

2/2026 anteprima

Rivista di diritto dei media

ISSN 2532-9146

Le proposte di riforma dei Digital Omnibus tra deregolamentazione e interventi correttivi

Matteo Paolanti

Sommario

1. Il Digital Package come elemento di discontinuità in un contesto unitario. – 2. Le finalità generali e la struttura del Digital Omnibus. – 2.1 Il contenuto del Digital Omnibus. Un risultato farraginoso. – 3. La (fu) proposta di Digital Omnibus on AI. – 4. Una riflessione critica sul futuro digitale europeo. – 4.1 Il confronto con i modelli extra-UE: la visione di Stati Uniti e Cina. – 4.2 Il cittadino alla prova degli effetti della regolamentazione europea. – 4.3 Questioni ordinamentali e politiche aperte. – 5. Considerazioni conclusive.

1. Il Digital Package come elemento di discontinuità in un contesto unitario

Negli ultimi anni l'UE ha tentato di imporsi come modello su più livelli. Nata per essere un organismo rivolto essenzialmente a fini di integrazione economica¹, col tempo ha cercato di acquisire un maggior peso in termini più strettamente geopolitici, fino a occuparsi anche di tematiche sociali e di interesse universale (si pensi alle normative ambientali).

Questi cenni, che sintetizzano quella che si potrebbe definire l'evoluzione della “*mission*” storica dell'UE, sono utili a incorniciare le vicende che l'hanno riguardata nel decennio appena trascorso. Dal 2016 in poi, infatti, grazie all'importantissimo traguardo rappresentato dall'approvazione del Regolamento Generale sulla Protezione dei Dati Personali (d'ora in poi

¹ A questo riguardo si veda l'art. 2 del Trattato di Roma sull'istituzione della Comunità economica europea che recitava: «La Comunità ha il compito di promuovere, mediante l'instaurazione di un mercato comune e il graduale ravvicinamento delle politiche economiche degli Stati membri, uno sviluppo armonioso delle attività economiche nell'insieme della Comunità, un'espansione continua ed equilibrata, una stabilità accresciuta, un miglioramento sempre più rapido del tenore di vita e più strette relazioni fra gli Stati che ad essa partecipano».

GDPR), si può dire che si sia aperta un'era particolare della regolamentazione digitale in seno al contesto europeo². Tuttavia, sarebbe riduttivo minimizzare la questione in questi termini: il legislatore europeo, difatti, non si è limitato a gestire dei fenomeni di rilevanza giuridica, ma ha impresso una *policy* generale alla sua attività, affinché nel menzionato GDPR, come anche negli altri atti che lo hanno succeduto (le normative in tema di cybersicurezza, gli interventi relativi ai media digitali, Digital Services Act e Digital Markets Act, fino a giungere al più recente AI Act), potesse intravedersi la volontà di perseguire quei valori liberali, democratici e sociali su cui la stessa UE trova origine e fondamento³.

In questa ottica, a cavallo tra un passato ingombrante, un presente complesso e un futuro poco chiaro, si pone il c.d. “Digital Package” (formato da Digital Omnibus e Digital Omnibus on AI), ossia un tentativo ambizioso delle istituzioni europee per semplificare il comparto legislativo nell’ambito digitale⁴.

Il suo annuncio⁵ e la sua prima esposizione al pubblico di certo non hanno lasciato inerti i commentatori: è sembrato, a prima vista, che l’UE volesse tradire più di un decennio di attività ritrattando su numerose norme create nei tempi più recenti⁶. Inoltre, hanno contribuito a generare il clamore iniziale e le conseguenti perplessità sia l’ampiezza dell’oggetto dell’intervento⁷, sia la centralità attribuita ai temi della governance dei dati e dell’intelligenza artificiale, ambiti già caratterizzati da un elevato livello di attenzione politica, economica e mediatica.

Per quanto tale intervento non stupisca del tutto un osservatore italiano – si potrebbe azzardare a dire che l’UE abbia scoperto il potere dei “decreti milleproroghe” e dei “decreti omnibus”, strumenti fin troppo cari al

² Per una ricostruzione diacronica di questo percorso si rimanda a S. Calzolaio, *Protezione dei dati personali* (voce), in *Dig. disc. pubbl.*, Torino, 2017.

³ L’approvazione del GDPR (regolamento (UE) 2016/679) va inquadrata come esito di un percorso di “costituzionalizzazione” europea della protezione dei dati, fondato sull’art. 8 CDFUE e sull’art. 16 TFUE, che ne hanno fatto un diritto fondamentale autonomo. Per la ricostruzione, v. nota *supra* 1.

⁴ Per una importante trattazione introduttiva delle questioni qui affrontate, si veda E. M. Tripodi, *Il “Digital Omnibus”: semplificazione (o deregolamentazione) del contesto digitale europeo?*, in *Rivista di diritto di internet*, 1, 2026, 3 ss.

⁵ Commissione europea, Digital Omnibus on AI Regulation Proposal, 19 novembre 2019.

⁶ R. Mahieu, *The Ominous Omnibus: Dismantling the Right of Access to Personal Data*, in *VerfBlog*, 3 dicembre 2025; H.C.H. Hofmann, *This Is Not Simplification: How to Simplify the Digital Acquis Without Undermining Rights*, in *VerfBlog*, 3 gennaio 2026.

⁷ Come si può leggere dal testo condiviso dalla Commissione, esso va a toccare quasi tutte le normative “digitali” che sono state introdotte dalle Commissioni Juncker e Von der Leyen I.

nostro ordinamento nazionale⁸ – è ancora corretto affermare che sul contenuto di tali proposte vi siano perplessità e dubbi. In particolare, appare complesso decifrarne la scelta politica che ne è alla base, che potrebbe essere sia di mera semplificazione ed efficientamento del sistema, come pure di deregolamentazione a seguito di nuove necessità di stampo economico-politico.

Seguendo questa traccia introduttiva, il presente contributo si pone l'obiettivo di analizzare e provare a comprendere i cambiamenti in corso nell'ordinamento digitale europeo, cercando di individuare gli effetti delle scelte del legislatore, con una prospettiva al futuro dell'Europa tecnologica, la quale non può permettersi di abbandonare la corsa per il progresso a favore di altri Stati. Nello specifico, verranno analizzate le modifiche afferenti al primo grande impianto legislativo dell'Europa digitale contemporanea – ossia il GDPR e le normative satelliti (in particolare il Data Act del 2023) – e all'ultimo intervento la cui applicazione è ancora sospesa per alcune parti, cioè l'AI Act. Nel considerare tali interventi come momenti emblematici dell'evoluzione della legislazione digitale europea nell'ultimo decennio, si intende verificare se la riforma si configuri quale un mero ammodernamento del quadro giuridico vigente ovvero se il cambiamento in corso assuma una portata più ampia rispetto alle aspettative iniziali.

2. Le finalità generali e la struttura del Digital Omnibus

Guardando al contesto in cui si inserisce la COM(2025) 837 (d'ora in poi Digital Omnibus o DO), è opportuno primariamente distinguere le questioni oggetto di analisi.

Andando per ordine, come accennato in precedenza, la proposta di Digital Omnibus emerge da un più ampio impegno della Commissione von der Leyen II, la quale, sin dal suo insediamento, ha confermato la promessa di intervenire attivamente nell'ambito delle strutture digitali⁹. Il DO si caratterizza per un cambio di prospettiva che va verso una rinnovata “semplificazione” della normativa europea. Tale obiettivo, però, non emerge dal nulla; il diverso impegno strategico europeo si trova esplicitato in alcuni

⁸ È noto che, soprattutto negli ultimi decenni, il legislatore abbia usufruito, almeno nell'ambito italiano, degli strumenti suddetti per scopi multiformi. A questo riguardo, risalendo nel tempo, si vedano: N. Lupo, *Decreto legge e manutenzione legislativa: i decreti legge «milleproroghe»*, in A. Simoncini (a cura di), *L'emergenza infinita. La decretazione d'urgenza in Italia*, Macerata, 2006, spec. 180 ss.; G. Tarli Barbieri, *Analisi di alcuni casi emblematici di patologie del decreto legge milleproroghe*, in *Osservatorio sulle fonti*, 2, 2008.

⁹ Si veda a riguardo: Commissione europea, *Speech by President von der Leyen at the European Parliament Plenary on the new College of Commissioners and its programme*, 27 novembre 2024.

documenti programmatici: tra di essi, non si possono non ricordare i rapporti Draghi (2024) e Letta (2024)¹⁰, fondamento della comunicazione “*A simpler and faster Europe*” (COM(2025)47 final)¹¹ nonché delle conclusioni del Consiglio europeo del 23 ottobre 2025 che hanno richiamato l’urgenza di un’agenda ambiziosa di semplificazione e migliore regolamentazione¹². La Commissione ha fatto notare come l’accumulo di norme (particolarmente rilevante dopo la pandemia da Covid-19) abbia avuto effetti avversi sulla competitività del mercato europeo. Per tale motivo – e non solo – essa identifica nel Digital Omnibus un primo passo per ottimizzare l’applicazione dell’*acquis* digitale, con l’obiettivo di garantire costi inferiori e vantaggi competitivi alle imprese responsabili che abbiano la volontà e i mezzi di gestire questo ulteriore cambiamento nel panorama giuridico europeo¹³. Questa premessa è desumibile chiaramente dalla relazione illustrativa della bozza di riforma. A tal riguardo, il documento è formato da tre componenti fondamentali che si integrano reciprocamente per fornire una visione completa della proposta normativa. La prima parte è costituita dalla relazione illustrativa, dove la Commissione evidenzia l’accumulo progressivo di normative digitali adottate negli ultimi anni e la contestuale creazione di esternalità sia positive che negative. Per quanto l’UE abbia trasmesso al resto del mondo l’aspirazione a una gestione consapevole e democratica della nuova risorsa digitale, allo stesso tempo si ritiene che questa azione composita abbia finito per generare eccessiva complessità giuridica, rappresentata da sovrapposizioni normative, inflazione legale e definizioni non perfettamente allineate tra i diversi strumenti legislativi¹⁴. A ciò si aggiunge il particolarismo ordinamentale degli Stati membri, il quale, nonostante l’uso delle fonti di integrazione diretta – i regolamenti – non ha potuto evitare che si creassero squilibri dovuti alle esigenze differenziate dei diversi contesti nazionali¹⁵.

¹⁰ M. Draghi, *The future of European competitiveness*, 9 settembre 2024; E. Letta, *Much more than a market*, aprile 2024.

¹¹ Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions “*A simpler and faster Europe: Communication on implementation and simplification*”, COM/2025/47 final, 11 febbraio 2025.

¹² Conclusioni del Consiglio europeo, EUCO 18/25, Bruxelles, 23 ottobre 2025, punti 48-52.

¹³ Le ragioni su cui muove l’azione della Commissione possono essere riscontrate nella Relazione introduttiva alla proposta di Regolamento del Digital Omnibus (spec. 1-10).

¹⁴ *Ibid.*

¹⁵ L’ultimo dei riferimenti a cui si fa eco non può che essere rappresentato dalla recente legge italiana n. 132/2025 in materia di intelligenza artificiale. Essa, pur riprendendo in gran parte l’impianto dell’AI Act e la sua *policy*, si scontra inevitabilmente con le necessità particolari dell’ordinamento italiano. Cfr. M. Iaselli, *Commentario alla legge sull’intelligenza*

La seconda parte del documento è rappresentata dal testo normativo vero e proprio, che si articola secondo lo schema tipico degli atti legislativi dell'Unione: un preambolo, contenente i riferimenti ai trattati e i "considerando" (le c.d. *whereas clauses*), seguito dal dispositivo, che in questo caso è suddiviso in soli undici articoli. Il *corpus* normativo costituisce il cuore operativo dell'intervento e si distingue per la sua natura tecnica e per l'approccio selettivo alle modifiche proposte.

Infine, la terza parte è costituita dalla dichiarazione legislativa, finanziaria e digitale, che evidenzia le implicazioni della proposta sotto il profilo della compatibilità con il quadro finanziario pluriennale, degli impatti digitali e delle modalità di implementazione. Questa sezione, che potrebbe apparire di primo acchito di interesse puramente burocratico o economico, in realtà si rivela particolarmente rilevante, in quanto delinea gli impatti economici attesi e le modalità di monitoraggio dell'efficacia delle misure proposte.

2.1 Il contenuto del Digital Omnibus. Un risultato farraginoso

Venendo ora al vero e proprio testo giuridico, l'art. 1 costituisce il nucleo centrale del progetto, ed è dedicato alle modifiche al regolamento (UE) 2023/2854 (*Data Act*). Questa voce si compone di svariati paragrafi che introducono emendamenti sistematici e di grande portata al suddetto regolamento, consolidando e riunendo al suo interno le disposizioni di altri tre atti normativi: il regolamento (UE) 2018/1807 sulla libera circolazione dei dati non personali, il regolamento (UE) 2022/868 sulla governance dei dati e la direttiva (UE) 2019/1024 sui dati aperti.

Per ragioni di chiarezza espositiva, le innovazioni apportate dall'art. 1 possono essere organizzate in distinti blocchi tematici. Il primo (paragrafi 1-2) riguarda l'aggiornamento dell'ambito di applicazione del *Data Act* e delle sue definizioni, per accogliere i nuovi capitoli che verranno inseriti. Un secondo blocco (paragrafi 3-4) introduce una nuova norma che consente ai detentori di dati di rifiutare la divulgazione di segreti commerciali a un utente quando esiste un rischio elevato di acquisizione, uso o divulgazione illeciti a paesi terzi o entità sotto il loro controllo, soggetti a giurisdizioni con protezioni più deboli rispetto a quelle disponibili nell'Unione¹⁶. Un

artificiale. Principi, governance e applicazioni settoriali. Legge 23 settembre 2025, n. 132, Roma, 2025; V. Franceschelli - A. Sirotti Gaudenzi, La legge italiana sull'Intelligenza Artificiale. Commento alla Legge 23 settembre 2025, n. 132, Rimini, 2025; A. F. Uricchio, Intelligenza artificiale tra regolazione ed esperienze applicative. Prime considerazioni dopo l'approvazione della legge italiana su AI, in Il diritto amministrativo, 1, 2026.

