Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 – Anticipazione fascicolo
V ed. Incontro fra i giovani studiosi di diritto UE

I confini del diritto dell'Unione nella regolazione dell'IA: il caso dei sistemi a rischio minimo

Davide Baldini*

SOMMARIO: 1. L'architettura regolatoria dell'AI Act e i suoi limiti strutturali. – 2. Le lacune nella categorizzazione dei sistemi di IA. – 3. La natura dell'armonizzazione operata dall'AI Act: perimetro applicativo e vincoli per gli Stati membri. – 4. AI Act e disciplina dell'uso dei sistemi di IA: tra armonizzazione selettiva e spazi di autonomia residua. – 5. Mercato interno e diritti fondamentali: le restrizioni sull'utilizzo dei sistemi di IA alla luce del fondamento mercantilistico dell'AI Act. – 6. Le discipline nazionali sull'utilizzo dei sistemi di IA: tra spazi di autonomia residua e profili di tensione con il diritto dell'Unione. – 7. Vuoti regolatori e conflitti normativi: quale futuro per la regolamentazione dell'intelligenza artificiale nell'Unione?

1. *L'architettura regolatoria dell'AI Act e i suoi limiti strutturali*

Il regolamento (UE) 2024/1689 ("AI Act")[1], proposto dalla Commissione europea nel 2021 e adottato in via definitiva nel 2024,

* Dottorando in *European and Transnational Legal Studies* presso l'Università di Firenze e l'Università di Maastricht (co-tutela).

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858,

rappresenta il primo tentativo organico a livello globale di disciplinare lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale secondo un approccio giuridico orizzontale e sistematico. L'AI Act adotta un approccio regolatorio basato sul rischio ("*risk-based approach*") per i diritti fondamentali, la sicurezza e lo stato di diritto. Si tratta di un modello di regolazione che classifica "a monte" i sistemi di IA in funzione della loro finalità di utilizzo prevista[2], operando una classificazione in sistemi a rischio inaccettabile, elevato e limitato (o "di trasparenza") prevedendo, per ciascuna categoria, obblighi proporzionati al potenziale impatto delle tecnologie coinvolte[3].

Sempre in punto di tecnica regolatoria, l'AI Act adotta il paradigma del *New Legislative Framework* ("NLF"), ossia il quadro normativo introdotto dall'Unione europea a partire dal 1985 per armonizzare la disciplina di alcuni prodotti e promuoverne la libera circolazione nel mercato interno, attraverso l'armonizzazione delle normative in materia di produzione e commercializzazione[4]. Applicando tale modello al settore dell'intelligenza artificiale, il regolamento estende allo sviluppo,

(UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

[2] La distinzione tra l'approccio basato sul rischio "a monte" ("*top down*") dell'AI Act – in cui è la normativa stessa ad identificare *ex ante* categorie di rischio, stabilendone limiti e obblighi – e quello "a valle" ("*bottom up*") adottato dal GDPR (regolamento (UE) 2016/679) – dove i destinatari degli obblighi (titolari del trattamento) sono chiamati a valutare autonomamente i rischi delle proprie attività e a definire le misure di mitigazione più adatte sulla base del principio di *accountability* – è ben espressa da: G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *CMLR*, n. 59, 2022, pp. 473-500.

[3] Il presente contributo si concentra sugli aspetti di regolazione dei sistemi di intelligenza artificiale. Resta, pertanto, esclusa dall'analisi la disciplina dei modelli di IA per finalità generali di cui al Capo V dell'AI Act, la quale si configura come del tutto autonoma rispetto a quella dei sistemi di IA.

[4] Risoluzione del Consiglio 85/C 136/01, del 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione. Successivamente, il quadro regolatorio del NLF è stato consolidato nel regolamento (CE) 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e che abroga il regolamento (CEE) n. 339/9, nella decisione 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE e nel regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011.

distribuzione e utilizzo dei sistemi di IA gli strumenti tipici del NLF, come le procedure di valutazione di conformità ai requisiti essenziali dettati della normativa e l'apposizione della marcatura "CE" sul prodotto, a cui consegue la possibilità di commercializzarlo in tutta l'Unione[5]. In questo contesto, i sistemi di IA sono dunque considerati alla pari di un prodotto, la cui fabbricazione e commercializzazione sono assoggettate a requisiti essenziali di conformità da verificare attraverso procedure standardizzate tramite auto-certificazione o, in ipotesi limitate, controlli di terza parte. In caso di esito positivo, è possibile apporre la marcatura "CE" sul prodotto e commercializzarlo nel mercato di ogni Stato membro. In questa architettura, un ruolo centrale viene affidato agli operatori di sistemi di IA[6], che sono generalmente tenuti ad auto-certificare la conformità del proprio sistema di IA, nonché alle autorità nazionali di vigilanza del mercato[7].

Al fine di tracciare il proprio ambito di applicazione, l'AI Act definisce "sistema di IA" «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[8]. La definizione in parola è stata mutuata e riflette da vicino quella stabilita nella raccomandazione OCSE

[5] Per un'analisi critica in merito all'adeguatezza del quadro regolatorio del NLF per regolamentare i sistemi di IA si veda, *ex multis*: M. VEALE, F. Z. BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, in *Computer Law Review International*, n. 22, 2021, pp. 97-112, spec. p. 102; E. CIRONE, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in questa *Rivista*, n. 2, 2024, pp. 51-71.

[6] Con questa espressione l'AI Act identifica tutti i soggetti che, a vario titolo, risultano coinvolti nel ciclo di vita del sistema di IA. L'art. 3, par. 8, AI Act definisce come "operatore": «un fornitore, un fabbricante del prodotto, un *deployer*, un rappresentante autorizzato, un importatore o un distributore».

[7] Per un'analisi del sistema di vigilanza previsto dall'AI Act, si veda: S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in questa *Rivista*, n. 2, 2024, pp. 125-145.

[8] Per un'analisi della definizione e degli ampi confini della stessa, si veda: D. FERNÁNDEZ-LLORCA ET AL., *An Interdisciplinary Account of the Terminological Choices by EU Policymakers Ahead of the Final Agreement on the AI Act: AI System, General Purpose AI system, Foundation Model, and Generative AI*, in *Artificial Intelligence Law*, 2024.

sull'Intelligenza Artificiale[9] nell'ottica di favorire la convergenza su una nozione globale e favorire, così, la creazione di un "effetto Bruxelles" da parte dell'AI Act[10]. Tale definizione, assai ampia[11], disegna l'ambito di applicazione materiale del regolamento[12] ed è dunque di fondamentale importanza.

Al netto dei divieti di sviluppo, commercializzazione e utilizzo[13] previsti per i sistemi a rischio inaccettabile tassativamente elencati all'art. 5, la categoria destinataria della quasi totalità degli obblighi è quella dell'alto rischio, consistente in un numero limitato di sistemi anch'essi tassativamente elencati all'art. 6, per la quale vengono imposti requisiti stringenti lungo tutto il ciclo di vita del sistema[14]. Altri obblighi, principalmente di trasparenza e dalla portata assai limitata, vengono previsti per alcune ulteriori categorie di sistemi individuate all'art. 50, AI Act, talvolta indicati come "sistemi a rischio di trasparenza" o, più comunemente, "sistemi a rischio limitato"[15]. Tuttavia, come riconosciuto dalla stessa Commissione, la grande

---

[9] OCSE, *Explanatory memorandum on the updated OECD definition of an AI system*, in *OECD Artificial Intelligence Papers*, n. 8, 2024.

[10] E. CIRONE, *op. cit*. Sul tema più generale dell' "effetto Bruxelles" si veda: A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020.

[11] L'ampio campo di applicazione cattura alcune caratteristiche comuni alla maggior parte dei *software* oggi comunemente in uso, come osservato da: M. VEALE, F. Z. BORGESIUS, *op. cit.*, p. 109; D. FERNÁNDEZ-LLORCA ET AL., *op. cit.*

[12] Art. 2, par. 1, AI Act.

[13] Fatti salvi i sistemi di riconoscimento biometrico in tempo reale e in luogo aperto al pubblico per finalità di pubblica sicurezza, per i quali l'utilizzo viene strettamente regolato (mediante un divieto soggetto a eccezioni), ma non ne viene vietata la produzione o la distribuzione. Cfr. art. 5, par. 1, lett. *h)*, AI Act.

