tutto il ciclo di vita. Il

⁶⁴ 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.

⁶⁵ 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.

⁶⁶ 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.

⁶⁷ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la *cybersicurezza*, e alla certificazione della *cybersicurezza* per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (Regolamento sulla *cybersicurezza* – *Cybersecurity Act*), *GUUE* L 151, 7 giugno 2019.

⁶⁸ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di *cybersicurezza* 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.

⁶⁹ Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di *cybersicurezza* 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 *cyberresilienza* – *Cyber Resilience Act*, CRA), *GUUE* L, 20 novembre 2024.

Regolamento sulla solidarietà cibernetica⁷⁰ rafforza le capacità europee attraverso l'*European Cyber Shield*, il sistema di allerta europeo e la *EU Cybersecurity Reserve*. Il Regolamento DORA applica questi principi al settore finanziario⁷¹. La Commissione ha proposto un nuovo pacchetto sulla *cybersicurezza*, inclusa la revisione del *Cybersecurity Act*⁷². La *governance* coinvolge ENISA come *hub* tecnico centrale, l'*European Cybersecurity Competence Centre* (ECCC) che coordina la ricerca e l'innovazione, CERT-EU per le istituzioni europee, il *Cyber Crises Liaison Organisation Network* (EU CyCLONe) per la gestione coordinata di crisi *cyber* su larga scala e la rete CSIRTs che connette i *computer security incident response team* nazionali.

Il sesto *cluster* interessa le tecnologie strategiche e l'autonomia industriale. Il Regolamento europeo sui semiconduttori⁷³ menziona esplicitamente il rafforzamento della sovranità digitale come obiettivo cardine⁷⁴, collegandosi al *Chips Joint Undertaking*⁷⁵ che mobilita risorse pubbliche e private per R&D, attualmente oggetto di consultazione pubblica⁷⁶. Il Regolamento sull'industria a zero emissioni nette⁷⁷ e il Regolamento sulle materie prime critiche⁷⁸ rafforzano l'indipendenza europea con

⁷⁰ 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 *cybersicurezza*, e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (Regolamento sulla *cybersolidarietà* – *Cyber Solidarity Act*), *GUUE* L, 15 gennaio 2025.

⁷¹ 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.

⁷² Si veda <https://www.europarl.europa.eu/news/it/agenda/plenary-news/2026-01-19/8/le-nuove-proposte-sulla-cybersicurezza-dell-ue>.

⁷³ 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.

⁷⁴ Commissione europea, *Chips Act* – Relazione illustrativa, COM(2022) 46 final, p. 4.

⁷⁵ Si veda https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/chips-joint-undertaking_en.

⁷⁶ Si veda <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3932>.

⁷⁷ 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 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.

⁷⁸ 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

obiettivi quantitativi (produrre in Europa almeno il 40% del fabbisogno di tecnologie *net-zero*, estrarre almeno il 10% e processare almeno il 40% delle materie prime critiche entro il 2030). Il prossimo *Quantum Act* dovrebbe applicare una logica simile al *quantum computing*, stabilendo un *framework* per investimenti coordinati e sviluppo di competenze, riconoscendo che il *quantum computing* rappresenta una tecnologia potenzialmente *disruptive* dove l'Europa rischia di rimanere indietro senza che vi sia un intervento coordinato. Il prossimo *EU Space Act*⁷⁹ mira a rafforzare l'autonomia europea nelle tecnologie spaziali, dove l'UE ha già capacità significative attraverso Galileo, Copernicus e EGNOS, supportati dal Programma per una connettività sicura⁸⁰. L'*EU Cloud and AI Development Act*⁸¹ e l'*Advanced Materials Act*⁸² promettono di completare il quadro di autonomia strategica, mentre la Piattaforma STEP⁸³ crea un ombrello finanziario che mobilita risorse attraverso vari strumenti esistenti, coordinato da molteplici *Joint Undertakings* e *board* settoriali attraverso consorzi come ECIC⁸⁴ ed EDIC⁸⁵. Un ruolo crescente spetterà all'*Industrial Accelerator Act*⁸⁶, proposta che si prefigge di accelerare la transizione delle industrie europee ad alta intensità energetica attraverso tre assi principali: la semplificazione dei procedimenti autorizzativi, la creazione di *lead markets* per prodotti a bassa emissione e il rafforzamento delle catene di approvvigionamento con criteri “*clean, resilient,*

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, 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.

⁷⁹ Si veda https://defence-industry-space.ec.europa.eu/eu-space-act_en.

⁸⁰ 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.

⁸¹ 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>.

⁸² Si veda https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/chemicals-and-advanced-materials/towards-advanced-materials-act_en.

⁸³ 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.

⁸⁴ Art. 7, *European Chips Act*.

⁸⁵ Si veda <https://digital-strategy.ec.europa.eu/en/policies/edic>.