¹⁶ Si potrebbe ipotizzare che tale nuova regola trovi le sue radici anche, se non soprattutto,

terzo blocco tematico, poi, restringe l'ambito di applicazione del capitolo V del Data Act dalle "esigenze eccezionali" alle sole "emergenze pubbliche", eliminando i preesistenti articoli 14 e 15 del suddetto regolamento e creando una nuova norma (art. 15a) per le richieste di *disclosure* avanzate durante le emergenze pubbliche. La modifica è accompagnata da aggiustamenti sistematici dei riferimenti normativi e da una semplificazione e chiarificazione del linguaggio prescrittivo. Il quarto blocco introduce specifiche esenzioni al capitolo VI del Data Act sul passaggio tra servizi di elaborazione dati (il c.d. *switching* tra servizi *cloud*¹⁷). Il risultato di tale operazione è l'approntamento di un regime più "leggero" sia per i servizi di elaborazione dei dati personalizzati che per i servizi forniti da piccole e medie imprese (PMI) e piccole imprese a media capitalizzazione (SMC). Parallelamente, l'art. 1, par. 17 elimina l'art. 36 della precedente normativa concernente gli obblighi per i fornitori di *smart contract* di conformarsi a requisiti essenziali in materia di esecuzione di accordi di condivisione di dati. Ad ogni buon conto, la modifica più massiccia introdotta dal gargantuesco art. 1 è quella che introduce i titoli VIIa, VIIb e VIIc nel nuovo Data Act risultante dalla riforma. Nello specifico, si tratta dell'integrazione dei regimi giuridici al momento contenuti nel Data Governance Act. Vengono inserite, come nuovo titolo VIIa, le discipline relative ai servizi di intermediazione dei dati e alle organizzazioni per l'altruismo dei dati¹⁸, con modifiche sostanziali alla loro struttura; con gli altri due titoli (VIIb e VIIc) si introducono norme in tema di circolazione dei dati e di uso da parte di strutture pubbliche.

Tra le numerose innovazioni introdotte dal VIIa – il cui apparato normativo si estende fino all'art. 32g, a testimonianza dell'ampiezza degli interventi apportati – meritano particolare attenzione, da un lato, la riforma del regime di notifica applicabile ai fornitori di servizi di intermediazione dei dati, che da obbligatorio viene ricondotto a un modello di adesione volontaria; dall'altro, la sostituzione dell'obbligo di separazione giuridica dei ser-

nel modificato assetto geopolitico mondiale, il quale vede l'UE sempre più accerchiata da potenze illiberali che non condividono le stesse procedure e i medesimi standard di protezione delle sfere giuridiche individuali. Cfr. D. Alic, *The role of data protection and cybersecurity regulations in artificial intelligence global governance: A comparative analysis of the European Union, the United States, and China regulatory framework*, CEU, 2021.

¹⁷ Con esso s'intende il passaggio originario (da proprietario dei dati a servizio *cloud*) o derivato (da servizio *cloud* a servizio *cloud*) di dati o documenti in una struttura *cloud*. Il Data Act si è particolarmente occupato del fenomeno.

¹⁸ Con questo termine particolare si fa riferimento alla condivisione volontaria e gratuita di dati personali o non personali da parte di individui e imprese per finalità di interesse generale, come la ricerca medica, il contrasto ai cambiamenti climatici o il miglioramento dei servizi pubblici (art. 2 DGA).

vizi di intermediazione dei dati con un onere di separazione funzionale¹⁹. Con il nuovo titolo VIIb – il più breve dei tre, composto dal solo art. 32h – viene invece incorporato nel Data Act il divieto di imporre requisiti di localizzazione per i dati non personali all'interno dell'Unione, precedentemente previsto nel Regolamento sulla libera circolazione dei dati non personali. Resta fermo l'obbligo di notifica alla Commissione, mentre viene soppresso il punto di informazione unico nazionale presso il quale gli Stati membri avrebbero dovuto pubblicare i requisiti per la localizzazione dei dati.

Tuttavia, la parte più complessa dell'art. 1 riguarda l'introduzione del nuovo titolo VIIc (artt. 32i ss.). Ossia la riordinazione e la riforma del regime giuridico in materia di riutilizzo dei dati e dei documenti detenuti dagli enti del settore pubblico, che unisce le disposizioni del capitolo II del Data governance Act e della Direttiva sui dati aperti.

Le modifiche si pongono l'obiettivo di armonizzare la definizione di dati e documenti fornendo una netta distinzione tra contenuti digitali e contenuti non digitali. Vengono poi introdotti principi comuni di non discriminazione applicabili alla condivisione di dati governativi aperti e di determinate categorie di dati protetti, nonché il divieto di accordi esclusivi su possibili utilizzi preferenziali. In particolare, la novità significativa consiste nella possibilità per gli enti del settore pubblico di stabilire condizioni diverse e applicare tariffe più elevate per il riutilizzo da parte delle imprese designate come *gatekeeper*²⁰ ai sensi del Digital Markets Act²¹. L'art. 1 si chiude con una serie di disposizioni concernenti l'European data innovation Board (EDIB). L'EDIB, organo tecnico consultivo, sarà incaricato di supportare la Commissione nell'assicurare un'applicazione coerente del Data Act e di operare quale sede di coordinamento per l'elaborazione e l'armonizzazione delle politiche nel settore dell'economia dei dati.

Prima di procedere con il resto della trattazione del DO, merita dedicare alcune sintetiche considerazioni allo stile redazionale e alla qualità della tecnica normativa impiegata nell'art. 1. La disposizione di apertura del Digital Omnibus, con i suoi paragrafi densi di modifiche incrociate, rappresenta un esempio paradigmatico di ipertrofia normativa, intesa non solo come incremento quantitativo della regola, ma come stratificazione di rin-

¹⁹ Le due diverse previsioni legislative menzionate sono riconducibili ai novellati artt. 32e, par. 1, e 32f. Si rimanda alla normativa per comprendere al meglio come si presenti questa "separazione funzionale".

²⁰ Sulle scelte adottate dalla Commissione a riguardo dell'elezione a "*gatekeeper*" di alcune società del settore tecnologico si rimanda a: Commissione europea, Gatekeepers Portal.

²¹ Nell'ottica della lotta al monopolio delle c.d. "*Big Tech*" e della protezione della libera concorrenza, principio cardine dell'UE, l'art. 32k e seguenti cercano di contrastare la tendenza all'abbandono di dati sensibili e di valore alle piattaforme private provenienti da Paesi terzi.

vii, sostituzioni e integrazioni che finisce per disarticolare l'unità semantica della disposizione. La tecnica qui utilizzata del "consolidamento per incorporazione" comporta che il contenuto effettivo della norma non sia ricavabile dal testo che la esprime, ma debba essere ricostruito attraverso una lettura coordinata con una pluralità di atti preesistenti, trasformando l'attività interpretativa in un'operazione di vera e propria filologia giuridica. Ne deriva uno spostamento del baricentro della normazione: dalla formulazione diretta e autosufficiente della regola alla sua completa ricostruzione *ex post* da parte dell'interprete. Ciò incide non soltanto sulla chiarezza della disposizione, ma sull'accessibilità stessa dei diritti soggettivi, valore che – pur non sempre esplicitato – si collega strettamente ai principi di certezza, di affidamento e di conoscibilità della disciplina applicabile²². La distanza che si crea tra testo e norma effettiva si traduce in un aggravio dell'onere cognitivo posto a carico dei destinatari e in un ampliamento del margine di discrezionalità interpretativa, con il rischio di soluzioni applicative disomogenee. In settori a forte densità tecnico-regolatoria come quello digitale, tale assetto risulta particolarmente preoccupante: la funzione orientativa della norma, essenziale per operatori economici chiamati a pianificare condotte innovative e investimenti rilevanti, viene indebolita proprio nel momento in cui dovrebbe operare con maggiore intensità. La complessità non appare qui come effetto inevitabile della materia regolata, bensì come esito di una scelta di tecnica legislativa che sacrifica esigenze di trasparenza e intelligibilità, rendendo la disciplina difficilmente padroneggiabile persino per gli operatori specializzati e, di fatto, inaccessibile al cittadino²³. Andando avanti con la trattazione del testo legislativo, non è possibile intravedere un metodo diverso da quello su cui si è basata la disposizio-

²² F. Pizzetti - S. Calzolaio - A. Iannuzzi - E. Longo - M. Orofino, *La regolazione europea dell'intelligenza artificiale nella società digitale*, Torino, 2025, *passim*.

²³ In un'ottica comparativa con un ordinamento prossimo, la dottrina italiana ha da tempo posto in evidenza come la proliferazione normativa, la frammentazione delle fonti e il ricorso a tecniche legislative di particolare complessità – soprattutto nell'ambito dell'ordinamento interno, frequentemente caratterizzato dall'adozione di strumenti legislativi onnicomprensivi – incidano negativamente sulla qualità della legislazione. Tale problematica è oggetto di un dibattito consolidato in seno alla dottrina italiana da oltre trent'anni, che si è progressivamente attrezzata per affrontare le criticità derivanti da questo scenario. *Ex multis*, Zaccaria ha sottolineato, in un'opera collettanea redatta in qualità di Presidente del Comitato per la legislazione della Camera dei deputati, l'esistenza di «un rapporto diretto tra la qualità della lingua italiana nella scrittura delle leggi e gli obiettivi politici del legislatore». Tale principio trova riconoscimento anche sul piano costituzionale, come attestato dalla giurisprudenza della Corte costituzionale in materia di art. 5 c.p., che riconduce allo Stato il dovere di adottare norme chiare e comprensibili, idonee a consentire al cittadino di discernere ciò che gli è consentito e ciò che gli è vietato. Alla luce di tali considerazioni, si potrebbe sostenere che, mediante il Digital Omnibus, l'UE stia ripercorrendo un percorso ampiamente sperimentato dal legislatore italiano. Cfr. R. Zaccaria (a cura di), *La buona scrittura delle leggi*, Camera dei deputati, 2011.

ne precedentemente analizzata. Mentre l'art. 2 introduce nel regolamento (UE) 2018/1724 (*Single Digital Gateway*) ulteriori riferimenti pertinenti ai servizi di intermediazione dei dati in sede di avvio e chiusura di un'impresa, gli artt. 3, 4 e 5 sono dedicati alle correzioni del quadro normativo sulla protezione dei dati personali e sulla privacy.

A questo riguardo, il primo dei tre introduce modifiche al regolamento (UE) 2016/679 (GDPR), articolate in quindici paragrafi che affrontano questioni tra loro diverse²⁴. Al par. 1 viene precisata la nozione di dato personale, chiarendo che un'informazione non può essere qualificata come tale qualora non sussistano mezzi ragionevolmente utilizzabili per identificare, direttamente o indirettamente, la persona fisica cui essa si riferisce²⁵. Il terzo paragrafo introduce due ipotesi di deroga al divieto generale di trattamento di dati personali afferenti a categorie particolari. La prima permette il trattamento di dati biometrici qualora esso risulti necessario ai fini della conferma dell'identità dell'interessato, a condizione che i dati e gli strumenti impiegati per tale verifica rimangano sotto il controllo esclusivo del medesimo²⁶. La seconda riguarda il trattamento residuale di categorie particolari di dati personali, funzionale allo sviluppo e al funzionamento di sistemi o modelli di intelligenza artificiale²⁷.

I paragrafi successivi approfondiscono l'esercizio abusivo del diritto di accesso da parte degli interessati all'obbligo di informazione del titolare del trattamento nei confronti degli interessati, ai requisiti per il processo decisionale individuale automatizzato e agli obblighi di notifica delle violazioni dei dati personali all'autorità di controllo competente. Quest'ultimo aspetto, poi, introduce una modifica significativa: ai sensi del riformato art. 33, par. 1, GDPR, la notifica diventa obbligatoria solo se una violazione dei dati è suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, e il termine per la notifica viene esteso a novantasei ore²⁸. Procedendo nell'analisi del considerevole testo della norma, così come accaduto con l'art. 1, vengono inserite nuove previsioni all'interno della

²⁴ Come si può notare anche qui, la tecnica "*omnibus*" riguarda la maggioranza degli atti normativi di materia digitale promulgati negli ultimi anni dall'UE. Per un giudizio su questa tecnica si rimanda alla discussione sulla qualità dell'art. 1 e alla nota 23.

²⁵ Si veda art. 3, par. 1, lett. a), Digital Omnibus. Per un raffronto: «*Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.*».

²⁶ Art. 3, par. 3, lett. a).

²⁷ Art. 3, par. 3, lett. b).

²⁸ Art. 3, par. 8, lett. a).

struttura del Regolamento. Nello specifico, tre nuove norme, gli artt. 88a, 88b e 88c, le quali si rivelano molto interessanti per il loro contenuto.

Andando in ordine, il primo stabilisce il requisito del consenso per la memorizzazione o l'accesso a dati personali sull'apparecchiatura terminale (*device*) di persone fisiche. Tuttavia, a partire dal par. 3 della norma vengono delineate alcune eccezioni per ciò che concerne i dati già incamerati dalle piattaforme o dai fornitori di servizi²⁹. Nelle casistiche eccezionali si applica un regime precauzionale, che mantiene sospeso il dato in attesa di risposta dalla persona fisica, la quale può esprimersi riguardo al suo utilizzo³⁰.

Il successivo art. 88b introduce disposizioni relative alla comunicazione, in forma automatizzata e leggibile da sistemi informatici, delle scelte individuali dell'interessato, nonché all'obbligo per i fornitori di siti web di conformarsi a tali indicazioni una volta resi disponibili standard tecnici idonei a garantirne l'interoperabilità.

La norma si inserisce tra i meccanismi volti a rendere effettivo l'esercizio delle preferenze dell'utente in ambienti digitali caratterizzati da trattamenti automatizzati dei dati, incidendo in particolare sulle pratiche di profilazione, di personalizzazione dei contenuti e delle comunicazioni commerciali. Essa mira a strutturare modalità standardizzate di espressione e trasmissione della volontà dell'interessato, al fine di ridurre l'asimmetria informativa e operativa che connota i rapporti tra utenti e grandi piattaforme digitali, nei quali la selezione di contenuti, servizi e messaggi pubblicitari è frequentemente affidata a processi algoritmici basati su preferenze sia dichiarate sia inferite dal sistema.