[14] Tali obblighi insistono su tutti gli operatori di sistemi di IA, seppur con diversa intensità, e sono per la maggior parte vigenti in capo al fornitore e, in misura minore, al *deployer*. Essi sono indicati agli artt. 8-27, AI Act, e comprendono, principalmente l'istituzione di un sistema di gestione del rischio e un sistema di gestione della qualità, obblighi di assicurare la qualità dei dati usati per l'addestramento e l'utilizzo del sistema, la redazione e aggiornamento della documentazione tecnica inerente al sistema, obblighi di garantire un'adeguata supervisione umana, requisiti di robustezza, resilienza e cybersicurezza del sistema, obblighi di svolgere valutazioni d'impatto sui diritti fondamentali.

[15] Tale espressione è utilizzata dalla stessa Commissione europea, nell'ambito del grafico "a piramide" che illustra le categorie di rischio previste dal regolamento. Si veda la pagina informativa sull'AI Act: www.digital-strategy.ec.europa.eu/it/policies/regulatoryframeworkai#:~:text=La%20legge%20sull'IA%20 (regolamento,un'IA%20affidabile%20in%20Europa).

maggioranza dei sistemi di IA oggi presenti sul mercato dell'Unione non rientra in alcuna delle categorie di rischio previste dalla normativa, ma si colloca nella vasta area residuale dei cosiddetti sistemi a rischio "minimo"[16]. È importante sottolineare che, per tali sistemi, l'AI Act non impone alcun obbligo specifico agli operatori, limitandosi a raccomandare l'adozione volontaria di codici di condotta o buone pratiche[17].

Il legislatore dell'Unione ha quindi disegnato un ambito di applicazione materiale assai ampio, facendo leva sulla nozione di "sistema di IA" sopra esaminata, al quale non fa però seguito una disciplina altrettanto estesa del fenomeno dell'intelligenza artificiale. Viene così a prodursi un notevole disallineamento tra ambito di applicazione materiale (esteso a tutti i sistemi di IA, inclusi quelli a rischio minimo) e relativi obblighi sostanziali, presenti unicamente per i sistemi a rischio inaccettabile, ad alto rischio e a rischio limitato. Tale disallineamento, che risulta insolito nell'ambito degli strumenti normativi afferenti al *New Legislative Framework*, crea una "forbice" tra l'area in cui l'Unione afferma la propria competenza – ossia, tutta l'area dei "sistemi di IA" – e quella dove il legislatore ha effettivamente imposto obblighi per gli operatori di sistemi di IA.

La presente analisi intende quindi interrogarsi sulle implicazioni di tale disallineamento tra ambito applicativo e obblighi sostanziali, con particolare riguardo ai margini di intervento eventualmente residui in capo agli Stati membri nei settori che rientrano formalmente nell'ambito di applicazione del regolamento senza però dettare una disciplina, inserendosi nel dibattito dottrinale già in corso[18]. A tal fine,

---

[16] Commissione europea, pagina informativa sull'AI Act, disponibile presso www.digital-strategy.ec.europa.eu/it/policies/regulatory-framework-ai: «La legge sull'IA non introduce norme per l'IA ritenute a rischio minimo o nullo. La stragrande maggioranza dei sistemi di IA attualmente utilizzati nell'UE rientra in questa categoria. Ciò include applicazioni come videogiochi abilitati all'intelligenza artificiale o filtri antispam». L'espressione "sistemi a rischio minimo" non si rinviene dunque nel testo del regolamento, ma è così informalmente definita dalla Commissione europea.

[17] A rigore, risulta applicabile l'obbligo di "Alfabetizzazione in materia di IA" previsto all'art. 4 del regolamento per tutti i sistemi di IA, a prescindere dalla categoria di rischio. Tale obbligo, tuttavia, risulta sprovvisto di sanzione.

[18] Si vedano, tra gli altri: C. BURELLI, *Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità?*, in questa *Rivista*, n. 2, 2024; B.

il contributo si articola come segue: il paragrafo 2 mette in luce le lacune nella categorizzazione dei sistemi di IA e i problemi che ne derivano per la tutela effettiva dei diritti fondamentali; il paragrafo 3 esamina la natura dell'armonizzazione operata dall'AI Act alla luce della base giuridica nei Trattati, evidenziando i vincoli che ne discendono per gli Stati membri; il paragrafo 4 analizza la disciplina dell'uso dei sistemi di IA, distinguendo tra ambiti pienamente armonizzati e spazi di autonomia residua; il paragrafo 5 riflette sull'orientamento mercantilistico dell'AI Act e sulle tensioni con la tutela dei diritti fondamentali; il paragrafo 6 analizza alcune disposizioni normative nazionali in materia di utilizzo dei sistemi di IA, valutandone la compatibilità con il quadro di armonizzazione delineato dall'AI Act; infine, il paragrafo 7 conclude discutendo i possibili vuoti regolatori e i conflitti normativi che ne possono derivare, suggerendo che tali tensioni possano dar luogo a contrasti tra diritto dell'Unione e diritto nazionale.

2. *Le lacune nella categorizzazione dei sistemi di IA*

Come sopra osservato, l'AI Act si caratterizza per un ampio disallineamento strutturale tra l'ampiezza dell'ambito applicativo formale (molto estesa) e il perimetro degli obblighi sostanziali (assai limitato).

Tale disallineamento diviene particolarmente problematico alla luce di una ulteriore criticità già ampiamente discussa in dottrina[19], ossia la presenza di lacune nella categorizzazione del rischio dei sistemi di IA,

---

MARCHETTI, *Intelligenza artificiale, poteri pubblici e rule of law*, in *RIDPC*, n. 1, 2024, p. 49 ss.; G. GALLONE, *L'improcrastinabile esigenza di tracciare una via "italiana" per l'intelligenza artificiale nel procedimento amministrativo. Opportunità e legittimità di un intervento regolatorio nazionale a corredo dell'AI Act*", in *Giustizia Insieme*, 2025; M. INGLESE, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in questa *Rivista*, n. 2, 2024; M. VEALE, F. Z. BORGESIUS, *op. cit.*, pp. 108-110.

[19] L'impiego della tecnica legislativa del *New Legislative Framework* per tutelare i valori anzidetti risulta problematico, come evidenziato in dottrina. Sul punto si veda, *ex multis*: E. CIRONE, *op. cit.*; G. MALGIERI, C. SANTOS, *Assessing the (Severity of) Impacts on Fundamental Rights*, in *Computer Law & Security Review*, vol. 56, 2025, pp. 106-113; M. VEALE, F. Z. BORGESIUS, *op. cit*.

le quali appaiono difficilmente giustificabili da un punto di vista di tutela dei diritti fondamentali, della sicurezza e dello stato di diritto. Infatti, sebbene il regolamento dichiari tra i propri obiettivi la tutela di questi tre valori, le scelte del legislatore non sempre risultano coerenti con tali finalità: molti sistemi di IA suscettibili di generare rischi concreti e non trascurabili per i diritti e le libertà (discriminazioni, manipolazioni, dipendenze psicologiche, gravi asimmetrie informative, per citare i principali) sono stati ricondotti alla vasta categoria del "rischio minimo". Alcuni esempi possono aiutare a meglio inquadrare il problema.

È il caso, ad esempio, dei sistemi di *dynamic pricing*, utilizzati già da molti anni per stabilire in tempo reale il prezzo di prodotti e servizi venduti online. L'impiego di questi sistemi produce, secondo molteplici ricerche, gravi e sistematiche discriminazioni nei confronti di minoranze etniche, persone in condizioni di svantaggio economico e/o sociale e altri soggetti vulnerabili, il cui stato di bisogno per l'acquisto di determinati bene e servizi può condurre l'algoritmo a proporre prezzi più alti[20]. Nonostante tali evidenze risultino ampiamente documentate nella letteratura giuridica e scientifica, questi sistemi sono considerati "a rischio minimo" dall'AI Act e sfuggono, dunque, a qualsivoglia requisito tanto in merito allo sviluppo quanto all'utilizzo.