⁸⁶ 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.

circular, cybersecure”⁸⁷. Anche il settore del *defence tech* ha assunto importanza crescente: il Fondo europeo per la difesa⁸⁸ sta investendo oltre quattro miliardi di euro in tecnologie critiche (IA militare, tecnologie quantistiche, *cyber difesa*, sistemi autonomi). L’UE sta sviluppando una piattaforma federata DAIDS per la condivisione sicura di dati di difesa e un *cloud* militare sovrano⁸⁹. Nel 2025, le *startup* europee nel *defence tech* hanno raccolto 8,7 miliardi di dollari (+55%), con la *defence tech* diventata la categoria a più rapida crescita nel *venture capital* europeo (6,2% del totale)⁹⁰.

Il settimo *cluster* riguarda la connettività, le infrastrutture digitali e i servizi fiduciari. Il Codice europeo delle comunicazioni elettroniche (EECC)⁹¹ fornisce il *framework* armonizzato per la regolamentazione dei servizi di rete, con la gestione dello spettro radio⁹², l’armonizzazione delle bande di frequenza⁹³, la neutralità della rete⁹⁴ e le regole sul *roaming*⁹⁵. Il Regolamento sulle infrastrutture *gigabit* accelera lo sviluppo di reti ad altissima capacità con l’obiettivo di connettività *gigabit* per tutti entro il 2030⁹⁶. Il

⁸⁷ 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.

⁸⁸ 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.

⁸⁹ Euractiv, *Exclusive: EU wants defence data secured without US tech*, 2026; cfr. anche Commissione europea, *Cloud Sovereignty Framework*, versione 1.2.1, ottobre 2025.

⁹⁰ 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.

⁹¹ 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.

⁹² Decisione 676/2002/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa a un quadro normativo per la politica in materia di spettro radio nella Comunità europea (Decisione sullo spettro radio), GUCE L 108, 24 aprile 2002.

⁹³ 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.

⁹⁴ 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.

⁹⁵ 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.

⁹⁶ 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

Digital Networks Act (DNA), che dovrebbe chiudere il percorso di approvazione entro un anno, mira a sostituire il Codice con regole più semplici che riducono frammentazione normativa e adattano il *framework* alla convergenza tra telecomunicazioni⁹⁷, media e servizi digitali⁹⁸. La Direttiva sulla compatibilità elettromagnetica⁹⁹ e la Direttiva sulle apparecchiature radio¹⁰⁰ garantiscono l'uso efficiente dello spettro. Il Regolamento eIDAS¹⁰¹, aggiornato dall'eIDAS 2.0¹⁰², abilita l'identità digitale sicura attraverso l'*European Digital Identity Wallet* con mutuo riconoscimento transfrontaliero garantito. La *governance* è coordinata dal BEREC (*Body of European Regulators for Electronic Communications*), dal *Communications Committee* (COCOM) e dal *Gateway coordination group* per eIDAS, mentre il Regolamento sull'interoperabilità europea garantisce più in generale l'interoperabilità dei sistemi informativi pubblici attraverso standard comuni e architetture di riferimento.

L'ottavo e ultimo *cluster* riguarda il mercato unico digitale, la concorrenza e la protezione dei consumatori. Il DMA impone obblighi *ex-ante* sui *gatekeeper*, complementato dalla normativa antitrust. Sul fronte dei consumatori, la Direttiva sui diritti dei consumatori¹⁰³ garantisce diritti di recesso e informazioni precontrattuali,

che abroga la direttiva 2014/61/UE (Regolamento sulle infrastrutture *Gigabit – Gigabit Infrastructure Act*, GIA), GUUE L, 8 maggio 2024.

⁹⁷ Il settore delle telecomunicazioni non è analizzato in questo contributo dal momento che il tema affrontato riguarda l'ecosistema digitale nel suo complesso. Per un approfondimento e una serie di proposte concrete di riforma, si v. F. Bassanini e A. Perrucci (a cura di), *Telecomunicazioni: una politica industriale per la doppia transizione*, Bologna, 2025.

⁹⁸ M. Manganeli, *Il Digital Networks Act, fra nuove tecnologie, nuove dinamiche di mercato e vecchi principi regolatori*, «Rivista della Regolazione dei mercati», 2, 2025.

⁹⁹ 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.

¹⁰⁰ 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.

¹⁰¹ 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.

¹⁰² 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.

¹⁰³ 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 del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la

completata dalla Direttiva sulle pratiche commerciali sleali¹⁰⁴, dalla Direttiva sulle clausole abusive¹⁰⁵, dalla Direttiva sull'indicazione dei prezzi¹⁰⁶ e dalle direttive su *Digital content*¹⁰⁷ e *Digital contracts for goods*¹⁰⁸. Il Regolamento sulla sicurezza generale dei prodotti¹⁰⁹ rafforza la tracciabilità e gli obblighi per *marketplace* online. La Direttiva sulla responsabilità da prodotto difettoso¹¹⁰ copre esplicitamente software difettoso e sistemi IA sotto responsabilità oggettiva. La Direttiva sul diritto alla riparazione¹¹¹ e il Regolamento sulla progettazione ecocompatibile¹¹² promuovono sostenibilità ed economia circolare. La *governance* coinvolge la *DG Competition* per

direttiva 97/7/CE del Parlamento europeo e del Consiglio (Direttiva sui diritti dei consumatori), GUUE L 304, 22 novembre 2011.

¹⁰⁴ 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.