Tra le tre disposizioni citate, quella che suscita le maggiori perplessità è tuttavia l'art. 88c, il quale incide anche sull'ambito di applicazione dell'AI Act, con specifico riferimento alle attività di addestramento dei sistemi di intelligenza artificiale. Si legge chiaramente dal testo: «Qualora il trattamento dei dati personali sia necessario per gli interessi del titolare del trattamento nel contesto dello sviluppo e del funzionamento di un sistema di IA quale definito all'art. 3, punto 1, del regolamento (UE) 2024/1689 o di un modello di IA, tale trattamento può essere effettuato per motivi di

²⁹ Di seguito il testo del nuovo art. 88a, par. 3: «*Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following: (a) carrying out the transmission of an electronic communication over an electronic communications network; (b) providing a service explicitly requested by the data subject; (c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use; (d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service*».

³⁰ Art. 88a, par. 4, in art. 3, par. 15, DO.

legittimo interesse ai sensi dell'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679». Come si può intuire, si tratta di un'importante deroga rispetto alla regola attuale del consenso preventivo per il trattamento e l'uso specifico di determinati dati, aprendo ad una prima erosione del forte principio consensuale in materia di accrescimento delle capacità computazionali dei sistemi algoritmici complessi, i quali potrebbero così acquisire più facilmente dati su cui svolgere le loro elaborazioni.

Proseguendo, la restante parte della proposta di regolamento presenta una densità prescrittiva inferiore rispetto ai profili sinora esaminati. Ciò nondimeno, essa contiene disposizioni di rilievo che, pur meno articolate sotto il profilo tecnico, si inseriscono in continuità con gli ambiti già considerati, contribuendo a definirne in modo più compiuto l'assetto complessivo. Di seguito se ne dà una rapida illustrazione.

L'art. 4 funge da collegamento tra la prima e la seconda parte della proposta di riforma. Vengono introdotte modifiche mirate al regolamento (UE) 2018/1725 (EUDPR), al fine di allineare il suo testo con le numerose modifiche al GDPR introdotte nel già affrontato art. 3. La voce successiva prevede modifiche alla direttiva 2002/58/CE (*ePrivacy Directive*), eliminando l'art. 4 di tale direttiva e aggiungendo un sottoparagrafo dopo l'art. 5(3) che trasferisce nel *corpus* del GDPR le norme sulla memorizzazione e l'accesso ai dati personali dall'apparecchiatura terminale di una persona fisica. Per ciò che concerne gli artt. dal 6 al 9, essi sono ugualmente dedicati all'armonizzazione di numerose normative: a puro scopo indicativo, l'art. 6 prevede che la segnalazione degli incidenti (*data breaches*), obbligatoria ai sensi della Direttiva NIS2³¹, debba essere effettuata attraverso il nuovo punto di accesso unico (ESAP). Gli artt. 7, 8 e 9, poi, estendono l'obbligo di utilizzo del punto di accesso unico rispettivamente al Regolamento eIDAS³², al Regolamento DORA³³ e alla Direttiva CER³⁴.

³¹ A puro scopo informativo, La direttiva (UE) 2022/2555 (*Network and Information Security 2 – NIS2*) rappresenta il principale strumento dell'Unione Europea volto a conseguire un livello comune elevato di cybersicurezza delle reti e dei sistemi informativi, sostituendo e ampliando il quadro delineato dalla precedente direttiva del 2016 (appunto, la c.d. "NIS1").

³² Il regolamento (UE) 910/2014 (*eIDAS*) ha avuto il merito di istituire un quadro giuridico vincolante per l'identificazione elettronica e i servizi fiduciari nelle transazioni elettroniche nel mercato interno, definendo regole tecniche e giuridiche per firme elettroniche, sigilli, marche temporali e servizi di autenticazione.

³³ Il regolamento (UE) 2022/2554 – *Digital Operational Resilience Act (DORA)* ha contribuito a definire un quadro armonizzato di requisiti di *information and communication technology* (ICT) risk management, di governance della resilienza operativa, di segnalazione degli incidenti e di stress test per le istituzioni finanziarie e i servizi correlati, nonché per i fornitori terzi considerati critici per la funzione operativa delle entità finanziarie.

³⁴ Completa il quadro la direttiva (UE) 2022/2557 – *Critical Entities Resilience (CER)*, che

L'art. 10 contiene disposizioni sulle varie abrogazioni e sulle clausole transitorie per l'adeguamento dei mezzi e delle infrastrutture alla nuova normativa – sempre che la proposta rimanga così com'è. Il primo paragrafo abroga il regolamento (UE) 2019/1150 (Regolamento P2B), considerato di rilevanza residuale alla luce di norme recenti che coprono in gran parte le stesse questioni. In deroga, il secondo paragrafo prevede che alcune disposizioni della normativa P2B continueranno ad applicarsi fino al 31 dicembre 2032, per garantire la certezza giuridica per gli atti contenenti riferimenti incrociati a tali disposizioni. Si noti che *in extremis* sono previsti ulteriori termini di applicazione differenziati per specifiche disposizioni: ad esempio l'art. 5(2) entra in applicazione sei mesi dopo la pubblicazione, mentre alcune norme relative al punto di accesso unico per la segnalazione degli incidenti entrano in applicazione diciotto mesi dopo l'entrata in vigore del Regolamento.

Per concludere, l'analisi d'insieme del DO mette in luce un intervento normativo di notevole ampiezza e ambizione sistemica, volto a razionalizzare e accorpare una pluralità di discipline eterogenee nell'ambito dell'economia dei dati e della protezione delle informazioni personali. Tuttavia, tale obiettivo appare perseguito attraverso soluzioni redazionali e strutturali che accentuano la complessità del quadro regolatorio, sollevando interrogativi rilevanti in termini di chiarezza, accessibilità e certezza del diritto. Ne emerge un impianto normativo che, pur aspirando a una maggiore coerenza e armonizzazione, si traduce in un esito drammaticamente farraginoso, la cui effettiva efficacia applicativa e capacità di orientare gli operatori giuridici ed economici resta affidata, in larga misura, al futuro lavoro dell'interprete.

sostituisce la precedente disciplina sulle infrastrutture critiche in settori come l'energia, i trasporti, la sanità, le infrastrutture digitali, etc. CER richiede agli Stati membri di adottare strategie nazionali per identificare e designare tali entità, effettuare valutazioni periodiche dei rischi, adottare misure tecniche, di sicurezza e organizzative proporzionate ai rischi individuati e notificare tempestivamente gli incidenti che minacciano la continuità dei servizi essenziali.

3. La (fu) proposta di Digital Omnibus on AI³⁵

Insieme al Digital Omnibus appena analizzato, la Commissione europea ha presentato un'ulteriore proposta di regolamento, che fa da gemello al precedente.

La COM(2025) 836 final³⁶ (d'ora in poi "Digital Omnibus on AI" o "DOAI") si iscrive nel medesimo percorso tracciato dal provvedimento sopra esaminato e trova la propria ragion d'essere nella sua impostazione riformatrice. Seguendo lo schema già utilizzato, si procede qui a un esame dei contenuti della proposta iniziale di riforma, al fine di evidenziarne gli aspetti più rilevanti. Nel tentativo di avanzare con un'impostazione quanto più possibile schematica – esigenza resa particolarmente avvertibile dalla diffusa complessità che caratterizza il Digital Package – occorre anzitutto rilevare che il DOAI presenta un'estensione inferiore rispetto al DO. Ciononostante, la disciplina incide su una pluralità di ambiti, di notevole rilievo per l'analisi dottrinale. Sebbene la proposta di regolamento si suddividesse in soli tre articoli, una lettura coerente del testo consente di identificare una struttura logica sottostante che organizza le modifiche intorno a sei assi strategici interdipendenti, i quali sono stati immessi in una lunga lista di paragrafi dentro l'art. 1³⁷.

Una delle modifiche più significative avrebbe riguardato il regime di entrata in vigore delle disposizioni, disciplinato dall'art. 113 dell'AI Act. Secondo il testo originario, il capitolo III (concernente i sistemi ad alto rischio³⁸)

³⁵ Il presente paragrafo prende in considerazione la versione del regolamento originariamente proposta dalla Commissione europea. Nel corso del successivo *iter* legislativo, il testo è stato oggetto di modifiche da parte delle istituzioni dell'Unione, che hanno interessato anche alcune delle disposizioni maggiormente rilevanti ai fini della presente analisi, attenuando, in taluni casi, i rischi e le criticità qui evidenziati. Pur tenendo conto di tali modifiche, anche di carattere sostanziale, si ritiene nondimeno opportuno soffermarsi – tra le righe dell'esposizione delle norme qui analizzate – sulla *policy* sottesa alla proposta originaria, in quanto essa consente di cogliere le premesse e gli orientamenti che hanno guidato l'intervento riformatore e che si collegano alle più ampie considerazioni sviluppate nei §§ 4 ss. della presente trattazione.

³⁶ Nel frattempo, modificata, approvata e entrata in vigore come regolamento (UE) 2026/1744.

³⁷ Similmente alla tecnica legislativa usata per il Digital Omnibus, anche per la proposta di regolamento qui in discussione, la Commissione ha optato per accorpare la maggior parte delle norme sotto solo due voci.

³⁸ Ai sensi dell'Allegato III, in combinato disposto con l'art. 6, par. 2, dell'AI Act, rientra nella categoria dei sistemi di IA ad alto rischio un'ampia gamma di applicazioni il cui malfunzionamento può determinare danni significativi. Vi appartengono, tra gli altri, i sistemi di identificazione biometrica e di riconoscimento facciale, i sistemi di social scoring, i *chatbot* impiegati in ambito medico, nonché i sistemi di guida autonoma. Per tali sistemi, l'AI Act prevede un apparato di requisiti particolarmente stringente, che

sarebbe entrato in vigore il 2 agosto 2026 (cosa effettivamente avvenuta), mentre per i sistemi del capitolo I, soggetti a regolamenti di armonizzazione, la data era stata fissata al 2 agosto 2027. La Commissione, col Digital Omnibus on AI aveva intenzione di introdurre un meccanismo innovativo di “*linking* temporale” mediante il quale l’attivazione di queste scadenze sarebbe stata resa condizionata alla previa decisione della Commissione che avesse certificato la disponibilità di misure adeguate di supporto alla conformità dei sistemi³⁹. Una volta che la Commissione avesse adottato la decisione di certificazione, il periodo di applicazione sarebbe iniziato a decorrere: sei mesi per i sistemi di cui all’allegato III e dodici mesi per i sistemi di cui all’allegato I⁴⁰.

Ad ogni buon conto, la proposta disponeva di introdurre contemporaneamente una “rete di sicurezza” temporale mediante l’istituzione di *deadlines* oltre le quali le disposizioni si sarebbero applicate automaticamente, indipendentemente dalla certificazione della Commissione: il 2 dicembre 2027 per l’allegato III e il 2 agosto 2028 per l’allegato I. Questo duplice meccanismo (*trigger* condizionato + *deadline* massima) avrebbe consentito flessibilità nel breve termine garantendo certezza nel medio termine.

La ragione sottostante questo approccio è esplicitamente enunciata nella parte illustrativa della proposta. In particolare, secondo la Commissione, i tempi rigidi di implementazione originariamente previsti non sarebbero stati tarati sulla velocità reale dei processi di armonizzazione tecnica e sulla capacità amministrativa dei sistemi di supervisione nazionali, mettendo in difficoltà le realtà europee sul piano della *compliance* al nuovo assetto normativo⁴¹.

Un secondo asse strutturale della proposta ha riguardato l’estensione di privilegi normativi dalle piccole e medie imprese (SME) alle piccole imprese di media capitalizzazione (SMC, *small mid-cap enterprises*), e la conseguente calibratura dei requisiti di conformità sulla base della dimensione

comprende, tra l’altro, valutazioni e test di conformità obbligatori, l’adozione di misure di sicurezza e di gestione del rischio, obblighi di trasparenza in ordine alle modalità di funzionamento del sistema e forme di supervisione umana. Un esempio paradigmatico è rappresentato dai sistemi di riconoscimento facciale impiegati per la sorveglianza in tempo reale di spazi accessibili al pubblico. A questo riguardo, senza la volontà di essere esaustivi si rimanda alle seguenti fonti: G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell’UE e negli USA: alea IActa est*, in *DPCE Online*, 2, 2024, 1111 ss.; O. Pollicino - F. Donati - G. Finocchiaro - F. Paolucci, *La disciplina dell’intelligenza artificiale*, Milano, 2025.

³⁹ Queste misure comprendono tre categorie specifiche: standard armonizzati, specifiche tecniche comuni, e linee guida della Commissione. art. 1, par. 31, COM(2025) 836 final.

⁴⁰ Art. 1, par. 31, lett. a) i-ii.

⁴¹ Relazione introduttiva COM(2025) 836 final, punto 22, 18.

organizzativa dell'operatore.

L'art. 1 par. 3, della proposta si poneva l'obiettivo di introdurre formalmente definizioni legali di SME e SMC, incorporando i criteri quantitativi della raccomandazione 2003/361/EC (per le SME) e della nuova raccomandazione 2025/1099 (per le SMC)⁴². Scendendo nello specifico, l'art. 11, come delineato dalla proposta, avrebbe consentito alle SMC e alle SME di fornire la documentazione tecnica sull'uso di AI ad alto rischio in forma semplificata, utilizzando *templates* specificamente sviluppati dalla Commissione⁴³. Similmente, l'art. 17 sarebbe stato emendato per stabilire che l'implementazione del sistema di gestione della qualità sia adeguata alla dimensione dell'organizzazione del *provider*, con esplicito riferimento alle SMC e alle SME⁴⁴.