Anche il caso dei *chatbot* è emblematico. È ormai noto come l'interazione con tali sistemi possa portare persone in condizioni di vulnerabilità psicologica a dipendenze affettive che in alcuni casi sfociano nel ritiro completo dalla vita sociale o, finanche, al suicidio, come ampiamente documentato sia da studi scientifici[21] sia da recenti notizie di cronaca[22]. Nonostante ciò, l'AI Act considera tali sistemi

[20] *Ex multis*: L. DRECHSLER, J. C. B. SÀNCHEZ, *The Price Is (Not) Right: Data Protection and Discrimination in the Age of Pricing Algorithms*, vol. 9, n. 13, 2018; M. D. SUMON GAZI ET AL., *Ethical Considerations in AI-driven Dynamic Pricing in the USA: Balancing Profit Maximization with Consumer Fairness and Transparency*, in *Journal of Economics, Finance and Accounting Studies*, vol. 6, n. 2, 2024, pp. 100-111.

[21] *Ex multis*: A. YANKOUSKAYA ET AL., *Can ChatGPT Be Addictive? A Call to Examine the Shift from Support to Dependence in AI Conversational Large Language Models*, in *Hum.Cent. Intell. Syst.*, n. 5, 2025.

[22] Si tratta, in particolare, di individui – spesso, ma non sempre, con preesistenti problemi di carattere relazionale – che hanno sviluppato casi di vere e proprie relazioni sentimentali e estrema dipendenza nei confronti delle conversazioni con

come "a rischio limitato", assoggettandoli agli obblighi poco più che simbolici di cui all'art. 50, i quali si riducono all'obbligo di progettare il sistema in maniera tale da far sì che l'utente sia consapevole di stare interloquendo con una macchina, anziché con un essere umano.

Un ulteriore esempio è quello dei sistemi di raccomandazione ("*recommender systems*"), ossia sistemi basati su algoritmi finalizzati a suggerire contenuti, risultati di ricerca, prodotti o servizi a un utente, spesso basandosi su informazioni raccolte riguardo alle sue preferenze, comportamenti o caratteristiche simili ad altri utenti. Questi sistemi vengono utilizzati in una molteplicità di ambiti, tra cui la raccomandazione di contenuti da parte delle piattaforme – incluse quelle *social*, dove possono essere impiegati per promuovere contenuti estremisti e *fake news* su larghissima scala – nei motori di ricerca (ad esempio, *l'auto-fill* di Google o di qualsiasi altro motore di ricerca online), o nel campo della pubblicità personalizzata, che può arrivare ad includere forme particolarmente invasive come il *micro-targeting*, ovvero essere impiegati per promuovere servizi controversi come le scommesse online, che possono portare persone vulnerabili a compiere scelte contrarie ai propri interessi o a quelli della propria famiglia, a creare o a esasperare dipendenze (emblematico, in tal senso, il caso della pubblicità personalizzata online relativa ai siti di scommesse[23]).

L'esclusione di questi e di molti altri sistemi di IA[24] dalle categorie del rischio inaccettabile e dell'alto rischio – ossia, l'esclusione dalle due categorie di sistemi di IA destinatarie di effettivi obblighi – risultano difficilmente giustificabili alla luce dei già menzionati obiettivi di tutela[25]. Soprattutto, alla luce del disallineamento anzidetto, l'AI Act

chatbot. Ad esempio: I. EL ATILLAH, *Man ends his life after an AI chatbot zencouraged' him to sacrifice himself to stop climate change*, in *Euronews*, 2023; "*Mother says AI chatbot led her son to kill himself in lawsuit against its maker*", in *The Guardian*, 2024.

[23] F. MIHAI ET AL., *AI Personalization and Its Influence on Online Gamblers' Behavior*, in *Behavioural Sciences*, vol. 15, n. 6, 2025, p. 779 ss.

[24] Per una critica in tal senso, con specifico riguardo ai sistemi di IA utilizzati nel settore pubblico, si veda: G. GALLONE, *op. cit*. L'autore, sul punto osserva: «Eppure, non v'è dubbio che vi siano moltissime possibili applicazioni dell'IA nel settore pubblico non rientranti nell'elencazione di cui all'allegato III ma destinate ad incidere ugualmente in maniera significativa su diritti e libertà fondamentali dell'individuo».

[25] Simili esclusioni appaiono il frutto delle pressioni – invero assai forti – operate dall'industria dell'IA e dalle *Big Tech* durante il procedimento legislativo. Si veda sul

sembra produrre per tali sistemi un effetto perverso rispetto all'obiettivo dichiarato di proteggere i diritti fondamentali, la sicurezza e lo stato di diritto: non solo esclude tali sistemi da qualsiasi obbligo sostanziale, ma limita anche la possibilità per gli Stati membri di intervenire autonomamente per colmare le lacune, poiché essi rientrano comunque nella definizione di "sistema di IA" e, di conseguenza, nell'ambito di applicazione del regolamento.

Paradossalmente, è dunque proprio nella categoria del "rischio minimo" che si concentra il rischio maggiore: quello di produrre lacune di tutela per la maggior parte dei sistemi di IA oggi operativi nel mercato interno, incluse numerose casistiche che risultano tutt'altro che scevre di rischio.

3. *La natura dell'armonizzazione operata dall'AI Act: perimetro applicativo e vincoli per gli Stati membri*

Come appena osservato, l'AI Act produce una vasta area formalmente inclusa nel proprio ambito di applicazione, ma di fatto priva di tutele, ossia quella dei sistemi di IA "a rischio minimo". Questa area include, tuttavia, fattispecie concretamente problematiche nell'ottica di protezione dei diritti fondamentali, della sicurezza e dello stato di diritto. Quanto precede impone di chiarire la portata effettiva dell'armonizzazione realizzata dall'AI Act, ossia l'effettiva estensione del "campo occupato", al fine di comprendere se e in che misura essa precluda interventi nazionali volti a colmare i vuoti di tutela evidenziati al paragrafo precedente.

Ciò solleva dunque quesiti in ordine alla opportunità – se non alla vera e propria legittimità – della tecnica di armonizzazione adottata dal legislatore dell'Unione[26]. È dunque alla sua natura giuridica e alla base legale prescelta che occorre ora rivolgere l'attenzione, per verificare

---

punto: J. TALLBERG ET AL., *AI Regulation in the European Union: Examining Non-State Actor Preferences*, in *Business and Politics*, vol. 26, n. 2, 2023, pp. 218-239.

[26] G. GALLONE, *op. cit.*, il quale evidenzia le profonde tensioni che la lacunosa categorizzazione del rischio operata dall'AI Act è suscettibile di generare nei confronti dei principi supremi di rango costituzionale, evocando finanche la possibile attivazione dei contro-limiti. Si veda anche: M. VEALE, F. Z. BORGESIUS, *op. cit.*, pp. 108-110.

quali margini residuino, se del caso, agli Stati membri per sopperire alle anzidette lacune di tutela.

Come noto, caratterizzare l'estensione dell'armonizzazione richiede, in primo luogo, l'identificazione dell'ambito di applicazione materiale della misura (il "campo occupato") e, in secondo luogo, la determinazione della natura della competenza residua degli Stati membri all'interno di tale campo[27]. In tal senso, l'AI Act dichiara di stabilire «regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione» (art. 1, par. 1, AI Act). Il campo occupato, dunque, non è solo il Titolo III relativo ai sistemi "ad alto rischio" – ossia, come detto, i sistemi effettivamente destinatari di obblighi – ma tutta l'amplissima categoria dei "sistemi di IA". Secondo la valutazione d'impatto della Commissione, l'AI Act mira a «prevenire azioni unilaterali degli Stati membri che rischiano di frammentare il mercato e imporre oneri normativi ancora maggiori agli operatori che sviluppano o utilizzano sistemi di intelligenza artificiale»[28], indicando in maniera chiara – ancorché implicita – che il regolamento intende raggiungere un livello di armonizzazione massima.

Come noto, quando disposizioni di diritto derivato comportano una "armonizzazione massima", le capacità degli Stati membri di agire in quel settore vengono meno. In tal caso, in ossequio al principio del primato[29], gli Stati membri sono tenuti a disapplicare le eventuali norme nazionali confliggenti, applicare la normativa dell'Unione rilevante e, di conseguenza, accettare prodotti conformi a tale normativa nel proprio mercato. Se una disposizione, tuttavia, non realizza un'armonizzazione massima, ovvero armonizza solo determinate aree, gli Stati membri mantengono la competenza per adottare norme più rigorose.