¹⁰⁵ 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.

¹⁰⁶ 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.

¹⁰⁷ 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.

¹⁰⁸ 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.

¹⁰⁹ 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.

¹¹⁰ 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.

¹¹¹ 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.

¹¹² 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.

l'*enforcement antitrust*, l'*European Competition Network* (ECN) che coordina le autorità nazionali di concorrenza e l'*High-Level Group on DMA*.

La sopra delineata normativa a otto cluster rappresenta un tentativo – articolato – di *governance* democratica della trasformazione tecnologica. L'obiettivo di tale produzione normativa è tentare di dimostrare come sia possibile costruire un'economia digitale competitiva e innovativa che rispetti diritti fondamentali, protegga l'ambiente¹¹³, garantisca sicurezza e promuova equità sociale. La tensione tra tali obiettivi anche 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. Il *Digital Fitness Check* affronta tale complessità attraverso una valutazione sistematica dell'impatto cumulativo delle regole digitali europee che riconosce esplicitamente le preoccupazioni su oneri di *compliance*, sovrapposizioni normative e potenziali effetti negativi su innovazione e competitività¹¹⁴.

4. Dalla regolazione alla politica industriale

Lo sviluppo dell'industria digitale europea e 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”.

Questo quadro chiaro-scuro è quello su cui si innestano gli atti normativi e le politiche europee sul digitale, descritte nel paragrafo precedente, che nel loro complesso testimoniano un generale cambio di paradigma nell'intervento pubblico europeo: lo spostamento progressivo da un'impostazione prevalentemente regolatoria, nel senso classico di disciplina pro-concorrenziale del mercato e tutela di diritti dei consumatori, verso un'impostazione che incorpora esplicitamente strumenti di politica economica e industriale e, più di recente, anche relativi alla difesa e alla sicurezza nazionali.

La regolazione europea dei mercati digitali nasce in un contesto completamente diverso rispetto a quello della liberalizzazione e regolazione pro-concorrenziale delle *public utilities* tradizionali (telecomunicazioni, energia, trasporti a rete, servizi postali). L'iniziale approccio regolatorio al digitale aveva infatti lo scopo principale di creare le

¹¹³ Sui problemi dell'*AI Act* rispetto alla tutela dell'ambiente, si veda N. Rangone, *Intelligenza artificiale, tutela dell'ambiente e regolazione europea*, «Biolaw Journal-Rivista di biodiritto», 1, 2025.

¹¹⁴ 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.

precondizioni e gli incentivi alla fornitura e l'adozione dei servizi (direttiva *e-commerce*), con obiettivi primari di tutela del cittadino/consumatore, al fine di 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 attribuito intenzionalmente buona parte dell'onere sull'*incumbent* ex-monopolista (regolazione asimmetrica), *in primis* attraverso obblighi di accesso alle infrastrutture essenziali a condizioni eque, trasparenti e non discriminatorie, 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 di minori dimensioni e sui nuovi entranti, che non hanno la possibilità di distribuire 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)¹¹⁵.

Peraltro, come descritto nel paragrafo 2, nei mercati digitali si sono progressivamente creati assetti estremamente concentrati, fino a forme di quasi-monopolio o oligopolio ristretto a livello globale. Tuttavia, la genesi di queste posizioni dominanti è diversa da quella delle utilities, poi liberalizzate: non deriva (in via principale) da barriere

¹¹⁵ 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. Draghi, op. cit.

giuridiche alla concorrenza (monopoli legali o concessioni esclusive), ma da dinamiche di mercato e di innovazione in contesti globali¹¹⁶.

Nei mercati e nell'industria digitale non esiste quindi un percorso politico-normativo da invertire, redistribuendo risorse, asset e rendite prodotti 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/infrastruttura, nel digitale, il “fattore scarso” è un insieme di risorse, che si collocano a un livello superiore rispetto all'infrastruttura, e.g., capitale, conoscenza, utenti, algoritmi, dati, standard, che di per sé non sono scarse, ma lo è il loro uso complementare e orchestrato, 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 agevolanti un *level playing field* concorrenziale può non essere sufficiente a creare le condizioni economiche perché un entrante raggiunga la necessaria 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; tuttavia, anche interventi *ex ante*, se non accompagnati da leve di scala e investimento, rischiano di migliorare la “correttezza” del gioco concorrenziale senza cambiarne tuttavia il risultato industriale.

Il *Digital Markets Act* (DMA), come accennato, 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 obiettivi: la contendibilità, volta a creare spazi di potenziale concorrenza, e l'equità, tesa a limitare pratiche di sfruttamento e riequilibrare i rapporti

¹¹⁶ 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*. F. Chirico e A. Manganelli, *Mercati e servizi digitali*, in *Economia e Diritto della Regolazione. Reti, piattaforme e servizi di pubblica utilità*, a cura di C. Cambini, G. Napolitano e A. Nicita, Bologna, Il Mulino, 2024.

tra piattaforme e imprese utenti/*complementors*. Il perseguimento e anche il raggiungimento di questi obiettivi può rendere il mercato “più aperto”, attraverso obblighi di portabilità e interoperabilità, e 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.