Alla norma qui richiamata se ne aggiungono altre, come i riformati artt. 63-70-99 AI Act, i quali, nonostante spazino per quanto riguarda il tema (dai codici di condotta ai sistemi sanzionatori), sono frutto di una politica chiara. La logica che sottende questa stratificazione di privilegi è esplicitamente teorizzata nella memoria illustrativa: le imprese piccole e medie affrontano proporzioni di carico normativo significativamente superiori alle grandi imprese, in quanto i costi amministrativi non scalano linearmente con la dimensione. È immaginabile, a puro scopo esemplificativo, che un obbligo procedurale che comporta costi fissi di €100.000 rappresenti una percentuale di onere molto superiore per un'impresa di 50 dipendenti rispetto a un'impresa con 5.000 dipendenti. La differenziazione proporzionale dei requisiti sarebbe stata quindi razionalmente giustificata dal principio economico dell'allocazione efficiente degli oneri normativi⁴⁵. Il terzo asse organizzativo della proposta ricalca quasi perfettamente le motivazioni alla base del DO, ossia l'eliminazione di complessità procedurali che non aggiungono valore protettivo, con particolare attenzione alla riduzione di duplicazioni amministrative. Il riformato par. 8 dell'art. 28 AI Act poneva la possibilità, per gli organismi di valutazione della conformità elencati nell'allegato I, sezione A, di presentare una richiesta unificata al fine di accedere a una procedura unica di valutazione della conformità del soggetto interessato (di regola un'impresa o un ente). Alla lettera dell'AI Act originario, tali organismi erano tenuti a esperire procedimenti distinti dinanzi a diverse autorità notificanti, con conseguenti duplicazioni sul pia-

⁴² Rispettivamente: le SME rimangono definite dal criterio di duecentocinquanta dipendenti e fatturato fino a cinquanta milioni di euro, mentre le SMC comprendono imprese con fino a duemilacinquecento dipendenti e fatturato fino a cinquecento milioni di euro.

⁴³ Art. 1, par. 8, COM(2025) 836 final.

⁴⁴ Art. 1, par. 9, COM(2025) 836 final.

⁴⁵ Relazione introduttiva COM(2025) 836 final, punto 4, 12.

no documentale e temporale. Il diverso regime giuridico sottoposto dalla Commissione alle altre Istituzioni europee avrebbe consentito il consolidamento in un unico procedimento che soddisfa contemporaneamente tutti i requisiti⁴⁶.

Continuando, si può notare come l'art. 49, par. 2, dell'AI Act viene abrogato. Con esso, è eliminato l'obbligo di registrazione nel *database* centralizzato dell'UE per quei sistemi di intelligenza artificiale impiegati in contesti pericolosi che, pur rientrando in ambiti tipicamente sensibili, non sono qualificati come ad alto rischio. Ciò avviene quando il fornitore, ai sensi dell'art. 6 par. 3 AI Act, abbia concluso che il sistema è destinato esclusivamente allo svolgimento di compiti preparatori o procedurali di portata limitata. Questo emendamento riconosceva che l'obbligo di registrazione centralizzata non aggiunge valore protettivo per sistemi che, per definizione, non presentano rischi significativi nel concreto. In ogni caso, sarebbe permaso l'obbligo di documentare la valutazione fatta dal soggetto utilizzatore e di renderla disponibile alle autorità competenti su richiesta, mantenendo aperta la possibilità di controllo *ex post*⁴⁷.

Procedendo secondo la struttura dell'originale AI Act e della conseguente COM(2025) 836 final, si trova un quarto asse strategico della proposta. Si tratta dell'espansione e della razionalizzazione delle c.d. *regulatory sandboxes* e dei regimi di *real-world testing*, come strumenti di equilibrio tra innovazione e supervisione⁴⁸.

L'art. 57, come modificato dalla proposta, avrebbe conferito al nuovo AI Office della Commissione il potere di istituire una *sandbox* normativa comunitaria per i sistemi di intelligenza artificiale che rientrano nella competenza esclusiva della Commissione stessa⁴⁹. La *sandbox* europea si poneva l'obiettivo di consentire ai fornitori (con priorità per le SME) di sviluppare, addestrare e testare sistemi innovativi di intelligenza artificiale in un ambiente controllato, con supervisione attiva ma con flessibilità normativa, anteriormente alla loro commercializzazione.

Su questo fronte, il riformato art. 58, par. 1, specificamente conferiva alla stessa Commissione il potere di adottare atti di implementazione che definiscono in dettaglio le modalità di istituzione, sviluppo, operazione, *governance* e supervisione di tali *sandboxes*. A ciò si accompagnava la previsione

⁴⁶ Art. 1, par. 10, COM(2025) 836 final.

⁴⁷ Art. 1, par. 14, COM(2025) 836 final.

⁴⁸ Per un inquadramento del fenomeno delle “*regulatory sandboxes*” nel contesto digitale europeo si rimanda, *ex multis*, a: F. Bagni - F. Seferi (eds.), *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, CINI's Cybersecurity National Lab, 2025; E. Longo, *Regulatory Sandboxes: A Wager on Europe's AI Strategy*, in *BioLaw Journal*, 3, 2025, 293 ss.

⁴⁹ Art. 1, par. 17, COM(2025) 836 final.

esplicita di principi comuni riguardanti criteri di eleggibilità e selezione, procedure di applicazione e partecipazione⁵⁰.

Benché gli spazi controllati rappresentino uno strumento efficace, la sperimentazione richiede necessariamente un'estensione a contesti esterni. In questa prospettiva, i riformati artt. 60 e 60-*bis* andavano a disciplinare il diritto di condurre prove in condizioni reali al di fuori di ambienti controllati. Lo stesso art. 60 estendeva la possibilità di *testing* in condizioni reali non solo ai sistemi biometrici e ad alto rischio di cui all'allegato III, ma anche ai modelli ad alto rischio incorporati in prodotti soggetti alla legislazione di armonizzazione di cui all'allegato I, sezione A (quali i dispositivi medici, i sistemi di aviazione civile, i sistemi automobili)⁵¹.

Il nuovo art. 60-*bis*, invece, introduceva un meccanismo ancora più flessibile per i sistemi ad alto rischio incorporati in prodotti soggetti alla legislazione di cui all'allegato I, sezione B (quale la Direttiva sulla sicurezza nelle ferrovie). Per siffatti strumenti, il test in condizioni reali veniva autorizzato mediante "accordi volontari" conclusi per iscritto tra Stati membri interessati e la Commissione⁵².

Proprio a partire dal rischio, dalla sua analisi e dalla prevenzione di eventuali incidenti, si muovono gli ultimi due pilastri su cui si basa la proposta originaria del DOAI: la centralizzazione della supervisione e l'*AI literacy*.

Il quinto asse organizzativo della proposta ha riguardato la concentrazione della supervisione e dell'*enforcement* di determinate categorie di sistemi ad alto rischio presso il neo-istituito AI Office della Commissione europea⁵³. L'art. 75 AI Act, come radicalmente emendato, avrebbe attribuito alla Commissione (operante tramite l'AI Office) competenza esclusiva di coordinamento per due categorie di mezzi:

- (a) Sistemi di intelligenza artificiale basati su modelli AI *general-purpose* (GPAI), laddove il modello e il sistema siano sviluppati dal medesimo fornitore;
- (b) Sistemi di intelligenza artificiale incorporati in piattaforme online

⁵⁰ Art. 1, par. 18, COM(2025) 836 final.

⁵¹ Art. 1, par. 19, COM(2025) 836 final. Il testo definitivo del DOAI presenta un vero e proprio articolo a sè stante legato alla normativa sull'aviazione civile. Cfr. art. 2 regolamento (UE) 2026/1744.

⁵² Art. 60-*bis*, par. 2, AI Act; art. 1, par. 20, COM(2025) 836 final.

⁵³ Com'è noto, l'AI Office (Ufficio europeo per l'IA) è stato istituito con Decisione della Commissione C(2024) 390 final del 24 gennaio 2024, all'interno della DG CONNECT (in vigore dal 21 febbraio 2024; pubbl. in GU C/2024/1459 del 14 febbraio 2024). Non è un'agenzia autonoma, ma una struttura interna alla Commissione, competente per i modelli GPAI, la vigilanza, gli strumenti di valutazione, le sandbox e il segretariato dell'AI Board. Cfr. a riguardo S. Calzolaio, *Autorità, governo, attuazione dell'AI Act*, in F. Pizzetti - S. Calzolaio - A. Iannuzzi - E. Longo - M. Orofino, *La regolazione europea dell'intelligenza artificiale*, cit., 139 ss.

molto grandi o motori di ricerca online di rilevanti dimensioni, come designati secondo il Regolamento DSA 2022/2065⁵⁴.

In ogni caso, l'esclusività che risulta dalla presente assunzione di competenza avrebbe implicato contemporaneamente l'esclusione di altre categorie di sistemi dalla supervisione della Commissione: in particolare, sarebbero rimasti sotto la competenza delle autorità nazionali e degli organismi di supervisione settoriali i sistemi ad alto rischio correlati a prodotti soggetti a legislazione di armonizzazione settoriale (allegato I). Su questo versante, molto probabilmente, l'istituzione europea di governo vuole responsabilizzare i singoli Stati membri affinché si occupino della materia e, soprattutto, perché si attivino nell'implementazione di quelle regole sancite dall'AI Act "originario"⁵⁵.

Tornando alla norma, la motivazione alla base dell'accentramento trova sede nel considerando introduttivo della proposta: i sistemi basati su modelli di GPAI incorporati in servizi e/o prodotti facenti capo a multinazionali del settore digitali hanno naturali caratteristiche transfrontaliere e di impatto sistemico che richiedono supervisione coerente e complessiva a livello comunitario⁵⁶. La Commissione, complice il suo ruolo e la sua posizione rispetto ai singoli Stati, dispone di informazioni, competenze e capacità di *enforcement* superiori rispetto alle autorità nazionali. La centralizzazione eviterebbe, quantomeno sulla carta, che la frammentazione, derivante da procedimenti paralleli di diversi enti nazionali, minacci lo stesso schema di protezione individuato dalla strategia europea negli ultimi dieci anni⁵⁷.

Con riferimento ai singoli ordinamenti nazionali, l'art. 77, come proposto, andava a riconoscere espressamente alle autorità nazionali il diritto di accedere alle informazioni e alla documentazione detenute dalle autorità di vigilanza del mercato in applicazione dell'AI Act. Questo diritto di accesso si accompagnava all'obbligo della autorità preposta alla sorveglianza di sollecitare informazioni direttamente dai fornitori quando necessario.

Merita un discorso a parte la questione relativa alla c.d. "*AI literacy*", ossia la conoscenza del mezzo automatizzato da parte di coloro che utilizzano gli strumenti dotati di IA o coloro che sono sottoposti agli effetti dell'utilizzo⁵⁸.

⁵⁴ Art. 1, par. 25, lett. b), Digital Omnibus on AI. È chiaro che il riferimento sia quasi del tutto esplicitato nei confronti delle c.d. "*Big Tech*".

⁵⁵ AI Act, considerando 148-154.

⁵⁶ COM(2025) 836 final, considerando 14.

⁵⁷ U. Pagallo, *The Politics of Data in EU Law: Will It Succeed?*, in *Digital Society*, 1, 2022; G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022.

⁵⁸ Con riferimento all'*AI literacy*, l'AI Act vi dedica il considerando 20, nel quale

L'originario art. 4 AI Act dispone alcuni compiti in capo a coloro che gestiscono l'utilizzo di strumenti automatizzati. L'obbligo è configurato in termini diretti e vincolanti: i fornitori e gli utilizzatori di sistemi AI devono garantire un livello adeguato di alfabetizzazione in materia di IA del proprio personale e dei soggetti terzi che operano i sistemi per loro conto, in considerazione delle competenze tecniche, dell'esperienza, della formazione e del contesto operativo⁵⁹. Ciò che la Commissione ha proposto con un nuovo art. 4 è un vero e proprio capovolgimento strutturale del regime di responsabilità: dalla responsabilità primaria diretta e verticale verso le organizzazioni private si sarebbe transitati a una responsabilità diffusa e orizzontale della Commissione e degli Stati membri di "incoraggiare" comportamenti conformi⁶⁰. La disposizione specificava poi che il suddetto emendamento rimane «*without prejudice to the broader measures taken by the Commission and the Member States to promote AI literacy and competences for the wider population, including learners, students, and citizens at different ages and in particular through education and training systems*»⁶¹.

Per comprendere adeguatamente i profili problematici di questa politica riformatrice, è essenziale analizzare il mutamento di natura giuridica dell'obbligo. Nel regime originario, l'art. 4 si configura come obbligo positivo vincolante (si usa infatti l'espressione «adottano misure»⁶²): il *provider/de-*

si afferma che: «Al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i *deployer* e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA. Tali nozioni possono variare in relazione al contesto pertinente e possono includere la comprensione della corretta applicazione degli elementi tecnici durante la fase di sviluppo del sistema di IA, le misure da applicare durante il suo utilizzo, le modalità adeguate per interpretare l'output del sistema di IA e, nel caso delle persone interessate, le conoscenze necessarie per comprendere in che modo le decisioni adottate con l'assistenza dell'IA incideranno su di esse. Nel contesto dell'applicazione del presente regolamento, l'alfabetizzazione in materia di IA dovrebbe fornire a tutti i pertinenti attori della catena del valore dell'IA le conoscenze necessarie per garantire l'adeguata conformità e la sua corretta esecuzione». In ogni caso, tale forma di conoscenza assume un valore peculiare e non appare riducibile a una mera attività esplicativa analoga a quella riferibile a strumenti tecnologici ordinari. Come evidenziato da taluni, essa rinvia a presupposti di natura più profonda, che investono dimensioni culturali, cognitive e istituzionali di particolare rilievo. Cfr. Y. Yumi, *Establishing the concept of AI literacy*, in *European Journal of Bioethics*, 12(2), 2021, 353 ss.

⁵⁹ Art. 4 AI Act.

⁶⁰ Art. 1, par. 4, COM(2025) 836 final.

⁶¹ Relazione introduttiva COM(2025) 836 final, punto 5, 12-13.

⁶² Di seguito si riporta il testo integrale: «I fornitori e i *deployer* dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in

ployer ha il dovere di adottare misure concrete, documentabili e verificabili, finalizzate a garantire un sufficiente livello di *AI literacy* di qualsiasi persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA. La violazione di questo obbligo costituisce un'infrazione potenzialmente passibile di sanzione; sebbene non espressamente elencata nel catalogo delle violazioni dell'AI Act (art. 99), tale inosservanza rimane contestabile presso le autorità di vigilanza del mercato nel contesto del loro potere generale di *enforcement* dell'AI Act nei singoli ordinamenti degli Stati membri⁶³.

Nel nuovo regime proposto, l'art. 4 si sarebbe trasformato in una previsione programmatica in cui si stabilisce un generico obbligo pubblico di incentivazione: la Commissione e i Paesi dell'Unione sono solo tenuti a "incoraggiare" (*«shall encourage»*), termine che nella grammatica giuridica indica un dovere di promozione e facilitazione, non di imposizione cogente.