Coerentemente con tale finalità di massima armonizzazione, da un lato, il cons. n. 1 dell'AI Act afferma che «Lo scopo del presente

---

[27] S. WEATHERILL, *The Fundamental Question of Minimum or Maximum Harmonisation*, in S. GARBEN, I. GOVAERE (eds.), *The Internal Market 2.0*, Oxford, 2020.

[28] Commissione europea, *Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206final, 2021, p. 57. Traduzione dell'autore.

[29] G. GAJA, A. ADINOLFI, *Introduzione al diritto dell'Unione europea*, Bari, 2014, pp. 180-187.

regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione»; dall'altro, sebbene il preambolo dell'AI Act individui una doppia base giuridica negli artt. 16 e 114 TFUE, il cons. n. 3 chiarisce che la base giuridica principale è quest'ultima[30]. Come noto, l'art. 114 TFUE, consente iniziative legislative dell'Unione volte a ottenere il ravvicinamento delle legislazioni nazionali, ove ciò si renda necessario a migliorare il funzionamento del mercato interno.

L'ulteriore base legislativa individuata nell'art. 16 TFUE, ovverosia nell'attuazione del diritto alla protezione dei dati di carattere personale, costituisce il fondamento di legittimità dell'AI Act per un numero assai limitato di disposizioni. In particolare, si tratta di quelle che impongono regole relative al trattamento dei dati personali, ossia con riguardo ai sistemi di IA per l'identificazione biometrica, quelli di polizia predittiva e quelli di categorizzazione biometrica, come espressamente chiarito dal cons. n. 3 dell'AI Act[31]. Si tratta dunque, a ben vedere, di una base giuridica complementare e circoscritta, funzionale a garantire la legittimità delle disposizioni specifiche relative al trattamento dei dati personali, – ancorandole, correttamente, al fondamento giuridico dell'art. 16 TFUE – senza alterare il carattere unitario e prevalente dell'art. 114 TFUE, quale fondamento generale dell'AI Act. Più in particolare, in linea con la giurisprudenza della Corte di giustizia, l'inserimento di una seconda base giuridica è giustificato dal fatto che,

[30] Quella delineata dall'art. 114, TFUE, è una "competenza concorrente"; di fatto, gli Stati membri possono legiferare in questo ambito solo nella misura in cui l'Unione non lo abbia già fatto, in ossequio al principio del primato del diritto dell'Unione: G. GAJA, A. ADINOLFI, *op. cit.*, pp. 128-135. Pertanto, nel momento in cui l'Unione legifera in questo ambito, gli Stati membri perdono la possibilità di farlo.

[31] Si veda, sul punto, il cons. n. 3 dell'AI Act, ultimo periodo: «Nella misura in cui il presente regolamento prevede regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, consistenti in limitazioni dell'uso dei sistemi di IA per l'identificazione biometrica remota a fini di attività di contrasto, dell'uso dei sistemi di IA per le valutazione dei rischi delle persone fisiche a fini di attività di contrasto e dell'uso dei sistemi di IA di categorizzazione biometrica a fini di attività di contrasto, è opportuno basare il presente regolamento, per quanto riguarda tali regole specifiche, sull'articolo 16 TFUE. Alla luce di tali regole specifiche e del ricorso all'articolo 16 TFUE, è opportuno consultare il comitato europeo per la protezione dei dati».

per taluni profili regolati dal testo normativo, la protezione dei dati personali costituisce un obiettivo autonomo e indissolubilmente connesso all'obiettivo principale di armonizzazione del mercato interno[32]. Pertanto, il ricorso all'art. 16 TFUE, si limita a fondare quelle previsioni che incidono direttamente sul trattamento e la protezione dei dati personali, in particolare nelle ipotesi di utilizzo dei sistemi di IA in contesti di particolare delicatezza quali l'identificazione biometrica e le attività di contrasto[33].

In base a quanto precede, ne consegue che la base giuridica fondante la legittimità del regolamento resta, in via preponderante, l'art. 114 TFUE, mentre la base giuridica dell'art. 16 TFUE, ha natura residuale e limitata agli aspetti sopra indicati. Da ciò pare possibile affermare che l'AI Act persegue, nell'ambito del diritto dell'Unione, un obiettivo eminentemente mercantilistico, in quanto diretto a promuovere il buon funzionamento del mercato interno.

Sul punto, come chiarito dalla Corte di giustizia, la base giuridica di cui all'art. 114 TFUE, risulta, in linea di principio, compatibile unicamente con l'adozione di misure volte a evitare genuinamente la frammentazione del mercato, il che di norma accade laddove venga raggiunto un livello di armonizzazione massima, tale da impedire agli Stati membri di prevedere ulteriori regole che possano ostacolare la circolazione di merci e servizi oggetto di armonizzazione[34].

---

[32] Sul punto, v. in generale Corte giust. 11 giugno 1991, C-300/89, *Commissione/Consiglio*, punti 10-17, ove si afferma che l'utilizzo di una pluralità di basi giuridiche è ammissibile soltanto qualora gli obiettivi e i contenuti dell'atto siano inscindibilmente connessi. Si veda altresì, *inter alia*: P. CRAIG, G. DE BÙRCA, *EU Law: Text, Cases and Materials*, Oxford, 2015, p. 616.

[33] Questa conclusione è espressamente accolta dalla Commissione europea: Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/1689 (regolamento sull'IA), Bruxelles, 29 luglio 2025, C (2025) 5052final, p. 4.

[34] Il *leading case*, in tal senso, è costituito dalla sentenza "Tobacco Advertising I": Corte giust. 5 ottobre 2000, C-376/98, *Germania/Parlamento e Consiglio*, punti 101-105. La giurisprudenza della corte in materia di armonizzazione è tuttavia assai complessa e non sempre coerente, come osservato in dottrina, tra gli altri, da S. WEATHERILL, *op. cit.*, pp. 14-15.

4. *AI Act e disciplina dell'uso dei sistemi di IA: tra armonizzazione selettiva e spazi di autonomia residua*

Chiarito il fondamento giuridico nei Trattati e il connesso livello di armonizzazione che il regolamento si propone in linea di principio di ottenere, parrebbe già possibile concludere che quest'ultimo non consente alcuno spazio residuo di manovra agli Stati membri per quanto riguarda l'imposizione di ulteriori regole nei confronti degli operatori di sistemi di IA.

Tuttavia, un più attento esame della disciplina sostanziale dettata dal regolamento rivela una realtà maggiormente complessa. L'AI Act, infatti, pone due ordini di regole completamente distinti per quanto riguarda, da un lato, *l'immissione sul mercato*[35] e *la messa in servizio*[36] e, dall'altro, *l'utilizzo* di sistemi di IA. Il modo in cui l'AI Act potrebbe limitare ulteriori regole sulla immissione nel mercato e sull'utilizzo differisce e, di conseguenza, questi aspetti vanno analizzati separatamente.

Partendo dal caso più semplice, pare possibile affermare che la disciplina relativa all'immissione nel mercato e alla messa in servizio di tutti i sistemi di IA (non solo quelli ad alto rischio), risulta essere completamente armonizzata dall'AI Act[37]. Ciò è infatti espressamente indicato all'art. 1, par. 1. In tale ipotesi, laddove gli Stati membri intendano introdurre ulteriori restrizioni alla commercializzazione di qualsiasi sistema di IA, ad esempio per finalità di tutela dell'ambiente, dovranno avvalersi delle limitate eccezioni previste dall'art. 114 TFUE, soggette a notifica e approvazione da parte della Commissione.

Per quanto riguarda, invece, la disciplina concernente l'utilizzo dei sistemi di IA, definire il livello di armonizzazione apprestato dal regolamento risulta essere un compito decisamente più complesso. Ciò anche per una ragione storica: gli strumenti legislativi adottati

---

[35] Con "immissione sul mercato" si intende «la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione» (art. 3, n. 9, AI Act).

[36] Con "messa in servizio" si intende «la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista» (art. 3, n. 11, AI Act).