Peraltro, come richiamato, gli ecosistemi digitali che le *big tech* hanno costruito attorno ai principali servizi di piattaforma base, in ragione del loro predominio su scala globale, ha condizionato e sta condizionando le dinamiche economico-industriali in tutto il comparto digitale. E, con esso, in ragione delle elevate esternalità, sull’intero tessuto economico-sociale.

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 determina automaticamente capacità produttive, filiere, investimenti e scala, che possano riequilibrare il mercato, soprattutto quando i mercati di riferimento sono globali e gli incumbent sono al centro di ecosistemi su loro calibrati e da loro orchestrati.

La giustificazione dell’intervento pubblico nell’economia si è quindi progressivamente spostata, in Europa, in un certo senso ricalibrandosi verso gli altri attori pubblici a livello globale: non più e non solo correggere inefficienze statiche, come rimedio puntuale al potere e ai fallimenti di mercato, ma rafforzare la capacità competitiva dell’Europa, attraverso il rafforzamento della capacità delle sue imprese di fornire servizi e infrastrutture digitali, anche aumentando (nel tempo) la loro scala, così come la loro capacità di costruire e orchestrare alcuni segmenti degli ecosistemi digitali.

Del resto, l’evoluzione del contesto geo-politico ha reso necessario questo spostamento anche alla luce di una necessaria “autonomia strategica” e resilienza verso crisi o rischi che impattino sulla capacità produttiva, commerciale e infine anche “politica”, nel senso pieno del termine¹¹⁷, dell’Europa e dei suoi stati membri.

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

¹¹⁷ C. Scarpa, *Cosa c’è di nuovo nella “nuova” politica industriale europea?*, «Rivista della regolazione dei mercati», 2, 2024.

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, contendibilità dei mercati); dall’altro lato, tentazioni di piegare il diritto della concorrenza e la regolazione pro-mercato a finalità di protezione dei campioni europei, con effetti potenzialmente distorsivi¹¹⁸.
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 consentano interoperabilità e riducano *lock-in*, mentre la politica industriale costruisce e abilita alternative credibili (infrastrutture, piattaforme, standard, progetti comuni e domanda pubblica).
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 soluzioni¹¹⁹. D’altro canto, il “traino” americano nell’industria digitale non è riconducibile soltanto all’iniziativa privata: gli investimenti pubblici, a cominciare da quelli nel settore della difesa, hanno storicamente svolto un ruolo determinante nel finanziare la ricerca di base, creare domanda iniziale per tecnologie innovative e sostenere la scalabilità delle soluzioni – come dimostra il caso emblematico degli investimenti federali nella difesa e nella sicurezza nazionale che hanno alimentato filiere tecnologiche poi divenute commerciali.

¹¹⁸ M. Grillo, *Concorrenza e politica industriale: cosa cambia con la globalizzazione*, «Rivista della regolazione dei mercati», 2, 2024.

¹¹⁹ M. Mazzucato e C. Perez, *Redirecting growth: inclusive, sustainable and innovation-led*, in *A Modern Guide to Uneven Economic Development*, a cura di E.S. Reinert e I.H. Kvangraven, 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*, «Rivista della regolazione dei mercati», 1, 2025.

5. La Politica industriale verso la “sovrànità digitale” e la “autonomia strategica”

Come evidenziato dai report Draghi e Letta, l’Unione europea è dinnanzi a una sfida esistenziale: colmare il divario di competitività (che è soprattutto determinato dai gap di innovazione e di produttività) con Stati Uniti e Cina e ridurre le dipendenze strategiche da paesi terzi.

Come ricordato, attualmente, l’UE dipende dai paesi stranieri per oltre l’80% dei suoi prodotti, servizi e infrastrutture digitali. Tale situazione sta rappresentando il principale *trigger* delle recenti azioni di politica economica nell’industrie digitali. Ed è in questo contesto che il concetto di sovranità digitale¹²⁰ è emerso sempre più, catalizzato dalla pandemia COVID-19 che ha esposto drammaticamente le vulnerabilità e le dipendenze dell’Europa¹²¹ (sebbene il termine risalga già ai tempi del programma Galileo, nel 2000)¹²².

Il concetto di sovranità digitale, pur essendo diventato centrale nel discorso politico europeo, rimane caratterizzato tuttavia da una certa ambiguità definitoria sovrapponendosi, peraltro, con i concetti “autonomia strategica digitale” e “sovrànità dei dati” – e con un significato che è più politico che giuridico¹²³. Il concetto interpretativo chiave in questo puzzle è forse quello di “autonomia strategica”¹²⁴ – inizialmente definito (significativamente) come autonomia strategica “aperta” – con cui si 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. In questo senso, la

¹²⁰ P. Bellanger, *De la souveraineté en général et de la souveraineté numérique en particulier*, «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 *Enciclopedia del diritto. Potere e Costituzione*, diretto da M. Cartabia e M. Ruotolo, 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. Cows, F. Casolari, J. Morley, M. Taddeo e L. Floridi, *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, «Internet Policy Review», 2021, p. 3.

¹²¹ P. Zuddas, *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell’emergenza sanitaria*, «Osservatorio AIC», 3/2020, p. 83.