Lasciando ad un momento successivo le notevoli considerazioni sociopolitiche di tale approccio, dal punto di vista puramente giuridico, una siffatta trasformazione produrrebbe almeno tre conseguenze strutturali. *In primis*, l'eliminazione della responsabilità diretta privata: le imprese/gli enti non sono più *primary duty-bearer* rispetto all'art. 4, bensì soggetti passivi verso cui si dirigono iniziative pubbliche di incentivazione. La *compliance* non è più giuridicamente obbligatoria sulla base di un rapporto di causalità tra mezzo, utilizzatore attivo e soggetto passivo del rapporto d'uso di strumenti AI, ma piuttosto una conseguenza auspicata di uno stimolo esterno dai vaghi contorni. Secondo, la frammentazione della catena di responsabilità; mentre nel regime originario un'autorità nazionale di sorveglianza poteva verificare il livello di *AI literacy* di un'organizzazione, nel regime prospettato l'*accountability* si articolerebbe su due livelli indipendenti:

- (a) il livello di "incoraggiamento" erogato da Commissione/Stati membri, valutabile soltanto *ex post* e sulla base di criteri poco chiari;
- (b) l'effettiva implementazione dell'incoraggiamento ricevuto da parte del *provider/deployer*, il cui fallimento non è più direttamente sanzionabile, non esistendo più un reale principio giuridico vincolante.

Infine, l'introduzione di asimmetrie di *enforcement*: gli strumenti a disposizione degli enti pubblici che dovrebbero farsi carico del compito di incoraggiare i privati a trovare "la retta via" sono sostanzialmente limitati a quelli di *soft governance* (linee guida, buone pratiche, seminari e iniziative di

considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.»

⁶³ Art. 85, par. 1, AI Act: «Fatti salvi altri ricorsi amministrativi o giurisdizionali, qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del presente regolamento può presentare un reclamo alla pertinente autorità di vigilanza del mercato».

confronto, campagne di sensibilizzazione). Contrariamente al regime del GDPR, dove l'obbligo di mettere in atto «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio»⁶⁴ rimane diretto sui *data controller* con una conseguente sorveglianza rigorosa da parte delle autorità di protezione dei dati, il rivisto art. 4 non prevedeva parametri di *performance* né meccanismi di verifica sull'efficacia dell'incoaggiamento erogato.

Ricapitolando, la COM(2025) 836 final articolava il suo intervento intorno a sei pilastri strategici che, sebbene destinati a operare in sinergia, rivelavano sottotraccia alcune tensioni strutturali significative.

Dai meccanismi di temporalità flessibile (asse 1), passando attraverso la calibratura proporzionale dei gravami su imprese di diverse dimensioni (asse 2), l'eliminazione di ridondanze procedurali (asse 3), la creazione di spazi di sperimentazione controllata (asse 4), fino alla centralizzazione della supervisione presso la Commissione (asse 5) e il ribaltamento della filosofia di responsabilità in materia di *AI literacy* (asse 6), il DOAI originario configurava un arcipelago normativo i cui nessi logici non sono sempre coerenti – non deve stupire, a questo proposito, che sia andato incontro a modifiche.

In primo luogo, si deve evidenziare una tensione tra flessibilità implementativa e certezza normativa. Mentre i pilastri 1, 2 e 3 hanno mosso verso una maggiore elasticità nei tempi e nelle modalità di conformità, gli assi 5 e 6 comportavano, paradossalmente, un irrigidimento della supervisione centralizzata e una smaterializzazione degli obblighi in capo ai privati (nel caso dell'*AI literacy* il rilievo è lampante e preoccupante). In altre parole, la Commissione avrebbe guadagnato potere di *enforcement* e di controllo proprio mentre ridimensionava gli obblighi vincolanti cui si sottoposero i privati sotto il *framework* originale dell'AI Act.

In secondo luogo, si riscontra una discrasia tra approccio settoriale e approccio orizzontale. I primi quattro assi sono chiaramente orientati a facilitare l'innovazione nelle SME/SMC e a ridurre la complessità burocratica per gli operatori. Al contrario, l'asse 5 (centralizzazione) si manifesta in modo orizzontale-deterritorializzato, applicandosi indistintamente a qualsiasi sistema di GPAI di grandi fornitori, indipendentemente dal settore di implementazione.

In terzo luogo, e più criticamente, il mutamento di *policy* sull'*AI literacy* – cassato in larga parte dal nuovo art. 1, par. 5, regolamento (UE) 2026/1744 – avrebbe rappresentato una variazione di paradigma senza precedenti

⁶⁴ Art. 32, par. 1, GDPR: «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio».

nella filosofia regolativa europea. L'idea di una transizione da un obbligo primario vincolante a un obbligo pubblico di incoraggiamento segna un allontanamento dalla struttura di *accountability* verticale che ha caratterizzato il GDPR, il DSA, e il DMA⁶⁵.

Infine, una considerazione trasversale: sia il DO che il DOAI si inscrivono entro una strategia di competitività dinamica per la quale la Commissione non intende eliminare la regolazione digitale europea, bensì ricalibrarne la pressione al fine di rendere le aziende europee più agili, innovative e capaci di competere con fornitori (soprattutto) cinesi e statunitensi. L'obiettivo si rivela più che legittimo e comprensibile nel contesto geopolitico attuale. Tuttavia, la politica del diritto che fa da sfondo al Digital Package non fornisce garanzie credibili circa il fatto che la maggiore leggerezza regolativa non comporterà un graduale scadimento della protezione dei cittadini europei.

Se questo cambio di passo avrà successo nel rilancio competitivo europeo, rimane al momento questione aperta. Ciò che è certo è che l'insorgere di tali proposte segna una transizione verso una politica regolativa più fluida, meno prevedibile e potenzialmente esposta a maggiori rischi di sotto-*enforcement*.

4. Una riflessione critica sul futuro digitale europeo

Compiuta la ricognizione sul contenuto delle proposte di riforma, è possibile trarre numerosi spunti di riflessione.

Il Digital Package emerge come espressione di un cambio di paradigma strategico nell'architettura normativa continentale. Non si tratta di un mero aggiustamento tecnico, bensì di una rotazione significativa nella filosofia regolativa che ha animato il decennio 2016-2025. Per comprendere a pieno questo mutamento, è essenziale contestualizzare i due Digital Omnibus: essi, infatti, si collocano in una fase di transizione storica della *leadership* occidentale e globale. Tale fase è segnata, da un lato, dalla prospettiva confusa e destabilizzante della seconda amministrazione Trump negli Stati

⁶⁵ Per distinguere il filo conduttore, che si dipana in vari ambiti, si rimanda ad alcune riflessioni eterogenee ma comunque unite dall'ottica della comparazione dei diversi (ma simili) regimi giuridici. C. Argelich Comelles, *Towards a European regulation on the liability of online platforms for algorithmic discrimination in consumer contracts*, in *Journal of European Consumer and Market Law*, 5, 2023, 1 ss.; P. Hacker - J. Cordes - J. Rochon, *Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond*, in *European Journal of Risk Regulation*, 15(1), 2024, 49 ss.; A.S. D'Amico, *The DMA's Consent Moment and its Relationship with the GDPR*, in *European Journal of Risk Regulation*, 16(1), 2025, 170 ss.

Uniti e, dall'altro, dalle pressioni sempre più incisive esercitate dalla Cina sulla sovranità tecnologica europea. A ciò si aggiunge una consapevolezza ormai diffusa all'interno delle istituzioni dell'Unione secondo cui il modello regolatorio affermatosi a partire dal GDPR, pur apprezzabile sotto il profilo della tutela dei diritti fondamentali, ha generato costi di *compliance* significativi per le imprese europee, soprattutto per le PMI. Tali costi, inoltre, non si sono tradotti in un rafforzamento della competitività globale delle piattaforme europee. Al contrario, il quadro normativo ha finito per operare in un contesto in cui le grandi imprese extra-UE hanno continuato ad accrescere il proprio potere di mercato, senza che ciò si accompagnasse a un livello di protezione dei cittadini effettivamente uniforme⁶⁶.

In questa cornice, il Digital Package non deve essere percepito come una rinuncia totale ai valori europei, bensì un riposizionamento strategico: l'Unione intende permanere come attore normativo globale, ma con un proposito di "regolazione intelligente", ossia come artefice di una legislazione vincolante su pochi principi giuridici "identitari" (*ex multis*: non discriminazione, portabilità dei dati, trasparenza, etc.), ma flessibile nelle modalità di conformità, nelle tempistiche di implementazione e nel carico amministrativo distribuito sugli operatori di diverse dimensioni che operano nel settore del *tech*.

Tuttavia, come forse si è potuto intuire, tale riorganizzazione – certamente ambiziosa e, sul piano teorico, di indubbio interesse – non risulta esente da fratture logiche e da nodi normativi tuttora irrisolti. Nel prosieguo dell'analisi si intende individuare tre direttrici lungo le quali incanalare la riflessione critica sulle proposte regolatorie fin qui esaminate, al fine di cogliere le diverse dimensioni entro cui si articola la novella legislativa: quella giuridico-comparatistica, quella sociale e quella politico-economica.

4.1 Il confronto con i modelli extra-UE: la visione di Stati Uniti e Cina

Per comprendere il significato strategico del Digital Package, diviene indispensabile collocarlo all'interno del panorama internazionale della regolazione digitale. Difatti, la scelta normativa europea non avviene nel

⁶⁶ Negli ultimi anni si sono avvicinate numerose controversie tra gli organismi di controllo europei e le grandi piattaforme sorte nel settore digitale. Alcune di queste hanno portato a sanzioni di un certo rilievo, per motivi tra di loro eterogenei. A questo riguardo si vedano i seguenti casi: European data protection Board, *1.2 billion euro fine for Facebook as a result of EDPB binding decision*, 22 maggio 2023; Commissione europea, *Commission finds Apple and Meta in breach of the Digital Markets Act*, 23 aprile 2025; A. Vicinanza, *Il primo atto di enforcement del Digital Services Act tra tensioni geopolitiche: la sanzione della Commissione europea nei confronti di X (Twitter)*, in *Blog AISDUE*, 18 gennaio 2026.

vuoto, ma in una competizione dove Stati Uniti e Cina hanno già definito paradigmi alternativi di *governance* tecnologica, ciascuno con conseguenze profondamente diverse per i cittadini e le aziende⁶⁷.

Il contesto normativo degli Stati Uniti rappresenta il polo più prossimo al liberismo regolativo. A differenza dell'UE, che ha optato per un modello di regolazione che opera principalmente *ex ante* (il GDPR si applica prima dell'immissione sul mercato di servizi di trattamento dati; l'AI Act fa altrettanto per i sistemi di IA), gli Stati Uniti procedono tramite un modello di intervento *post-hoc* e *case-by-case*. La libertà contrattuale e imprenditoriale opera *ex ante* praticamente senza limiti; l'*enforcement* si concentra dopo che un danno concreto è stato causato. Un esempio emblematico lo si trova nel *Federal Trade Commission Act*, il quale proibisce «*unfair or deceptive acts or practices*»⁶⁸, ma la determinazione di cosa costituisca ingiustizia o inganno avviene in sede giudiziale, non tramite linee guida prescrittive o standard normativi predefiniti.

Nonostante questa architettura possa apparire *prima facie* permissiva, la ricerca empirica dimostra che l'*enforcement* è reattivo e considerevole quando applicato. Nel 2024, il Dipartimento di giustizia e il *Consumer financial protection bureau* hanno ottenuto un patteggiamento di \$8 milioni dalla società Fairway Mortgage per “*systematic redlining*” algoritmico nella contea di Birmingham, Alabama: la società aveva diretto annunci pubblicitari quasi esclusivamente verso aree a popolazione bianca e approvava le domande di prestito di richiedenti neri al 43% del tasso riservato a candidati bianchi nella medesima area geografica⁶⁹. Similmente, l'azienda SafeRent ha subito una sanzione di \$2.2 milioni nel 2024 per aver utilizzato algoritmi che penalizzavano sistematicamente famiglie afroamericane e ispanico-americane a basso reddito negando loro l'accesso a unità abitative per le quali

⁶⁷ Secondo alcuni, lo slancio degli ultimi anni nei confronti del settore digitale può trovare dei parallelismi solo nella corsa allo spazio che caratterizzò i primi decenni della Guerra fredda, dove Stati Uniti e Unione sovietica si combattevano cercando di introdurre sempre maggiori innovazioni fino anche a portare l'uomo sulla Luna. Ad ogni buon conto, oggi il clima è cambiato: il ruolo degli Stati è mutato, i privati hanno acquisito poteri di cui non disponevano nel secolo scorso e il mondo non è più basato su due macro-poli antagonisti tra loro; forse, è tutto diventato più complicato. Cfr. I. Ulnicane, *Against the new space race: global AI competition and cooperation for people*, in *AI and society*, 38, 2023, 681 ss.; Siemens, *A new Space race report*; S. Braddock, *The world's next great space race is digital: AI and the power of smaller models*, in *ERP Today*, 16 settembre 2024.

⁶⁸ «*The Federal Trade Commission Act is the primary statute of the Commission. Under this Act, as amended, the Commission is empowered, among other things, to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce*». La norma viene richiamata anche dall'ordine esecutivo sull'AI emanato dal presidente Trump l'11 dicembre 2025.

⁶⁹ U.S. Department of Justice, *Justice Department Secures \$8M from Fairway Independent Mortgage Corporation to Address Redlining in Black Communities in Birmingham, Alabama*, 15 ottobre 2024.

erano altrimenti qualificate⁷⁰.

Ad ogni buon conto, venendo al presente, merita di essere segnalata l'adozione da parte dell'amministrazione Trump dell'ordine esecutivo dell'11 dicembre 2025 "*Ensuring a national policy framework for Artificial Intelligence*"⁷¹. L'intervento sembra segnare una significativa riconfigurazione degli equilibri ordinamentali statunitensi in materia di regolazione dell'IA⁷². L'atto appare indicativo di un parziale ripensamento dell'impostazione tradizionalmente incentrata su meccanismi di *enforcement ex post*, senza tuttavia tradursi in una convergenza verso un modello di regolazione simile a quello di origine europea.