[37] M. VEALE, F. Z. BORGESIUS, *op. cit.*, p. 109.

nell'ambito del NLF si limitano tipicamente a stabilire obblighi relativi alla fase di produzione e commercializzazione di beni e servizi, senza mai imporre obblighi agli utenti a valle dell'installazione o del primo utilizzo; di conseguenza, non vi sono chiare analogie in tal senso[38].

Come punto di partenza dell'analisi in merito all'armonizzazione operata nell'ambito dell'utilizzo dei sistemi di IA, sulla base delle considerazioni già svolte, pare possibile affermare che l'AI Act non rappresenti uno strumento generale di "armonizzazione minima", volto cioè a stabilire un livello regolatorio orizzontale di base. Come sopra osservato, peraltro, misure generali di "armonizzazione minima" non sono in linea di principio ammesse dalla Corte di giustizia dell'UE laddove la misura sia stata adottata sulla base dell'art. 114 TFUE, come in questo caso. Anche il dato testuale pare confermare questa preliminare conclusione: l'art. 1, lett. *a)* stabilisce che l'AI Act prevede «regole armonizzate per […] l'uso dei sistemi di IA nell'Unione», mentre il cons. n. 1 indica che: «Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni […] all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento».

La circostanza che l'AI Act non comporti in via generale un'armonizzazione minima sull'utilizzo dei sistemi di IA, tuttavia, non esclude di per sé qualsiasi spazio di manovra residuo per gli Stati membri con riguardo alla previsione di ulteriori regole in questo ambito. Sul punto, infatti, come già osservato in dottrina[39], l'AI Act potrebbe essere caratterizzato come uno strumento di armonizzazione "parziale" o "incompleta".

Qui, però, occorre ad avviso di chi scrive ulteriormente distinguere le regole legate alla trasparenza nell'utilizzo e quelle legate all'utilizzo "in sé e per sé". In particolare, un'armonizzazione massima in relazione all'uso dei sistemi di IA parrebbe aver avuto luogo in relazione ai sistemi a "rischio limitato", per i quali tuttavia l'art. 50 si limita a dettare regole volte a garantire la trasparenza verso l'utente finale, sia per i casi di commercializzazione che di utilizzo[40]. Sul punto, infatti, la lettera d)

[38] *Ibidem*.
[39] In questo senso: G. GALLONE, *op. cit.*; M. INGLESE, *op. cit*.
[40] Tali obblighi di trasparenza gravano, a seconda dei casi, sul fornitore o sul *deployer*. Nel primo caso, si tratta delle ipotesi previste ai paragrafi 1 e 2 dell'art. 50 AI Act,

dell'art. 1 dell'AI Act afferma che quest'ultimo stabilisce «regole di trasparenza armonizzate per *determinati* sistemi di IA»[41]. Una simile indicazione, tuttavia, non si rinviene per i casi di utilizzo di sistemi di IA "in sé e per sé", al di fuori cioè dei profili legati alla trasparenza.

Seguendo tale ipotesi, l'AI Act costituirebbe uno strumento legislativo che armonizza soltanto *alcune* regole legate all'utilizzo dei sistemi di IA – nello specifico, quelle legate alla "trasparenza nell'utilizzo", dettate all'art. 50 – e non altre. Al di fuori degli aspetti legati alla trasparenza dei sistemi a rischio limitato, dunque, l'AI Act lascerebbe agli Stati membri un'ampia libertà di legiferare su altre questioni legate all'utilizzo di tali sistemi.

5. *Mercato interno e diritti fondamentali: le restrizioni sull'utilizzo dei sistemi di IA alla luce del fondamento mercantilistico dell'AI Act*

Nel precedente paragrafo si è osservato che il diritto derivato (l'AI Act) non offre una clausola generale che delimiti con chiarezza l'area lasciata alla normazione nazionale. In via interpretativa, si è tuttavia inquadrato l'AI Act come un regolamento che opera un'armonizzazione selettiva: in particolare, la disciplina relativa all'immissione nel mercato e alla messa in servizio di tutti i sistemi di IA risulterebbe pienamente armonizzata, mentre la disciplina legata all'utilizzo verrebbe armonizzata unicamente nella misura in cui riguarda gli obblighi di trasparenza nell'utilizzo dei sistemi verso gli utenti finali – come previsto dall'art. 50 per i soli sistemi "a rischio limitato"[42] –, ma non anche per quanto attiene all'utilizzo *tout court* dei sistemi di IA, il quale rimane, almeno in linea di principio, nella disponibilità residuale degli Stati membri. Per quanto qui di particolare interesse, in tale

ossia i sistemi destinati a interagire con persone fisiche e quelli che generano contenuti audio, visivi o testuali sintetici. Nel secondo, rientrano le ipotesi previste ai paragrafi 3 e 4 del medesimo articolo, riguardanti i sistemi biometrici e i cosiddetti *deepfake*. Si noti altresì, come verrà discusso più diffusamente al par. 6 (*infra*) che l'art. 50, par. 6, AI Act, lascia la possibilità agli Stati membri di prevedere ulteriori norme di trasparenza legate all'utilizzo, limitatamente ai sistemi di IA "a rischio limitato".

[41] Enfasi aggiunta.

[42] Sebbene la specifica clausola contenuta all'art. 50, par. 6, AI Act, consenta agli Stati membri di prevedere obblighi più stringenti per i *deployer* di tali sistemi, come meglio indicato nel prosieguo di questo paragrafo.

disponibilità residuale rientra la disciplina dell'utilizzo dei sistemi di IA a rischio minimo.

In buona sostanza, la distinzione appena ricostruita consente di delineare i confini della competenza residua degli Stati membri nell'ambito della commercializzazione (pienamente armonizzata) e dell'utilizzo (selettivamente armonizzato) dei sistemi di IA. Resta tuttavia da chiarire in che misura le discipline nazionali che intervengano sull'utilizzo dei sistemi di IA possano ritenersi compatibili con il diritto dell'Unione, alla luce della giurisprudenza della Corte di giustizia sul principio di libera circolazione e sulle misure di effetto equivalente. È a tale verifica che si dedica il presente paragrafo, facendo altresì leva su esempi concreti di discipline nazionali già vigenti in questo ambito.

A tal fine, occorre considerare l'orientamento consolidato della Corte di giustizia, in base al quale le restrizioni d'uso imposte a livello nazionale possono configurare misure di effetto equivalente a restrizioni quantitative ai sensi degli artt. 34 e 36 TFUE, qualora incidano in modo diretto e sostanziale sull'accesso al mercato dei prodotti o dei servizi interessati, come stabilito dalla sentenza *"Italian Trailers"* che costituisce il *leading case* in materia[43]. Secondo tale giurisprudenza, in questi casi, la compatibilità delle norme nazionali con il diritto dell'Unione è subordinata alla presenza di giustificazioni oggettive o di esigenze imperative di interesse pubblico (tra cui la tutela della salute, della sicurezza pubblica o dei diritti fondamentali), le quali devono essere invocate e dimostrate dallo Stato membro. Questo approccio amplia notevolmente il raggio d'azione dell'art. 34 TFUE, includendovi sia le restrizioni alla vendita sia quelle sull'utilizzo di prodotti e servizi nel territorio nazionale.

Secondo questo approccio, eventuali restrizioni nazionali relative all'uso di sistemi di IA devono non solo basarsi sulle giustificazioni sopra indicate, ma devono altresì superare un test di proporzionalità particolarmente stringente: lo Stato membro è tenuto a dimostrare che la misura sia idonea, necessaria e proporzionata rispetto all'obiettivo perseguito e che dunque non esistano alternative meno impattanti per il mercato interno dell'Unione.

[43] Corte giust. 10 febbraio 2009, C-110/05, *Commissione/Italia*.

Sul punto va ulteriormente tenuto conto, come già osservato nel paragrafo 3 del presente contributo, che la base giuridica dell'AI Act nel diritto dell'Unione si rinviene primariamente dal ravvicinamento delle legislazioni degli Stati membri al fine di evitare frammentazioni che risulterebbero in un *vulnus* al mercato interno; in altri termini, l'AI Act ha essenzialmente uno scopo "mercantilistico", al netto delle poche disposizioni che trovano la base giuridica nell'art. 16 TFUE[44].