¹²² C. Hobbs, *L’Europa alla ricerca di una sovranità digitale: sfide e interessi in gioco*, «Agenda Digitale», 8 ottobre 2020.

¹²³ G. Finocchiaro, *La sovranità digitale*, «Diritto Pubblico», 2022, pp. 809 e ss.

¹²⁴ 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.

sovranità digitale europea va intesa come “sovranità relativa”, ossia una sovranità che si esercita in un contesto di interdipendenze e che richiede scelte consapevoli su dove concentrare le risorse e l’azione pubblica.

In questo contesto, come descritto, si inserisce la Bussola della competitività, che mira in prima istanza a ridurre le dipendenze strategiche dell’UE (terzo pilastro), anche colmando il divario di innovazione (primo pilastro) e rendendo la transizione verde un vantaggio di competitività (secondo pilastro). Tutti questi pilastri (e in particolare il primo e il terzo) mirano in ultima analisi a rafforzare l’“autonomia strategica” europea, ma lo fanno da angolazioni diverse e con tempistiche distinte.

L’obiettivo di autonomia strategica può essere infatti perseguito attraverso azioni di *policy* che rientrano sostanzialmente in due tipologie generali: (I) misure volte a promuovere catene di approvvigionamento alternative basate sull’industria 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 mutualmente escludenti, la distinzione è importante dal punto di vista analitico e normativo.

L’approccio restrittivo richiede un’attenta valutazione, in particolare se sviluppato e portato a compimento nel breve periodo. Qualsiasi dipendenza ha infatti 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 un impatto specifico sulla produttività e sulla competitività¹²⁵. La ricerca di una maggiore indipendenza comporta, quindi, nel breve termine potenziali rischi, tra cui un possibile rallentamento della diffusione di beni e servizi digitali, 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 è altamente complesso, ma è nondimeno essenziale per garantire che gli sforzi volti a diminuire le dipendenze non ostacolino – inavvertitamente – il ciclo di innovazione che la stessa Bussola per la Competitività mira ad accelerare¹²⁶.

D’altra parte, un approccio abilitante eurounitario può consentire progressivamente alle imprese europee di competere in modo più efficace, sia nei mercati privati che negli appalti pubblici. In questo ambito si inseriscono anche le misure abilitanti di intervento pubblico diretto e, in prima battuta, le azioni del PNRR che hanno finanziato

¹²⁵ Draghi, op. cit.

¹²⁶ Z. Mayers, *A framework for understanding EU competitiveness*, CERRE issue paper, 2024.

in diversa misura tutti i profili del digitale (a titolo esemplificativo, HPC, sostegno alla ricerca, *cloud* e satelliti). Tuttavia, è fondamentale tenere conto del vincolo di sostenibilità economica delle azioni intraprese e da intraprendere, valutare cioè se i finanziamenti previsti presentano prospettive per futuri guadagni di competitività – valutazione *ex ante* che probabilmente non sempre è stata portata a compimento per quanto concerne i fondi PNRR.

Vero è che gli obiettivi abilitati dal lato dell’offerta, ad esempio il sostegno alla costruzione di reti digitali, *cloud*, e altre infrastrutture digitali, si giustificano sotto un profilo economico anche in ragione del fatto che i guadagni di produttività derivanti dalle tecnologie *general-purpose* (GPT) spesso si manifestano con un ritardo temporale¹²⁷; tuttavia, tali obiettivi devono comunque essere valutati rispetto alla domanda attuale e prevista. In altri termini, perché il sostegno all’“investimento anticipatorio” sia efficace, deve comunque riflettere effetti di produttività differenziati, esternalità e capacità di assorbimento. Nel caso dei *data center* e delle *AI factories*, ad esempio, le tendenze della domanda e della disponibilità a pagare devono essere accuratamente valutate, ad evitare dimensioni di investimento (e di impatti ambientali) che poi si rivelino non sostenibili.

Quindi, ogni approccio abilitante deve essere progettato con attenzione poiché le politiche abilitanti possono soddisfare vincoli sostanziali, ossia: (I) di sostenibilità *ex post*, soprattutto in caso di (II) effetti di dipendenza, cioè quando un sostegno eccessivo o prolungato potrebbe creare dipendenza dall’intervento pubblico, piuttosto che costruire una capacità reale; oppure anche in caso di (III) effetti soglia, cioè quando un sostegno insufficiente non riesce a superare gli svantaggi strutturali, generando costi (pubblici) senza ritorni in termini di vantaggi competitivi.

Nell’attuale contesto, è quindi complicato immaginare un avanzamento sistematico su tutti i possibili fronti di autonomia strategica: occorre invece optare per strategie di diversificazione e verticalizzazione. Si pensi, ad esempio, allo sviluppo e applicazione di sistemi di IA, anche sostenuti dalla domanda pubblica, negli ambiti economici e

¹²⁷ Ciò avviene perché l’adozione e le capacità complementari tendono a seguire il dispiegamento infrastrutturale solo dopo un periodo di aggiustamento. Cfr. E. Brynjolfsson, *The productivity paradox of information technology*, «Communications of the ACM», 36 (12), 1993, pp. 66-77; E. Brynjolfsson, D. Rock e C. Syverson, *The Productivity J-Curve: How Intangibles Complement General Purpose Technologies*, «American Economic Journal: Macroeconomics», 13 (1), 2021, pp. 333-72. 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, il cui sviluppo non può essere trainato dalla domanda di mercato corrente.

industriali che possono generare guadagni di competitività per il sistema europeo. Peraltro, è chiaro che applicazioni verticali dell'IA richiedono anche l'accelerazione nella realizzazione dei *Common European Data Spaces* settoriali.