Piuttosto, l'ordine esecutivo si colloca lungo la direttrice di una strategia di *federal preemption*, orientata a rafforzare il ruolo del potere federale quale argine alla proliferazione di iniziative normative statali ritenute virtualmente distorsive o eccessivamente onerose per l'industria tecnologica⁷³. In tale prospettiva si inserisce, tra l'altro, l'istituzione di una *AI litigation Task force* presso il Dipartimento di giustizia, incaricata di valutare e, se del caso, contestare la compatibilità delle legislazioni statali in materia di intelligenza artificiale con i principi del commercio interstatale e con la *policy* federale delineata dall'ordine esecutivo.

È opportuno chiarire nuovamente che tale evoluzione non configura un avvicinamento al modello europeo di regolazione *ex ante*, bensì un tentativo di razionalizzare in ottica centralizzata un'impostazione sostanzialmen-

⁷⁰ S. Bhuiyan, *She didn't get an apartment because of an AI-generated score – and sued to help others avoid the same fate*, in *The Guardian.com*, 14 dicembre 2024. Questi casi dimostrano che l'*enforcement ex post* statunitense, sebbene limitato, laborioso e lento, produce effetti concretamente deterrenti quando applicato. Tuttavia, il costo di questa deterrenza è sostenuto dalle vittime, che devono documentare il danno, intraprendere azioni legali costose, e navigare il complesso sistema giudiziale americano. Non esiste protezione preventiva, e questo porta a forti effetti escludenti nei confronti delle fasce più disagiate della società.

⁷¹ E.O., 11 dicembre 2025, *Ensuring a national policy framework for Artificial Intelligence*. Sull'approccio di Trump in tema di regolamentazione dell'IA e per una retrospettiva sulla policy del suo predecessore Biden si rimanda anche a E. Gherri, *Gli Executive Orders in materia di Artificial Intelligence: amministrazione Biden e Trump a confronto*, in questa Rivista, 2, 2025, 266 ss.

⁷² E.O., Section 7.

⁷³ A questo proposito, per dimostrare che non è solo il potere federale statunitense ad occuparsi di bloccare iniziative in tal senso, merita ricordare la vicenda della proposta di legge statale californiana SB 1047, su cui il governatore Newsom ha apposto il veto nel settembre 2024 per via di una politica di mantenimento di buoni rapporti con le grandi aziende del *tech* presenti sul territorio. La proposta californiana rappresenta uno degli scenari su cui Trump è voluto intervenire. Per completezza si rimanda alla lettera di veto del governatore Newsom: Office of the Governor, *Lettera di veto SB 1047*, 29 settembre 2024.

te deregolatoria: non tanto attraverso l'introduzione di standard sostanziali uniformi, quanto mediante la neutralizzazione dell'attivismo normativo decentrato e la preservazione di un contesto regolativo complessivamente favorevole allo sviluppo dell'innovazione tecnologica e alla tutela degli interessi degli oligarchi statunitensi del settore digitale⁷⁴.

Diametralmente opposto al modello americano si posiziona il *framework* cinese, che raffigura un esempio di innovazione tecnologica profondamente subordinata agli obiettivi e al controllo dello Stato⁷⁵.

Nel 2017, il governo centrale ha adottato il “*New generation AI development plan*”, identificando l'IA come priorità strategica nazionale con l'obiettivo dichiarato di divenire leader mondiale nella tecnologia entro il 2030⁷⁶. Diversamente dalla strategia digitale europea, che si è espressa come una molteplicità di atti tra loro connessi dal fine di proteggere *in toto* la sfera giuridica dei cittadini⁷⁷, la strategia cinese si è sviluppata come integrazione della tecnologia negli apparati di *governance* statale. Dalla pubblicazione delle “*Interim Measures for Generative AI Services*” (2023⁷⁸) e dai successivi aggiornamenti del 2024, la *Cyberspace administration of China* (CAC) ha centralizzato la supervisione degli algoritmi di raccomandazione dei contenuti, della sintesi profonda (*deepfake*) e dei sistemi di intelligenza artificiale generativa. Se il modello europeo articola la disciplina dell'intelligenza artificiale attribuendo rilievo distinto alle figure dei *providers* (sviluppatori) e dei *deployers* (utilizzatori finali), l'approccio regolatorio cinese si caratterizza per una configurazione profondamente diversa, riconducibile a tre tratti fondamentali.

In primo luogo, emerge una richiesta esplicita di allineamento ai cosiddetti *core socialist values*, in forza della quale i sistemi di intelligenza artificiale sono tenuti a operare in coerenza con gli obiettivi politici centrali e con l'indirizzo ideologico del Partito comunista cinese⁷⁹. In secondo luogo, la

⁷⁴ J.E. Cohen, *Oligarchy, State, and Cryptopia*” - Georgetown University Law Center Research Paper no. 20/2025, in *Fordham Law Review*, 94, 2025, 563 ss.

⁷⁵ Cfr. per una introduzione trasversale al tema S. Calzolaio, *Dalla protezione dei dati personali all'ordinamento dei dati (l'evoluzione del diritto cinese e del diritto europeo dei dati)*, in G. Di Cosimo (a cura di), *Processi democratici e tecnologie digitali*, Torino, 2023, 197 ss.

⁷⁶ *China's New Generation Artificial Intelligence Development Plan* – 2017.

⁷⁷ Commissione europea, *Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence*.

⁷⁸ P. Confino, *China just gave the world a blueprint for reining in generative A.I. like ChatGPT and Bard*, in *Fortune*, 14 luglio 2023. Si rimanda in questa sede, in prima battuta, ad un articolo di commento della normativa poiché manca una versione “ufficiale” del testo tradotto. In ogni caso, per completezza, si rimanda ad una versione “informale” al link chinalawtranslate.com.

⁷⁹ University of Virginia, National security Data and policy institute, *The Chinese Communist Party's Layered Artificial Intelligence Strategy*, Research paper, 21 luglio 2025.

disciplina presenta una strutturale opacità procedurale, in quanto le disposizioni regolatorie risultano frequentemente formulate in termini volutamente generici, come dimostrato dal ricorso a standard di tipo “*best effort*” in materia di accuratezza e affidabilità degli *output*. Infine, il quadro normativo si distingue per una marcata indeterminatezza dei meccanismi di *enforcement*, affidati a margini di discrezionalità amministrativa ampi e scarsamente tipizzati⁸⁰. I privati sanno che devono adattarsi, ma il confine fra conformità e violazione è deliberatamente indefinito, consentendo allo Stato, in estrema sintesi, una discrezionalità quasi illimitata.

Le recenti revisioni della legge sulla cybersicurezza (entrate in vigore il 1° gennaio 2026) hanno formalizzato il trattamento dell’IA come pilastro della cybersecurity nazionale, elevando il rango della regolazione⁸¹. Lo Stato fornisce espliciti incentivi per la ricerca e lo sviluppo dell’IA (contrariamente all’approccio statunitense di competizione non orchestrata), mantenendo simultaneamente il diritto di *audit*, sospensione e censura dei sistemi ritenuti non conformi agli interessi statali. L’ecosistema cinese rimane altamente innovativo (la Cina rimane pari agli Stati Uniti nella quantità di *breakthroughs* tecnologici pubblicati⁸²), ma sottoposto a indirizzo e sorveglianza statale pervasiva. I cittadini cinesi non dispongono di diritti di accesso ai dati, portabilità, cancellazione o rifiuto del trattamento comparabili al GDPR⁸³. La “protezione”, in pratica, è garantita non come diritto individuale inalienabile, bensì come funzione dello Stato nel perseguimento della stabilità politica e della sicurezza nazionale⁸⁴.

Sulla base della ricognizione comparativa svolta, e in coerenza con le considerazioni sviluppate nei paragrafi precedenti, il modello emergente dal complesso dei Digital Omnibus può essere letto come una configurazione istituzionale caratterizzata dalla coesistenza di elementi tra loro eterogenei:

⁸⁰ *Ibid.*

⁸¹ A. Huld, *Revisions to China’s Cybersecurity Law: Strengthened Oversight and Alignment with Emerging Technologies*, in *China briefing*, 5 novembre 2025.

⁸² Con tale terminologia, nel gergo scientifico attuale, s’intende la creazione o la scoperta di nuovi strumenti e/o funzionalità dalla grande importanza per il settore tecnologico-digitale. M. Yu, *Blockade and Breakthrough: China-U.S. Artificial Intelligence Technology Competition Under Chip Control Policies*, in *Advances in Economics, Management and Political Sciences*, 237, 2025, 205 ss.

⁸³ Nota *supra* 75.

⁸⁴ Nello specifico, pur prevedendo formalmente diritti di accesso, rettifica, cancellazione e portabilità dei dati (artt. 44 ss. della *Personal Information Protection Law* - PIPL), la disciplina cinese contempla ampie deroghe fondate su esigenze di sicurezza nazionale e attribuisce un ruolo centrale ai poteri di vigilanza e controllo esercitati dalla *Cyberspace Administration of China*. Ne consegue che, sul piano dell’effettività delle garanzie riconosciute agli interessati, il modello cinese si discosta in misura significativa da quello delineato dal GDPR.

da un lato, una tendenza alla centralizzazione delle funzioni di coordinamento e indirizzo in capo a strutture sovranazionali, quali l'AI Office; dall'altro, il ricorso esteso a strumenti di regolazione flessibile, standard tecnici e codici di condotta.

Tale combinazione non è di per sé incoerente sul piano teorico; tuttavia, essa presenta alcuni profili di potenziale criticità sotto il profilo dell'effettività regolatoria. Proprio grazie al raffronto comparato è possibile mettere in luce tali tensioni.

Il modello statunitense, pur caratterizzato da un minore livello di regolazione a monte, tende a concentrare l'*enforcement* in autorità giurisdizionali dotate di poteri investigativi e sanzionatori incisivi a valle. L'ordinamento cinese, per converso, si fonda su un controllo pubblico ampio e strutturalmente integrato, esercitato mediante strumenti normativi e amministrativi che assicurano elevata capacità di intervento, sebbene in un contesto di minore trasparenza e di garanzie giuridiche differenziate rispetto agli standard liberaldemocratici.

L'UE sembra invece collocarsi in una posizione intermedia, nella quale l'elevata ambizione regolatoria e la centralità attribuita alla tutela dei diritti fondamentali si accompagnano a un assetto di *governance* multilivello in cui le funzioni di applicazione restano in larga misura affidate ad autorità nazionali, coordinate da strutture europee con poteri prevalentemente di indirizzo e supervisione. In assenza di adeguate risorse amministrative, meccanismi di coordinamento effettivamente operativi e pratiche applicative consolidate, tale configurazione potrebbe tradursi in una tutela dei diritti formalmente avanzata ma esposta al rischio di applicazioni disomogenee. Ne deriva che la questione decisiva non riguarda tanto la coerenza astratta dell'impianto normativo europeo, quanto le condizioni istituzionali della sua attuazione: dotazione di poteri e risorse delle autorità competenti, chiarezza delle linee di responsabilità, capacità di coordinamento tra livelli nazionali ed europeo, nonché sviluppo di prassi amministrative e giurisprudenziali stabili e trasparenti. È su questo terreno che – probabilmente – si giocherà la trasformazione della tutela dei diritti da enunciazione normativa ad effettività sostanziale.

4.2 Il cittadino alla prova degli effetti della regolamentazione europea

Mentre il quadro comparatistico definisce il posizionamento strategico del Digital Package nello scenario geopolitico, un interrogativo più sostanziale si fa avanti: quali effetti concreti produrrà tale disciplina sui cittadini europei che dovrebbe tutelare? La ricerca empirica recente offre alcuni spunti,

evidenziando un fenomeno ricorrente: la distanza tra riconoscimento formale dei diritti e la loro effettività.

Quando il GDPR entrò in vigore nel 2018, i *policy-maker* europei teorizzarono che la trasparenza normativa avrebbe abilitato i cittadini all'autogoverno consapevole dei propri dati personali⁸⁵. Il proposito si basava su una visione razionale: fornire ai cittadini diritti chiari (accesso, cancellazione, portabilità) e creare meccanismi semplificati per esercitarli affinché il mercato e la società si auto-correggessero. Tuttavia, una ricerca sul tema offre un quadro radicalmente diverso. Alcuni ricercatori norvegesi hanno condotto uno studio dal 2018 al 2023 utilizzando il *framework* “*Knowledge-Attitude-Practice*” (KAP) per misurare l'impatto del GDPR sul comportamento dei cittadini, prendendo come riferimento un campione di più di mille individui⁸⁶. I risultati hanno fornito indicazioni rilevanti: gli intervistati hanno dimostrato conoscenza elevata sia del GDPR che dei meccanismi tecnologici con cui le persone vengono maggiormente a contatto nella vita di tutti i giorni (*cookies*, *tracking*, profilazione algoritmica, etc.). Tuttavia, paradossalmente, l'atteggiamento è rimasto scettico e difensivo. Coloro che hanno partecipato allo studio hanno riconosciuto il valore teorico dei diritti garantiti dal regolamento, ma ne hanno contestato la praticabilità effettiva, ritenendo che i costi connessi al loro esercizio (tempo, oneri burocratici, conflittualità con le imprese, incertezza dell'esito) superino i benefici attesi. Ancora più significativo: la prassi mostra che la maggior parte dei cittadini non ha esercitato attivamente i propri diritti. La conclusione dello studio è inequivocabile: «*Based on our empirical data, it should be safe to conclude that the GDPR has not changed too much for consumers*».⁸⁷

Questo dato macroscopico è confermato da uno studio sperimentale condotto da ricercatori delle Università di Amsterdam e Lovanio su circa settanta *online service providers* (OSPs) per verificare il grado di *compliance* con il diritto di accesso ai dati personali (art. 15 GDPR), comparando i dati del 2020 con quelli del 2022⁸⁸. Benché i risultati della ricerca abbiano mostrato alcuni miglioramenti⁸⁹, il quadro rimane allarmante nel complesso.

⁸⁵ GDPR, considerando 39-44.

⁸⁶ W. Presthus - H. Sørsum, *Five years with the GDPR: an empirical study emphasising information privacy and the consumer*, in *International Journal of Information Systems and Project Management*, 12(3), 2024, 5 ss.

⁸⁷ Ivi, 21.