Tale aspetto non è privo di conseguenze per il tema che ci occupa. Come noto, la Corte di giustizia interpreta infatti gli atti di diritto derivato in conformità al relativo fondamento giuridico nei trattati[45]. È dunque lecito attendersi che la Corte di giustizia privilegerà un'interpretazione del regolamento in senso mercantilistico, di armonizzazione, piuttosto che come strumento volto a proteggere i diritti fondamentali[46], laddove uno Stato membro adotti regole aggiuntive sull'utilizzo dei sistemi di IA a livello nazionale.

Un utile parallelo, ad avviso di chi scrive, può essere tracciato con l'evoluzione della giurisprudenza in una materia contigua a quella che

---

[44] Si veda quanto osservato al par. 3 di questo contributo, *supra*. Si tratta, essenzialmente delle disposizioni del regolamento che impongono regole relative al trattamento dei dati personali, ossia con riguardo ai sistemi di IA per l'identificazione biometrica, quelli di polizia predittiva e quelli di categorizzazione biometrica, come espressamente chiarito dal cons. 3 dell'AI Act.

[45] *Ex multis*: Corte giust. 10 dicembre 2002, C-491/01, *British American Tobacco*, dove la Corte ribadisce che l'art. 114 TFUE, consente misure volte a prevenire ostacoli agli scambi e eliminare distorsioni della concorrenza, e interpreta la direttiva oggetto del rinvio pregiudiziale (direttiva 2001/37/CE del Parlamento europeo e del Consiglio, del 5 giugno 2001, sul ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla lavorazione, alla presentazione e alla vendita dei prodotti del tabacco) proprio alla luce di tali obiettivi economici; Corte giust. 4 maggio 2016, C-547/14, *Philip Morris*, dove la Corte respinge l'idea che la direttiva tabacco (direttiva 2014/40/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, sul ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla lavorazione, alla presentazione e alla vendita dei prodotti del tabacco e dei prodotti correlati e che abroga la direttiva 2001/37/CE) abbia un fine "autonomo" di tutela della salute, chiarendo che l'obiettivo resta il miglioramento del funzionamento del mercato interno pur tenendo conto di un elevato livello di protezione della salute Si veda anche, per il diverso atteggiamento della Corte di giustizia sull'interpretazione della normativa dell'Unione sulla protezione dei dati personali, prima e dopo l'entrata in vigore dell'art. 16, TFUE, quanto indicato *infra* in questo paragrafo, alle note 60 e 61.

[46] S. DE VRIES, *Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation*, in *EP*, vol. 8, n. 2, 2023, pp. 583-610, spec. p. 597.

ci occupa, ossia la protezione dei dati di carattere personale: nella fase iniziale, sotto la vigenza della direttiva 95/46/CE[47], adottata sulla base dell'allora art. 100a TCE (oggi art. 114, TFUE), la Corte di giustizia ha spesso privilegiato una lettura funzionale al mercato interno, minimizzando il rilievo autonomo del diritto fondamentale alla protezione dei dati e valorizzando la portata dell'armonizzazione stabilita dal diritto derivato[48]. A valle dell'introduzione dell'art. 16 TFUE, da parte del Trattato di Lisbona come base giuridica di riferimento per gli strumenti dell'Unione in materia di protezione dei dati, a tale prima fase mercantilistica ha fatto poi seguito una tendenza giurisprudenziale, che permane tutt'oggi, fortemente diretta a rafforzare il diritto alla protezione dei dati personali a scapito di diritti e interessi contrastanti[49], come appare particolarmente evidente in celebri sentenze quali *Google Spain*[50], in cui la Corte ha sancito in linea di principio la prevalenza del diritto alla protezione dei dati di carattere personale sul

[47] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[48] La distinzione tra le tendenze giurisprudenziali pre-Lisbona (art. 114 TFUE, come base legale) e post-Lisbona (art. 16 TFUE, come base legale) sono ben ricostruite da: O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford, 2015, pp. 51-75. Come esempio della tendenza "mercantilistica" pre-Lisbona, è possibile citare le sentenze *Satamedia* (Corte giust. 16 dicembre 2008, C-73/07) e *ProMusicae* (Corte giust. 29 gennaio 2008, C-275/06), in cui la Corte – pur riconoscendo la rilevanza della direttiva 95/46 per la protezione dei diritti fondamentali alla protezione dei dati personali e alla tutela della vita privata – ha privilegiato la tutela della libera circolazione dei dati e la funzionalità del mercato interno rispetto a una piena protezione dei diritti, lasciando ampio margine di discrezionalità agli Stati membri nel bilanciamento degli interessi coinvolti. In particolare, in *Satamedia* la Corte ha enfatizzato la libertà d'espressione come bilanciamento della protezione dei dati, adottando una lettura estensiva del termine "giornalismo" quale limite alle disposizioni della direttiva 95/46; in *Promusicae* la Corte ha bilanciato il diritto di proprietà con la protezione dei dati, lasciando al giudice nazionale ampia discrezionalità nel sacrificare la seconda in favore della prima. In commento alle due sentenze, l'autrice osserva che il fondamento giuridico della direttiva 95/46 nell'art. 114, TFUE: «[…] is one explanation for why the Court failed to actively assert the Directive's fundamental rights underpinning in its early case law, such as Satamedia and Promusicae».

[49] La seconda fase, in cui la Corte valorizza la finalità di protezione dei diritti fondamentali da parte della normativa dell'Unione sulla protezione dei dati a seguito dell'entrata in vigore dell'art. 16, TFUE, è ben riassunta da: O. LYNSKEY, *op. cit.*, pp. 62-75.

[50] Corte giust. 13 maggio 2014, C-131/12.

diritto alla libertà di espressione e di informazione, in netto contrasto con quanto affermato nella sentenza *Satamedia*[51], che pre-data l'introduzione dell'art. 16 TFUE.

Come osservato, tuttavia, nel caso dell'AI Act la base giuridica principale resta quella dell'art. 114 TFUE. Ne discende che la logica sottesa al regolamento è prevalentemente mercantilistica: l'obiettivo primario è assicurare l'integrità del mercato interno, prevenendo la frammentazione normativa, più che costruire un quadro organico di tutela dei diritti fondamentali nell'ambito della commercializzazione e utilizzo di sistemi di IA.

6. *Le discipline nazionali sull'utilizzo dei sistemi di IA: tra spazi di autonomia residua e profili di tensione con il diritto dell'Unione*

Tale impostazione, come sopra osservato, è idonea a orientare anche l'interpretazione della Corte di giustizia, che tende a privilegiare letture coerenti con la funzione di armonizzazione del mercato interno propria dell'art. 114 TFUE[52], piuttosto che accentuare la dimensione di garanzia dei diritti fondamentali, che pure rientra tra gli obiettivi dichiarati dell'AI Act. In questo contesto, le discipline nazionali che introducono obblighi aggiuntivi rispetto a quelli stabiliti dall'AI Act – anche quando motivate da finalità di tutela dei diritti fondamentali – rischiano di essere lette come restrizioni non giustificate alla libera circolazione di prodotti e servizi basati sull'IA.

È proprio in questa prospettiva che possono già osservarsi, i primi potenziali attriti tra diritto nazionale e diritto dell'Unione, come dimostrano le recenti iniziative legislative adottate in alcuni Stati membri.

L'Italia, con la legge 23 settembre 2025, n. 132, recante "Disposizioni e delega al Governo in materia di intelligenza artificiale", in vigore dal 10 ottobre 2025, prevede all'art. 13 alcune disposizioni relative all'impiego dei sistemi di IA da parte degli esercenti professioni intellettuali. Il paragrafo 1, in particolare, contiene in capo al

[51] *Satamedia*, sopra citata.

[52] Come avvenuto durante la fase "pre-Lisbona" del diritto derivato in materia di protezione dei dati personali, vale a dire prima dell'introduzione dell'art. 16, TFUE. Si veda più diffusamente quanto indicato alle note 60 e 61, *supra*.

professionista un divieto di utilizzo di sistemi di IA in via esclusiva per rendere la propria prestazione, mentre il paragrafo 2 contiene un obbligo di informazione sull'utilizzo di sistemi di IA in favore dei propri clienti, laddove il professionista intenda utilizzarli a supporto dello svolgimento del proprio incarico professionale.