Con grande probabilità, uno strumento abilitativo molto rilevante sarà quello dell'uso strategico-industriale della domanda pubblica, volta a rafforzare le industrie nazionali dell'UE, soprattutto nel settore del *cloud* e dell'IA. Tuttavia, tali azioni avranno anche effetti “restrittivi”, limitando l'accesso al mercato per i fornitori non UE e, come descritto, la sfida principale sarà quindi gestire gli acquisti pubblici conciliando le esigenze di autonomia strategica e le esigenze di scelte efficienti per le pubbliche amministrazioni. Queste politiche dal lato della domanda pubblica saranno in gran parte basate sulla revisione della direttiva sul *public procurement*, 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 strategici¹²⁸.

In questo contesto, una ulteriore dimensione delle politiche orientate all'autonomia strategica si riferisce all'ambito di applicazione, ossia la distinzione fra misure rivolte ai privati (consumatori e imprese) e misure rivolte ai governi e altre amministrazioni pubbliche (“privato” vs “pubblico”)¹²⁹. Le opzioni di *policy* rivolte ai servizi per gli enti pubblici non implicano necessariamente minori *trade-off* economici; tuttavia, il quadro analitico è tipicamente 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.

Un settore paradigmatico dell'evoluzione della regolazione e della politica industriale europea è quello del *cloud*. Nonostante la composita regolazione pro-concorrenziale

¹²⁸ 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.

¹²⁹ 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.

del settore¹³⁰, questo è uno dei settori in cui si segnala una fortissima dipendenza strategica e un *deficit* di investimenti che l'Europa (fondi privati e/o pubblici) deve colmare per soddisfare la domanda (o parte di essa) in modi alternativi¹³¹. Come accennato, in coerenza con il percorso descritto, una delle principali azioni di policy dell'UE sarà la proposta di regolamento sullo sviluppo del *cloud* e dell'intelligenza artificiale (*Cloud and AI Development Act*, CAIDA), che rappresenta una chiara azione di politica industriale. Il CAIDA si concentra principalmente su misure “abilitanti” volte a rafforzare le industrie nazionali dell'UE nel settore del *cloud* e dell'IA – ad esempio attraverso (I) lo sviluppo di *data-center* altamente sostenibili, che consentano di triplicare nei prossimi cinque-sette la capacità di elaborazione dati nell'UE, e (II) la creazione di un'infrastruttura *cloud* sicura e “sovrana”, 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. Come accennato, è chiaro come alcune disposizioni relative allo sviluppo di una maggiore “autonomia e sovranità” potrebbero tuttavia funzionare come misure “restrittive”, limitando l'accesso al mercato per i fornitori non UE¹³².

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 ora integra preoccupazioni di sicurezza nazionale, autonomia, resilienza delle infrastrutture critiche e valori fondamentali europei volti ad affermare la propria

¹³⁰ Sia in termini di regolazione asimmetrica: il *cloud* è uno dei servizi di piattaforma base definiti dal DMA, sia in termini di regolazione simmetrica, a tutela del consumatore nello *switching* e terminazione dei contratti definita dal *Data Act*. Cfr. A. Manganelli, *La composita regolazione pro-concorrenziale dei servizi di Cloud*, «Mercato Concorrenza Regole», n 3/24, 2024.

¹³¹ Tale dipendenza è conseguenza 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.

¹³² In questo contesto, sono emerse soluzioni commerciali di “*cloud* sovrano” sviluppate anche 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. Recentemente, la definizione di un *Cloud Sovereignty Framework* (CSF), da parte della DG per i Servizi digitali della Commissione, ha tradotto il concetto di sovranità digitale in criteri oggettivi – *Sovereignty Effective Assurance Levels* e *Sovereignty Score* – che operano come requisiti di ammissibilità e criteri di aggiudicazione nei bandi UE per la fornitura di servizi *cloud*. Questo non è un atto normativo che vincola gli Stati membri; tuttavia, fornisce un modello comune di valutazione della “sovranità del *cloud*” che molte amministrazioni nazionali potrebbero adottare per standardizzare il concetto di “*cloud* sovrano”.

sovranità¹³³. 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 alquanto “opaca”, per quanto necessaria e fortemente richiesta dal mercato. 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 resistenze significative legate alla preservazione della sovranità nazionale¹³⁴. 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 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, anche con riguardo all’ecosistema digitale. 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 europei¹³⁵. 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 europeo¹³⁶. Senza dover guardare alle difficoltà di tali particolari Paesi, applicare il concetto di sovranità digitale all’Unione

¹³³ B. Marchetti, *L’esecuzione della regolazione digitale dell’Unione europea e il ruolo della Commissione*, «Rivista trimestrale di diritto pubblico», 4, 2024, p. 1096.