⁸⁸ P. Dewitte - J. Ausloos, *Chronicling GDPR Transparency Rights in Practice: The Good, the Bad and the Challenges Ahead*, in *International Data Privacy Law*, 14(2), 2024, 106 ss.

⁸⁹ In particolare, dallo studio richiamato nella nota precedente, emergono incrementi significativi nei livelli di consapevolezza dei cittadini: (i) quanto alla conoscenza dell'esistenza di disposizioni normative in materia, la percentuale passa dal 79% al 90%; (ii) con riferimento ai diritti alla portabilità dei dati, dal 54% all'87%; (iii) quanto alla possibilità di far valere la propria posizione giuridica dinanzi alle autorità competenti, dal

Numerose aziende negli anni hanno creato barriere strutturali: necessità di inviare reclami multipli prima di ricevere risposta, richieste di prove di identità eccessive (non necessitate dalla normativa in materia), violazione dei termini procedurali, fornitura dei dati in formati non intelligibili (es. *raw database dumps*)⁹⁰.

A quanto riportato, si aggiungano i problemi relativi all'efficacia sostanziale della sfera dei "diritti di trasparenza". Anche laddove i suddetti diritti, almeno formalmente, esistono – come nel GDPR (art. 15, art. 22) o nell'AI Act (art. 50) – la fruibilità pratica rimane estremamente bassa per ragioni strutturali al comparto del *tech*. In primo luogo, sussiste un problema epistemico: nemmeno i *designer* originali degli algoritmi comprendono pienamente come il sistema prende decisioni nel suo complesso (il noto dilemma della "*black box*" è argomento ormai molto trattato dalla dottrina⁹¹). Chiedere trasparenza algoritmica equivale, in molti casi, a pretendere qualcosa che non esiste ontologicamente – non per malafede, ma per limiti tecnici intrinseci. In secondo luogo, quando le aziende forniscono informazioni sulla trasparenza, frequentemente lo fanno in un linguaggio altamente tecnico. Per l'individuo medio, senza formazione in materia, il contenuto è molto spesso incomprensibile. In terzo luogo, il cittadino non ha accesso ai dati di *training*, alle specifiche di *fine-tuning*⁹², ai criteri di validazione, alle *performance metrics* sulle diverse demografiche. Egli dispone solo di quelle informazioni che l'azienda decide unilateralmente di rivelare (salvo obblighi di *disclosure* imposti dallo Stato), complice il diritto d'autore e la normativa sulla proprietà industriale.

Accanto a questa crisi della trasparenza, emerge un elemento altrettanto significativo: una frammentazione profonda riguardante i valori di riferimento che interessano lo sviluppo digitale europeo. Da un lato, il GDPR

74% al 96%.

⁹⁰ P. Dewitte - J. Ausloos, *Chronicle of GDPR Transparency Rights in Practice*, cit.

⁹¹ Il tema è stato molto studiato negli anni appena trascorsi, e ancora trova spazio nella discussione dottrinale. Di seguito si indicano, *ex multis*, alcuni testi rilevanti per l'approfondimento della tematica: F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, 2016; W. J. Von Eschenbach, *Transparency and the black box problem: Why we do not trust AI*, in *Philosophy & technology*, 34(4), 2021, 1607 ss.; G. Lo Sapio, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *Federalismi*, 16, 2021, 114 ss.; L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022; A. Simoncini, *Il linguaggio dell'Intelligenza artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, 2, 2023; S. Zuboff, *Il capitalismo della sorveglianza*, Roma, 2023; S. Amato, *Inquietudini digitali. Il "black box effect"*, in *Rivista di filosofia del diritto*, 1, 2025, 33 ss.

⁹² Per esigenze di chiarezza, con il termine "fine-tuning" ci si riferisce alla modifica dei parametri di un modello pre-addestrato per una specifica attività o uno specifico set di dati. Il modello viene riaddestrato con i dati relativi all'attività di destinazione, mantenendo la sua precedente esperienza. Cfr. Hewlett-Packard, *Cos'è il fine tuning (AI)?*.

e l'AI Act sono costruiti su una visione che tutela il cittadino da minacce concrete: la raccolta eccessiva di dati personali, la discriminazione algoritmica, la manipolazione tramite profilazione, la perdita di *agency* dovuta all'automazione. Dall'altro, una narrazione concorrente (sostenuta da grandi aziende *tech* e dai governi orientati verso la competitività come gli USA) individua nel controllo pubblico un freno inaccettabile all'innovazione⁹³. Il cittadino europeo è esposto su più fronti: valuta positivamente la teoria europea sulla protezione dei diritti fondamentali, ma è simultaneamente sottoposto ad un condizionamento politico-psicologico aggressivo che lo invita a "lasciare agire" l'industria, pena l'arretratezza competitiva dell'Europa con una conseguente perdita di benessere⁹⁴.

Emblematico di questa contraddizione è il fenomeno della c.d. "*consent fatigue*"⁹⁵: gli studi sulla manifestazione pratica del GDPR mostrano che molti cittadini, confrontati con schermate di *cookie banner* che chiedono consenso granulare e informato, scelgono facilmente l'opzione 'accetta tutto' pur di proseguire la navigazione. Ciò non accade per mancanza di conoscenza – come si è constatato poc'anzi⁹⁶ – ma perché il costo psicologico e temporale della decisione consapevole supera il valore percepito della protezione. Si tratta di una forma di "resa consenziente" che degrada la funzione effettiva del consenso come meccanismo di protezione. È un sintomo perfetto della contraddizione interna dell'intero sistema: il cittadino, razionalmente, rifiuta di esercitare i diritti che la legge gli conferisce, perché l'esercizio di quei diritti comporta costi che rendono irrazionale ed eccessivamente faticoso il loro esercizio⁹⁷.

4.3 Questioni ordinamentali e politiche aperte

La trasformazione da strumenti di *hard law* a *soft governance*, da diritti azionabili a obiettivi promozionali, non costituisce un fenomeno isolato ma

⁹³ Su questo fronte la battaglia è particolarmente accesa e i temi colpiscono numerose sfere dell'attualità. Cfr. J. Ryan - G. Riekes, *The EU has let US tech giants run riot. Diluting our data law will only entrench their power*, in *The Guardian.com*, 12 novembre 2025.

⁹⁴ Tra le voci, soprattutto statunitensi, si evidenzia un articolo del Wall Street Journal, il quale, nei mesi scorsi ha assunto il ruolo di denuncia/manifesto nei confronti della presunta inadeguatezza dell'approccio europeo nei confronti delle infrastrutture digitali. T. Fairless - D. Luhnnow, *The tech industry is huge – and Europe's share of it is very small*, in *The Wall Street Journal.com*, 25 maggio 2025.

⁹⁵ Z. Hou - Z. Mingxin, *'I don't get it, but I accept it'. Exploring uninformed consent to privacy policies: a neutralization perspective*, in *Computers & Security*, 153, 2025.

⁹⁶ Nota *supra* 86.

⁹⁷ Z. Hou - Z. Mingxin, *'I don't get it, but I accept it'*, cit.

riflette una frattura più profonda nell'architettura giuridica europea. Per comprenderla appieno occorre analizzare sia il meccanismo attraverso il quale avviene il cambiamento, sia le conseguenze ordinamentali che ne derivano.

Durante il periodo 2016-2025, il GDPR e i suoi successori (Digital Services Act, Digital Markets Act, AI Act, etc.) hanno affidato esplicitamente l'*enforcement* ad autorità nazionali decentralizzate (le *data protection authorities*, le *digital markets agencies*). Tale architettura diffusa era consapevolmente costruita per prevenire il rischio di "*regulatory capture*"⁹⁸: nessun ente avrebbe avuto potere sufficiente per diventare bersaglio dell'industria di suo riferimento; la diversità di approcci e la frammentazione fra le autorità nazionali avrebbe protetto più efficacemente il pluralismo.

Il Digital Omnibus, tuttavia, rovescia questa logica di responsabilità diffusa. Come già evidenziato (§ 3), esso attribuisce alla Commissione – tramite l'AI Office – competenza esclusiva su due categorie di sistemi: i modelli GPAI proprietari (in cui mezzo e infrastruttura appartengono al medesimo fornitore) e i sistemi di IA integrati nelle grandi piattaforme digitali.

La centralizzazione delle competenze presso un unico organo aumenta la concentrazione dei destinatari dell'attività di *lobbying* e riduce i contrappesi istituzionali. La ricerca empirica sul fenomeno della cattura regolatoria conferma questi rischi⁹⁹. Le *Big tech*, con budget operativi all'interno delle istituzioni europee pari a centinaia di milioni di dollari annui¹⁰⁰, dispongono di notevole capacità di influenza nei confronti dell'AI Office. Emerge così un paradosso: la centralizzazione persegue l'efficienza e il controllo, ma accresce il rischio di *regulatory capture*. Tale contraddizione rappresenta la principale vulnerabilità del sistema nel medio-lungo termine, poiché aumenta il pericolo che a livello centrale si possa erodere la visione centrata

⁹⁸ W. Y. Li, *Regulatory capture's third face of power*, in *Socio-Economic Review*, 21(2), 2023, 1217 ss. L'autrice sottolinea come, nonostante l'apparente semplicità della fattispecie, in realtà l'ipotesi di *regulatory capture* sia molto più sfaccettata di quanto si creda. Evitando di perdersi nelle singole interpretazioni, riducendo il fattore al suo minimo, si può definire questa distorsione come quei casi in cui una determinata autorità pubblica di controllo finisce per essere gestita e macchinata dagli stessi controllati a danno della collettività.

⁹⁹ Sul tema, considerato che il fenomeno in esame non è circoscritto al solo ambito digitale, si può fare riferimento a fonti eterogenee, riconducibili tanto alla letteratura economica quanto a quella giuridica, nonché a studi provenienti da diversi contesti geografici. Si vedano E. Dal Bó, *Regulatory Capture: a review*, in *Oxford Review of Economic Policy*, 22(2), 2006, 203 ss.; D. Carpenter - D.A. Moss, (eds.), *Preventing regulatory capture: Special interest influence and how to limit it*, Cambridge, 2013; K. Kausche - M. Weiss, *Platform power and regulatory capture in digital governance*, in *Business and Politics*, 27(2), 2025, 284 ss.

¹⁰⁰ Tra 2023 e 2025 le grandi società digitali hanno speso per le sole Istituzioni europee circa 360 milioni di euro, di cui 150 solo nel 2025. *Big Tech lobby budgets hit record levels*, in *CorporateEurope.org*, 29 ottobre 2025. Le distinte somme versate possono essere controllate periodicamente nel [Registro europeo per la trasparenza](#).

sui diritti fondamentali in favore di un regime normativo meno vincolante, nel quale la tecnologia diviene fine in sé, anziché rimanere strumento al servizio dei diritti.

Questo meccanismo di “liquefazione regolatoria”¹⁰¹ si iscrive in un fenomeno più ampio e preoccupante. Alcuni studiosi di *governance* hanno recentemente coniato il termine “*Broligarchy*” per designare l’ascesa delle grandi multinazionali digitali come nuovo centro di potere, capace di condizionare gli Stati nazionali, in particolare negli Stati Uniti¹⁰². Desta particolare preoccupazione la tendenza di tali imprese a operare *de facto* come istituzioni politiche, esercitando funzioni che dovrebbero essere riservate al settore pubblico. A differenza delle istituzioni, tuttavia, certe entità private non sono vincolate da meccanismi di *accountability* democratica e rispondono esclusivamente ai propri interessi economici¹⁰³.

¹⁰¹ L’espressione è impiegata in chiave analogica rispetto alla nozione di *modernità liquida* elaborata da Zygmunt Bauman, con cui si descrive una condizione sociale caratterizzata dalla dissoluzione delle strutture stabili, dalla precarietà dei legami collettivi e dall’individualizzazione delle responsabilità in assenza di un corrispondente potere effettivo di controllo sui processi sistemici. In tale prospettiva, per “liquefazione regolatoria” si intende non tanto una riduzione quantitativa dell’intervento normativo, quanto una trasformazione qualitativa delle forme della regolazione, che tendono a perdere stabilità, prevedibilità e centralità istituzionale, trasferendo sul soggetto privato poteri di gestione del rischio precedentemente mediati da strutture collettive.

¹⁰² Il termine «broligarchia» (neologismo formato da *brother* e *oligarchia*) è emerso nel dibattito pubblico in relazione a una fase recente della politica statunitense. In particolare, ha suscitato attenzione il fatto che, già in occasione della cerimonia di insediamento presidenziale, alcuni dei più influenti dirigenti delle principali piattaforme digitali globali hanno manifestato, in forme diverse, una convergenza con l’ideologia riconducibile allo slogan *Make America Great Again* (MAGA). In cambio di tale allineamento, figure come Elon Musk sono state descritte da alcuni osservatori come beneficiarie di un ruolo particolarmente rilevante nell’assetto del potere politico e istituzionale. Per queste ragioni, si è parlato dell’emergere di una «nuova oligarchia» negli Stati Uniti. Nello specifico, l’oligarchia di quei ragazzi/giovani adulti di inizio millennio (nel gergo “*bro*”) amanti della tecnologia e dei mezzi elettronici. Per avere un’idea ancora più chiara di questo contesto, si rimanda anche alla visione del pluripremiato lungometraggio di David Fincher *The Social Network*, incentrato sulla storia del fondatore di Facebook Mark Zuckerberg. Cfr. anche L. Norden - D. I. Weiner, *The rise of America’s Broligarchy and what to do about it*, in *Time*, 12 febbraio 2025.

¹⁰³ L’emergere di questi nuovi poteri privati non è un fenomeno nuovo nel dibattito della dottrina giuridica. Ormai da un decennio si è cominciato a discutere a riguardo del tema e varie opinioni si sono venute a delineare su come lo Stato dovrebbe agire, rispettivamente, per aiutare o per scoraggiare questi nuovi protagonisti della nostra epoca. *Ex multis*, si rimanda a: A. Chander, *Who Runs the Internet?* in W. Sandholtz - J. A. McCone (eds.), *Research Handbook on the Politics of International Law*, Cheltenham-Northampton, 2017, 418 ss.; M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista de Il gruppo di Pisa*, 2, 2021, 166 ss.; O. Grandinetti, *Le piattaforme digitali come “poteri privati” e la censura online*, in *Rivista italiana di informatica e diritto*, 1, 2022; E. Cremona, *I poteri privati nell’era digitale. Libertà fondamentali, regolazione del mercato, tutela dei diritti*, Napoli, 2023.