Questa iniziativa del legislatore italiano può aiutare a comprendere l'estensione della competenza residua in capo agli Stati membri, come sopra delineata. Seguendo la linea interpretativa fin qui tracciata, che vede l'AI Act come un regolamento di armonizzazione massima per le regole sulla commercializzazione dei sistemi di IA, e di armonizzazione selettiva per le regole sull'uso dei medesimi sistemi, la disposizione di cui all'art. 13, par. 1, dovrebbe essere considerata conforme con l'AI Act, in quanto si tratta sì di una restrizione sull'utilizzo di sistemi di IA, ma che non pone alcun obbligo di trasparenza in capo al professionista (*rectius* al *deployer*, utilizzando il lessico del regolamento). Tale disposizione dovrebbe, tuttavia, pur sempre passare il test di compatibilità con le norme del Trattato in materia di libera circolazione, come interpretate dalla Corte di giustizia da *Italian Trailers* in poi[53].

Quanto alla norma di cui all'art. 13, par. 2, a prima vista la stessa parrebbe invece porsi in contrasto con una delle aree di armonizzazione massima dell'AI Act, atteso che una disciplina sulla trasparenza nell'utilizzo dei sistemi di IA risulta già dettata all'art. 50, AI Act.

Sul punto, occorre tuttavia premettere una riflessione più ampia, tenendo conto della clausola di salvezza contenuta al par. 6 del medesimo art. 50. Questa norma dispone che gli obblighi di trasparenza previsti ai primi 4 paragrafi di tale articolo «lasciano impregiudicati […] gli altri obblighi di trasparenza stabiliti dal diritto dell'Unione o nazionale per i deployer dei sistemi di IA». A prima vista, la clausola in parola parrebbe consentire in via generale la previsione di norme nazionali volte a stabilire regole di trasparenza ulteriori per l'utilizzo dei sistemi di IA (ossia, per i *deployer*), ma tale conclusione merita un'analisi ulteriore. Anzitutto, da un punto di vista letterale, la clausola si riferisce unicamente ai sistemi di IA contemplati dai paragrafi 1-4 del medesimo art. 50, ossia ai "sistemi a rischio limitato". Ne consegue che la norma non costituisce una clausola di salvezza generale, idonea a

[53] Come discusso in apertura del presente paragrafo.

legittimare interventi nazionali ulteriori in materia di trasparenza nell'utilizzo di qualsiasi sistema di IA; piuttosto, tale disposizione va intesa come una clausola di armonizzazione minima, ma dalla portata assai limitata sia dal punto di vista oggettivo, sia da quello soggettivo. Cominciando dal primo aspetto, la clausola si applica alle sole ipotesi elencate nei paragrafi 1-4 (ossia, le ipotesi di sistemi di IA a "rischio limitato"); inoltre, si applica soltanto agli obblighi applicabili ai *deployer*. In buona sostanza, la disposizione in esame consente agli Stati membri di andare oltre le salvaguardie apprestate dal legislatore dell'Unione per i *deployer* dei soli sistemi a rischio limitato ma non anche di introdurre obblighi di trasparenza per sistemi di IA che non rientrano in tale categoria, ovvero che vi rientrano ma che sono rivolti al fornitore del sistema[54]. Tale interpretazione restrittiva dell'art. 50, par. 6, oltre che coerente con il dato letterale, appare in linea con la già esaminata finalità principalmente mercantilistica dell'AI Act, dovuta alla base giuridica dell'art. 114, TFUE.

A parere di chi scrive, ne consegue che una disciplina nazionale volta a porre obblighi in capo ai *deployer* (nella specie, *deployer* che sono altresì esercenti professioni intellettuali) di tutti i sistemi di IA a prescindere dalla categoria di rischio, come quella introdotta dalla legge italiana n. 132/2025, non può basarsi sulla clausola di salvezza disegnata dall'art. 50, par. 6. Di conseguenza, anche in questo caso la disposizione di legge nazionale dovrebbe misurarsi con il test di compatibilità con le norme del Trattato in materia di libera circolazione, in applicazione della giurisprudenza inaugurata da *Italian Trailers*. In tal senso, peraltro, pare difficile sostenere che ricorrano esigenze

[54] In concreto, quindi, la clausola di armonizzazione minima contenuta al par. 6 consente di prevedere ulteriori salvaguardie a livello nazionale, nella forma di ulteriori obblighi in capo ai *deployer* di sistemi di riconoscimento delle emozioni e di categorizzazione biometrica (art. 50, par. 3) e per i *deployer* di *deep fake* (art. 50, par. 4), ma non anche per i fornitori di sistemi che interagiscono direttamente con persone fisiche (art. 50, par. 1) né per i fornitori di sistemi che generano contenuti sintetici (art. 50, par. 2). Inoltre, come già osservato, è bene qui ricordare che la categoria del rischio limitato e i relativi obblighi sono cumulabili con quelli della categoria dell'alto rischio, laddove un dato sistema di IA integri allo stesso tempo le caratteristiche dell'art. 6 (alto rischio) e dell'art. 50 (rischio limitato): un caso emblematico è quello dei sistemi di riconoscimento delle emozioni, che rientrano sia nella categoria dell'alto rischio, sia in quella del rischio limitato.

imperative di tutela dei diritti fondamentali richieste dagli artt. 34 e 36 TFUE.

Un ulteriore esempio, questa volta in relazione a normative che predatano l'AI Act, è costituito dalla normativa francese in merito alla trasparenza algoritmica nel settore pubblico[55]. Anche tale norma rischia di porsi in contrasto con il diritto dell'Unione, nella misura in cui stabilisce obblighi di trasparenza legati all'utilizzo dei sistemi di IA ulteriori rispetto a quelli imposti dal regolamento e che fuoriescono dal perimetro assai angusto della clausola di salvezza dell'art. 50, par. 6, AI Act.

Questi esempi dimostrano come il margine di intervento degli Stati membri resti oggi particolarmente incerto, oscillando tra la necessità di preservare l'effetto utile dell'armonizzazione perseguita dall'AI Act e l'esigenza, costituzionalmente rilevante, di assicurare un adeguato livello di tutela dei diritti fondamentali nell'ambito dell'utilizzo di sistemi di IA a livello nazionale[56].

7. *Vuoti regolatori e conflitti normativi: quale futuro per la regolamentazione dell'intelligenza artificiale nell'Unione?*

Come osservato, l'AI Act prevede uno scollamento significativo ambito di applicazione materiale – che si estende a tutta la vastissima categoria dei "sistemi di IA" – e l'ambito effettivamente normato, che risulta limitato, nei fatti, a un piccolo sottoinsieme dell'ambito di applicazione. Tale disallineamento, oltre che inusuale per il diritto dell'Unione, risulta problematico per l'esatta individuazione del "campo occupato" dal legislatore dell'Unione in una materia di competenza concorrente.

---

[55] *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*, disponibile presso: www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746/. Si veda, per una breve analisi: L. EDWARDS, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, in *IEEE Security & Privacy*, vol. 16, n. 3, 2018, pp. 46-54.

[56] In tal senso anche G. GALLONE, *op. cit.*, il quale avverte la questione come particolarmente problematica soprattutto nel settore dell'utilizzo dell'IA nella pubblica amministrazione. L'autore arriva a ipotizzare la possibile attivazione dei contro-limiti in questo settore.

A valle dell'analisi della base giuridica e del dato testuale, l'AI Act va inteso – a parere di chi scrive – come strumento di armonizzazione selettiva, secondo il seguente schema:

(i) Piena armonizzazione per l'immissione sul mercato e la messa in servizio di tutti i sistemi di IA (art. 1, par. 1, AI Act), a prescindere dal livello di rischio, con effetto preclusivo rispetto a ulteriori requisiti nazionali in queste aree, salva naturalmente la possibilità di avvalersi delle eccezioni procedurali dell'art. 114, par. 4 e seguenti, TFUE;

(ii) Armonizzazione della trasparenza nell'uso dei sistemi di IA piena, ancorché perimetrata ai soli obblighi di trasparenza per i sistemi "a rischio limitato" (art. 1, lett. d) e art. 50, AI Act), fatta salva la possibilità per gli Stati membri di prevedere ulteriori obblighi per soli i *deployer* di sistemi di IA a rischio limitato (clausola di salvezza ai sensi dell'art. 50, par. 6, AI Act);

(iii) Competenza residua degli Stati membri sull'uso "in sé e per sé" (al di fuori della trasparenza), ma solo se le misure nazionali superano il test di proporzionalità di cui agli artt. 34 e 36 TFUE ai sensi della giurisprudenza sulle restrizioni d'uso (*Italian Trailers*).