¹³⁴ G. Hulko, J. Kalman e A. Lapsanszky, *The politics of digital sovereignty and the European Union’s legislation: navigating crises*, «Frontiers in Political Science», 7, 2025.

¹³⁵ *Ibidem*.

¹³⁶ *Ibidem*.

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 membri¹³⁷. Si tratta dello storico problema Unionale della crisi di legittimazione dell'ordinamento sovranazionale¹³⁸.

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 globali¹³⁹.

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 poco coordinati e frammentati, diluendo il loro impatto collettivo¹⁴⁰. 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 talora viene descritto come un fattore di maggiore incertezza e complicazione¹⁴¹. È un

¹³⁷ Bundesverfassungsgericht [Corte costituzionale federale], 30 giugno 2009, 123 BVerfGE 267, 380-406.

¹³⁸ *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*, «The Modern Law Review», 59:3, 1996, p. 349.

¹³⁹ *Vienna Declaration and Programme Action*, 2014.

¹⁴⁰ Letta, op. cit.

¹⁴¹ Macchia, op. cit. L'A. 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

percorso che vede già alla sua base la Bussola per la competitività (trattata in precedenza), la quale prende le mosse dai rapporti Letta e Draghi e delinea 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 illustrare le criticità relative a 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 fattuale¹⁴². 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***

scostamenti e deviazioni, più tornano a regolare controllare», in S. Cassese, *Regolazione e concorrenza*, in *Regolazione e concorrenza*, a cura di G. Tesaurò e M. D'Alberti, Bologna, 2000, p. 23.

¹⁴² *Ibidem*.

affrettata né presentata senza un’adeguata valutazione, consultazione e analisi d’impatto”¹⁴³.

L’uso attuale dell’*omnibus* mostra invece un modello ricorrente caratterizzato da carenza di evidenze empiriche, assenza di analisi comparative, consultazioni ristrette 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 diverse¹⁴⁴.

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 pubblica¹⁴⁵. 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.

Più in particolare, la proposta di regolamento *Omnibus* per l’IA¹⁴⁶ presenta criticità riconducibili a un approccio orientato all’alleggerimento degli oneri di compliance piuttosto che al miglioramento strutturale della competitività¹⁴⁷. Tra i profili più problematici: il rinvio dell’applicazione delle norme sui sistemi ad alto rischio, con

¹⁴³ 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.

¹⁴⁴ Corte di Giustizia UE, *Repubblica Ceca v Parlamento e Consiglio*, C-482/17, EU:C:2019:1035, dicembre 2019.

¹⁴⁵ *Ibidem*.

¹⁴⁶ COM/2025/836 final.

¹⁴⁷ Federation of European Data and Marketing, *Position paper on Digital & AI Omnibus Proposal*, 4 febbraio 2026.

scadenze al 2027-2028, che ha sollevato le preoccupazioni dell’EDPB e dell’EDPS¹⁴⁸; l’ampliamento della clausola di *grandfathering*¹⁴⁹; l’eliminazione dell’obbligo di registrazione per determinati sistemi IA¹⁵⁰; l’estensione del trattamento di categorie particolari di dati personali a tutti i sistemi e modelli IA¹⁵¹; e l’introduzione di un approccio soggettivo alla definizione di “dati personali”, con il rischio di escludere interi settori dall’ambito del GDPR¹⁵².

Lette congiuntamente, le modifiche rivelano uno spostamento da un modello centrato sui diritti a uno marcatamente pro-industria: privilegiando il controllo dei risultati invece di investire nei fattori strutturali della competitività (capitale, potenza di calcolo, dati di qualità e competenze), l’UE rischia di compromettere la propria “sovranità cognitiva”, favorendo l’adozione acritica di tecnologie sviluppate altrove¹⁵³. L’uso di procedure rapide senza adeguata consultazione pubblica ha sollevato dubbi sulla stessa trasparenza democratica¹⁵⁴. Lo studio del Parlamento europeo conferma che le modifiche possono ridurre l’eccesso di conformità, ma rischiano di generare maggiore incertezza giuridica¹⁵⁵. Il dibattito parlamentare si sta orientando verso scadenze certe e il ripristino dell’obbligo di registrazione, come proposto dalla Presidenza cipriota del Consiglio¹⁵⁶. L’efficacia dell’*AI Act* dipenderà dall’attuazione negli Stati membri, con rischi di *gold-plating*, divergenze interpretative e frammentazione istituzionale¹⁵⁷.

Quanto sopra delineato sembra, peraltro, contraddire l’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 europea¹⁵⁸. La dichiarazione si focalizza, peraltro, anche

¹⁴⁸ 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).

¹⁴⁹ *Ibidem*.

¹⁵⁰ N. Rangone, *The Paradoxes of the European Union’s AI Regulation*, «The Regulatory Review», in corso di pubblicazione.

¹⁵¹ *Ibidem*.

¹⁵² B. Lazarotto, *The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite*, «MediaLaws», 19 dicembre 2025.