Nel contesto del Digital Package, gli effetti di siffatto fenomeno si rovesciano in almeno tre dimensioni interconnesse. *In primis*, c'è la questione della concentrazione del mercato e del potere statale esercitato dai nuovi Leviatani digitali¹⁰⁴. Il DOAI, ad esempio, condensando il ruolo di supervisione presso la Commissione, crea una relazione bilaterale Commissione-Big tech in cui il vantaggio informativo e di potere rimane chiaramente con le aziende (che controllano gli algoritmi, i dati e l'*expertise* tecnica). L'AI Office della Commissione, pur teoricamente dotato di poteri di *enforcement*, rimane dipendente dalle informazioni e conoscenze fornite dalle stesse aziende che dovrebbe regolamentare¹⁰⁵.

In secondo luogo, c'è la questione dell'asimmetria nell'attività di *lobbying*. Come anticipato poco sopra, le spese di *lobbying* delle grandi società del tech presso le istituzioni europee hanno raggiunto la cifra di circa €150 milioni annuali. A titolo di confronto, il budget dell'intero AI Office della Commissione è stato stimato inizialmente in meno di un terzo della cifra spesa dalle aziende¹⁰⁶. La sproporzione di risorse comporta che il potere di persuasione dell'industria supera evidentemente quello dell'istituzione pubblica. Non è questione di malafede intenzionale, ma di semplice economia di potere: le aziende hanno incentivi finanziari enormi a smobilizzare risorse lobbistiche; le agenzie pubbliche hanno budget limitati e non possono competere su questo terreno.

Terza, e forse più rilevante strutturalmente, viene a mancare quello che l'economista Galbraith avrebbe individuato come "*countervailing power*" – ossia la capacità di altri attori (sindacati, associazioni di consumatori, o anche un tessuto sociale organizzato e politicizzato che possa riferirsi ai poteri dello Stato con dovuta coscienza) di esercitare pressione contraria e bilanciare il potere aziendale in una dinamica fruttuosa¹⁰⁷.

¹⁰⁴ M.D. Garasic, *Leviatano 4.0. Politica delle nuove tecnologie*, Roma, 2022.

¹⁰⁵ F. Pizzetti - S. Calzolaio - A. Iannuzzi - E. Longo - M. Orofino, *La regolazione europea dell'intelligenza artificiale*, cit.

¹⁰⁶ G. Volpicelli, *EU needs 'Oppenheimers' to run AI policy*, in *Politico*, 6 marzo 2024.

¹⁰⁷ Il termine, come accennato, è stato introdotto dall'economista J.K. Galbraith nel 1952 per descrivere, in origine, la capacità dei grandi acquirenti operanti nei mercati a valle di ottenere condizioni più favorevoli dai fornitori. Più precisamente, l'attenzione dell'autore si concentrava sul ruolo di poteri intermedi idonei a controbilanciare le asimmetrie strutturali del sistema economico (nel caso di specie, il mercato), contribuendo così a renderne il funzionamento complessivo più equilibrato ed efficiente per le parti coinvolte. Trasponendo tale categoria interpretativa al contesto attuale, si può osservare come nell'ecosistema digitale tenda a mancare un livello intermedio di potere capace di riequilibrare i rapporti tra i diversi attori. Ne deriva il rischio di una strutturazione delle relazioni in forma prevalentemente bilaterale tra soggetti privati dotati di ingenti risorse e autorità pubbliche, con conseguente indebolimento delle dinamiche di bilanciamento tipiche dei modelli pluralistici. Cfr. S. Kesting, *Countervailing, Conditioned, and Contingent: the power theory of John Kenneth Galbraith*, in *Journal of Post Keynesian Economics*, 28(1), 2005, 3 ss.

Nel contesto del Digital Omnibus, tale potere è sistematicamente indebolito. Le associazioni dei consumatori europee dispongono di budget neppure comparabili a quelli delle Big tech. Le associazioni per i diritti digitali (ad esempio EDRi) hanno scarso accesso diretto all'AI Office. I sindacati, tradizionali rappresentanti del *countervailing power*, possiedono scarsa *expertise* tecnologica per dialogare efficacemente con i soggetti *leader* dello sviluppo digitale. In altre parole, l'architettura istituzionale della riforma rischia di produrre una struttura di potere profondamente sbilanciata, in cui le grandi società operano come *de facto-state actors* imponendo la loro voce a discapito di tutti gli altri soggetti potenzialmente interessati.

5. Considerazioni conclusive

Compiuta questa ricostruzione, è possibile formulare alcune considerazioni conclusive di ordine generale: il Digital Package, lungi dal rappresentare un mero "aggiustamento tecnico" del panorama digitale europeo, appare come un passaggio di fase nella razionalità regolativa dell'Unione, segnato dal graduale slittamento da obblighi giuridicamente esigibili verso meccanismi più liquidi e semplificati. Tale cedimento incide direttamente sull'effettività dei diritti; esso rischia di trasformare la grammatica del costituzionalismo europeo (diritti come limite e doveri positivi in capo a pubblici poteri e operatori economici) in una semantica più astrusa e debole, nella quale la tutela è spesso affidata a norme complesse oppure a programmi, linee guida e, in ultima istanza, alla volontà conformativa degli stessi soggetti regolati.

In prospettiva, l'accentramento di poteri e competenze presso pochi organismi e la riallocazione di snodi decisionali a livello sovranazionale non devono essere letti esclusivamente nella chiave dell'efficienza amministrativa, bensì anche come ristrutturazione dei rapporti di forza entro cui si produce la normatività effettiva. Laddove l'interazione regolativa si riconfigura come relazione tendenzialmente bilaterale tra Commissione e grandi operatori tecnologici, il rischio non è soltanto quello – già ampiamente discusso in letteratura¹⁰⁸ – della cattura regolatoria in senso stretto, ma quello più ampio di una "cattura epistemica": l'autorità pubblica, pur dotata formalmente di poteri, finisce per dipendere in modo organico dalle strutture private, cambiando il paradigma dei rapporti tra le due sfere. Ne discende un potenziale indebolimento della catena di *accountability* democratica, perché la responsabilità per gli esiti (discriminazioni, compressioni dell'autonomia individuale, erosione della privacy effettiva) tende a disperdersi tra livelli e attori, rendendo opaca l'individuazione del centro decisionale imputabile.

¹⁰⁸ Note *supra* 98-99.

In tale contesto, l'ipotesi di una reazione costituzionale “dal basso” – tramite il sindacato dei tribunali ordinari e delle Corti costituzionali nazionali, organi chiamati a confrontarsi con effetti concreti e non soltanto con architetture normative astratte – assume rilievo non come prospettiva contingente, bensì come possibile meccanismo di riequilibrio. Qualora l'attuazione del Digital Package accentuasse la vaghezza precettiva, la riduzione dell'esigibilità dei diritti e la difficoltà di identificare un responsabile effettivamente controllabile, non è implausibile che l'intervento giurisprudenziale riattivi, in forme nuove, il lessico della certezza del diritto e della tutela sostanziale dei diritti fondamentali¹⁰⁹.

Da ultimo, la questione decisiva – e propriamente politica nel senso più alto del termine – riguarda la tenuta dell’“effetto Bruxelles¹¹⁰” quale strumento di proiezione esterna del modello europeo. Tale dinamica presuppone non soltanto l'esistenza di un assetto normativo formale, ma anche la credibilità del paradigma proposto: la capacità di rendere effettive le pretese regolative, di stabilizzare le aspettative e di dimostrare che i diritti non restano enunciazioni di principio, bensì si traducono in situazioni

¹⁰⁹ Con ciò, acutizzando un conflitto istituzionale latente tra razionalità legislativa-tecnocratica e razionalità giudiziale-costituzionale. Il rapporto tra potere giudiziario e poteri politico-economici costituisce uno dei nodi strutturali delle democrazie costituzionali contemporanee e, se si guarda al contesto italiano, assume una fisionomia particolarmente complessa per ragioni storiche, istituzionali e culturali. La letteratura giuridica italiana ha affrontato tale fenomeno secondo prospettive diverse: storico-istituzionale, con riferimento all'evoluzione dell'ordinamento giudiziario e delle garanzie di indipendenza; teorico-costituzionale, attraverso la rielaborazione del principio di separazione dei poteri e del ruolo dei “contropoteri” nello Stato di diritto; politico-istituzionale, analizzando i processi di politicizzazione della giurisdizione e di giurisdizionalizzazione della politica; infine, socio-giuridica, considerando l'impatto delle dinamiche economiche e mediatiche sulla legittimazione della magistratura. I contributi qui richiamati – afferenti pur sempre alla dottrina nostrana – si collocano entro questo quadro problematico e offrono strumenti concettuali e ricostruttivi utili a comprendere le radici, le trasformazioni e le criticità di questo complesso rapporto. Cfr. S. Sicardi (a cura di), *Magistratura e democrazia italiana: problemi e prospettive*, Napoli, 2010; G. Ferri, *Autonomia e indipendenza della magistratura tra 'vecchio' e 'nuovo' ordinamento giudiziario*, in *Rivista AIC*, 4, 2017; L. Pipino, *Magistratura e politica*, in *Costituzionalismo.it*, 1, 2022, 59 ss. Per quanto riguarda il rapporto tra politica e giurisdizione costituzionale si rimanda, *ex multis*, a: G. Zagrebelsky, *La Corte in-politica*, Intervento del Prof. Gustavo Zagrebelsky in occasione del XXIII Premio Giuseppe Chiarelli, Palazzo della Consulta, 20 ottobre 2004; A. Morrone, *Suprematismo giudiziario. Su sconfinamenti e legittimazione politica della Corte costituzionale*, in *Quaderni costituzionali*, 2, 2019, 251 ss.; N. Zanon, *Su alcune questioni e tendenze attuali intorno alla motivazione delle decisioni della Corte costituzionale, tra forma e sostanza*, in V. Marcenò - M. Losano (a cura di), *Come decide la Corte dinanzi a «questioni tecniche»*. *Incontri sulla giurisprudenza costituzionale*, Soveria Mannelli, 2020, 25 ss.

¹¹⁰ A. Bradford, *The Brussels Effect. How the European Union Rules the World*, Oxford, 2020. Per un confronto tra i tre poli presi in considerazione nel presente Saggio si rimanda anche a A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, Oxford, 2023.

giuridiche concretamente esercitabili, idonee a incidere sulle condizioni di vita della collettività e dei singoli. Se l'Unione sostituisce progressivamente obblighi e controlli con *governance* complesse ma morbide, essa rischia di indebolire proprio la condizione che, nell'ultimo decennio, ha reso il suo modello esportabile: l'idea che la regolazione europea sia al contempo garantista, operativa e fruttuosa per chi ne accoglie il disegno. Ne deriva un paradosso: nel tentativo di "alleggerire" l'ordinamento per ragioni di competitività, si può finire per ridurre sia la protezione effettiva dei cittadini, sia l'attrattiva sistemica del quadro europeo, rendendo l'Europa non un terzo polo, ma un ordinamento intermedio, meno incisivo e più vulnerabile alle pressioni dei nuovi poteri privati transnazionali.

Alla luce di quanto precede, la proposizione di simili riforme non dovrebbe essere valutata soltanto in termini di semplificazione o di efficientamento amministrativo, ma come scelta costituzionale implicita: una scelta sul grado di vincolatività della tutela, sull'idea della responsabilità degli enti e, in definitiva, sul tipo di cittadinanza digitale che l'UE intende riconoscere. La domanda che resta aperta – e che segna l'effettivo punto di chiusura di questa analisi – è se le istituzioni rappresentative, gli organi giurisdizionali e la società civile riusciranno a ricondurre la probabile transizione in atto entro una traiettoria coerente con il nucleo duro del costituzionalismo europeo¹¹¹, oppure se prevarrà una trasformazione silenziosa, con effetti difficilmente reversibili sull'assetto democratico e sulla proiezione geopolitica dell'Unione nell'era della società digitale.

¹¹¹ Per una riflessione più ampia (che non riguarda solo il diritto costituzionale europeo ma tutto l'assetto etico, giuridico e sociale occidentale) si rimanda al saggio divulgativo di U. Mattei, *La fine del diritto. La grande sostituzione tecnologica nell'era nuova*, Milano, 2025.

Abstract

Le proposte di riforma della Commissione europea in materia di legislazione digitale, presentate originariamente nel novembre 2025, si inseriscono in un più ampio processo di ridefinizione del rapporto tra regolazione dei mercati tecnologici e tutela dei diritti fondamentali nell'ordinamento dell'Unione. In tale contesto, il contributo analizza la tensione multilaterale tra esigenze di semplificazione normativa e obiettivi di competitività economica, da un lato, e la tradizionale centralità dei diritti e delle garanzie, dall'altro. Muovendo da una prospettiva costituzionale e comparata, si sostiene che la crescente pressione geopolitica esercitata dai modelli statunitense e cinese non implichi necessariamente il bisogno di un ripensamento in senso deregolatorio dell'approccio europeo.

Al contrario, si argomenta che la specificità dell'ordinamento dell'Unione possa rappresentare un modello alternativo di regolazione delle tecnologie digitali, fondato su un equilibrio tra innovazione, mercato e diritti fondamentali. Per raggiungere questo traguardo, tuttavia, serve che l'Unione metta in risalto il ruolo dei cittadini, informandoli e rafforzando la loro posizione nei confronti dei poteri privati del settore.

The European Commission's proposed reform of digital legislation, presented at the end of 2025, forms part of a broader process of redefining the relationship between the regulation of technology markets and the protection of fundamental rights within the EU legal order. In this context, this paper analyses the tension between the need for regulatory simplification and economic competitiveness objectives, on the one hand, and the traditional centrality of rights, on the other. Adopting a constitutional and comparative perspective, it argues that the growing geopolitical pressure exerted by the American and Chinese models does not necessarily imply the need for a deregulatory rethinking of the European approach. On the contrary, it is argued that the specific nature of the EU legal order could represent an alternative model for the regulation of digital technologies, based on a balance between innovation, economic prosperity and fundamental rights. To achieve this goal, however, the EU must support more citizens, informing them and strengthening their position with private sector powers.

Keywords

Digital Omnibus – personal data – artificial intelligence – digital regulation – law and policy