Ne discende che l'AI Act, pur non esaurendo la disciplina dell'uso in tutti i suoi profili, occupa totalmente il campo quanto a commercializzazione per tutti i sistemi e per la trasparenza nell'uso per i sistemi a rischio limitato; gli spazi nazionali per intervenire sull'utilizzo dei sistemi di IA restano peraltro stretti e destinati a un controllo rigoroso di compatibilità da parte della Corte di giustizia.

Ne consegue che lo spazio di manovra residuo per il legislatore dello Stato membro che intenda sopperire alla mancanza di qualsivoglia disciplina per i sistemi di IA a rischio minimo è piuttosto angusto, confinato a interventi marginali sull'utilizzo dei sistemi di IA e comunque soggetto a un penetrante scrutinio di compatibilità con il diritto dell'Unione. Tale margine ridotto, unito alla persistente assenza di qualsivoglia regolamentazione di sistemi di IA per l'amplissima categoria dei sistemi "a rischio minimo", che include fattispecie

tutt'altro che trascurabili in relazione al rischio per i diritti fondamentali, lascia presumere che nei prossimi anni potranno emergere tensioni tra iniziative nazionali e diritto dell'Unione, destinati a riaprire il dibattito sulla ripartizione delle competenze nella regolazione dell'intelligenza artificiale.

Con l'adozione dell'AI Act, l'Unione ha anzitutto inteso evitare che l'adozione di regole a livello nazionale ostacolassero il mercato unico digitale, impedendo il commercio di sistemi di intelligenza artificiale nell'Unione. Questo obiettivo appare senz'altro raggiunto per la categoria dei sistemi "a rischio inaccettabile", che risultano proibiti *tout court* quanto a commercializzazione e utilizzo, e quelli "ad alto rischio", per i quali il regolamento detta una disciplina comprensiva e rigorosa.

Tuttavia, l'AI Act crea una netta – e, come osservato al paragrafo 2, in molti casi discutibile – separazione tra i sistemi ad alto rischio, strettamente regolamentati, e quelli non ad alto rischio, che ricevono una regolamentazione poco più che simbolica (nel caso dei sistemi a rischio limitato) o del tutto assente (nel caso dei sistemi a rischio minimo). A ciò si aggiunge che gli Stati membri non hanno di fatto la possibilità di colmare tali lacune di tutela per i profili di immissione sul mercato e messa in servizio, mentre possono intervenire a certe condizioni nel disciplinarne ulteriormente l'utilizzo. Anche in tal caso, però, gli Stati membri si espongono al rischio di impugnazioni di fronte alla Corte di giustizia, vuoi perché l'AI Act potrebbe essere interpretato dalla Corte come strumento di armonizzazione massima anche in materia di utilizzo dei sistemi di IA, facendo leva sulla base giuridica dell'art. 114, TFUE, e sulla portata letterale dell'art. 1 del regolamento, vuoi nell'ambito della giurisprudenza relativa alle norme sulle limitazioni nell'utilizzo di prodotti e servizi[57].

Per altro verso, l'ampia cesura esistente tra ambiti pesantemente regolamentati (rischio inaccettabile e alto rischio), e ambiti scarsamente o affatto regolamentati (rischio limitato e – soprattutto – rischio minimo) risulta assai difficile da giustificare da un punto di vista di tutela dei diritti fondamentali, della sicurezza e dello stato di diritto e potrebbe, nel tempo, mettere pressione sui legislatori nazionali al fine

[57] Come discusso al par. 5, *supra*.

di agire per colmare tali lacune. Ciò, a maggior ragione, tenuto conto che, da un lato, la categoria del rischio minimo include alcuni sistemi il cui impiego risulta nei fatti molto impattante nei confronti dei diritti fondamentali[58] e, dall'altro, il settore dell'intelligenza artificiale risulta sempre più strategico per la crescita economica ed è oggi al centro di evidenti e crescenti tensioni geopolitiche tra Unione europea e Stati Uniti[59].

In definitiva, ad avviso di chi scrive, l'AI Act rappresenta un apprezzabile primo tentativo a livello globale di regolamentare in maniera orizzontale e sistematica il fenomeno dell'intelligenza artificiale. Tuttavia, il regolamento sembra lasciare spazi residui di intervento degli Stati membri che, per quanto limitati, con ogni probabilità vanno al di là delle intenzioni del legislatore e potrebbero generare conflitti interpretativi. A riprova di ciò, si è osservato come alcuni Stati membri, tra cui l'Italia, stiano già tentando di stabilire, ovvero abbiano già stabilito in passato, norme relative all'utilizzo dei sistemi di IA che vanno oltre a quanto previsto dall'AI Act. È verosimile che, nei prossimi mesi e anni, assisteremo a ulteriori tentativi di questo tipo, atteso che l'intelligenza artificiale e la sua regolamentazione avranno sempre più rilievo dal punto di vista economico e geopolitico tanto per l'Unione quanto per gli Stati membri.

[58] È il caso già visto, ad esempio, dei sistemi di *dynamic pricing*, *chatbot* e *recommender system*. V. par. 2, *supra*.
[59] C. CAULCUTT, *JD Vance warns Europe to go easy on tech regulation in major AI speech*, in *Politico*, February 2025.

ABSTRACT (ITA)

Il regolamento (UE) 2024/1689 ("AI Act") rappresenta il primo tentativo di disciplinare in maniera sistematica lo sviluppo, la commercializzazione e l'utilizzo dei sistemi di intelligenza artificiale attraverso un approccio orizzontale e basato sul rischio per i diritti e libertà fondamentali, la sicurezza e lo stato di diritto. Pur collocandosi nel solco del New Legislative Framework, l'AI Act si distingue per l'ampiezza del proprio ambito di applicazione materiale, che ricomprende tutti i "sistemi di IA" secondo l'ampia definizione adottata, e per la contemporanea limitazione degli obblighi sostanziali a un insieme ristretto di categorie: sistemi a rischio inaccettabile, ad alto rischio e, in misura marginale, a rischio limitato. Tale disallineamento produce una vasta area di sistemi – quelli a rischio c.d. "minimo" – formalmente inclusi nel campo di applicazione del regolamento, ma di fatto privi di disciplina anche quando pongono rischi concreti per i diritti fondamentali. Unita alla natura di armonizzazione massima derivante dalla base giuridica principale dell'AI Act, tale impostazione solleva interrogativi sull'esistenza o meno di spazio residuo di intervento degli Stati membri. L'articolo analizza le implicazioni di questa architettura normativa, evidenziando possibili conflitti tra diritto dell'Unione e diritto nazionale e riflettendo sulle sfide interpretative e applicative che l'AI Act pone rispetto all'equilibrio tra funzionamento del mercato interno, autonomia regolatoria nazionale e tutela effettiva dei diritti fondamentali.

ABSTRACT (ENG)

Regulation (EU) 2024/1689 ("AI Act") represents the first attempt to systematically regulate the development, commercialization, and use of artificial intelligence systems through a horizontal, risk-based approach aimed at safeguarding fundamental rights, security, and the rule of law. While situated within the framework of the New Legislative Framework, the AI Act stands out for the breadth of its material scope, which encompasses all "AI systems" according to the broad definition adopted, while substantive obligations are limited to a narrow set of

categories: unacceptable-risk systems, high-risk systems, and, to a marginal extent, limited-risk systems. This misalignment results in a wide range of systems – those considered to be of so-called "minimal" risk – being formally included within the Regulation's scope but substantially unregulated, even when they pose tangible risks to fundamental rights. Combined with the AI Act's maximum harmonization nature stemming from its primary legal basis, this approach raises questions about whether Member States retain any residual regulatory space. The article examines the implications of this regulatory architecture, highlighting potential conflicts between EU and national law and reflecting on the interpretative and enforcement challenges posed by the AI Act with regard to balancing the functioning of the internal market, national regulatory autonomy, and the effective protection of fundamental rights.