¹⁵³ Rangone, op. cit.

¹⁵⁴ Si veda <https://www.ombudsman.europa.eu/en/press-release/it/215989>.

¹⁵⁵ 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.

¹⁵⁶ M. Niestadt, *Digital Omnibus on AI*, EPRS, European Parliamentary Research Service, PE 782.651, febbraio 2026.

¹⁵⁷ Si veda <https://digital-strategy.ec.europa.eu/it/policies/market-surveillance-authorities-under-ai-act>.

¹⁵⁸ 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>.

sull'importanza di un panorama regolatorio chiaro, prevedibile ed equo¹⁵⁹ – 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 software¹⁶⁰. Tale impostazione si scontra però con una realtà difficile: come si è visto, permane una forte dipendenza da grandi piattaforme digitali 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 economica¹⁶¹.

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

L'analisi svolta consente alcune prime conclusioni che riteniamo utili a impostare una politica di sistema per il digitale europeo, nonostante si presentino come un elenco di auspicabili direttrici di intervento, senza indicazioni di priorità.

Al di là di una situazione complessiva di difficoltà dell'industria UE nella competizione 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.

Inoltre, è importante ribadire una ulteriore evoluzione della strategia europea per il digitale: 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 (avviando programmi di R&S e di promozione degli investimenti), da qualche tempo, accanto a questi obiettivi, ne sono emersi altri legati ai temi della difesa e della sicurezza, ad attestare la dimensione geopolitica che sempre più le tecnologie e i mercati digitali stanno assumendo.

¹⁵⁹ *Ibidem*.

¹⁶⁰ B.C. Larsen, *The Geopolitics of AI and the Rise of Digital Sovereignty*, Brookings, 8 dicembre 2022.

¹⁶¹ 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).

In questo complesso contesto, l'UE ha iniziato a reagire – finalmente con un approccio a più ampio spettro – a questa situazione di difficoltà¹⁶², aumentando sia il numero di settori digitali sia la tipologia 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*. 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 delle industrie a rete (*utilities*) a lungo caratterizzate – in Europa – dal monopolio dello Stato (energia, trasporti e, in minor misura, TLC). Ne deriva che il paradigma regolatorio pro-concorrenziale delineato dal *Digital Markets Act* (DMA) – che correttamente riprende una impostazione asimmetrica¹⁶³, va affiancato da interventi di politica industriale per il digitale.

Inoltre, la semplificazione della normativa in materia di digitale, invero assai articolata e complessa, è senz'altro un percorso necessario, al fine di accrescere l'efficacia delle azioni pro-concorrenziali e di sviluppo di capacità industriale europea 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*. Più in generale, il termine “semplificazione” rischia di essere utilizzato come un *jolly* retorico: la vera questione non è se regolare, ma come regolare. La semplificazione più efficace e necessaria è quella derivante da una visione complessiva di sistema che conduca al coordinamento e alla razionalizzazione delle politiche pubbliche per il digitale, sulla base di evidenze empiriche. L'obiettivo da evitare è anche quello di sovrapporre nuovi interventi a un quadro già ipertrofico, focalizzandosi invece sull'armonizzazione in sede di attuazione.

¹⁶² In realtà, la politica dell'UE in materia di digitale ha una storia pluridecennale, 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 infatti 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 risultate inefficaci a risolvere il gap di competitività del *Made in Europe*, per i motivi di cui si dirà.

¹⁶³ 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 a un nuovo paradigma regolamentare per i mercati digitali, necessita quella politica industriale di sistema, cui si è fatto cenno prima.

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 serie (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.

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 (a cominciare da quella pubblica), differenziando le fonti di approvvigionamento, ad evitare – per quanto possibile – situazioni di *lock in*¹⁶⁴. In questa prospettiva, ad esempio, 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 precisione¹⁶⁵. Tuttavia,

¹⁶⁴ In tale direzione, si segnala il *paper* del Tony Blair Institute for Global Change, *Sovereignty in the Age of AI: Strategic Choices, Structural Dependencies and the Long Game Ahead*, 2026.

¹⁶⁵ 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.

tali applicazioni verticali richiedono anche l'accelerazione nella realizzazione dei *Common European Data Spaces* settoriali, il cui ritardo rischia di vanificare il vantaggio competitivo europeo nei domini applicativi.

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 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, e di orchestrare segmenti dell'ecosistema, 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*. Tuttavia, le piattaforme digitali, intese sia come servizio sia come "infrastruttura di controllo", rappresentano un elemento chiave di vantaggio competitivo: è quindi essenziale che si sviluppino, per quanto possibile e nei contesti critici, anche piattaforme e orchestratori europei, affinché gli investimenti in infrastrutture strategiche non perdano la loro valenza di autonomia.

Un'ulteriore direttrice della politica digitale UE riguarda infatti anche 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 e 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. 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, tra gli altri, l'*Industrial Acceleration Act*, il *Cloud and AI Development 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 risultati 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*). A livello nazionale, il PNRR ha finanziato in diversa misura tutti i profili del digitale, ma la sfida, non semplice, è ora quella di tradurre questi investimenti in capacità strutturali durature e coordinate a livello europeo.