Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurìdico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

GIANLUCA CONTALDI*

I PROFILI GENERALI DELL'AI ACT

SOMMARIO: 1. Il percorso per l'adozione del regolamento europeo sull'intelligenza artificiale. – 2. La base giuridica del regolamento. – 3. La definizione di intelligenza artificiale e l'ambito di applicazione della normativa europea. – 4. La piramide del rischio. – 5. Il rischio inaccettabile. – 6. *I* sistemi ad alto rischio. – 7. La *governance* dell'IA. – 8. Un approccio timido del legislatore europeo?

1. *Il percorso per l'adozione del regolamento europeo sull'intelligenza artificiale*

Anche se la proposta di adozione di un regolamento elaborata dalla Commissione europea è stata presentata nel 2021[1], l'intenzione delle istituzioni europee di occuparsi di intelligenza artificiale è più risalente. Fin dalla comunicazione posta a base del c.d. mercato unico digitale, in effetti, la Commissione parla di «un'economia industriale e di servizio intelligente» e constata che «(l)a digitalizzazione offre possibilità senza precedenti anche a altri comparti dell'economia, come i trasporti (ad es., sistemi di trasporto intelligenti) o l'energia (ad es., reti intelligenti, contatori intelligenti)»[2].

Ovviamente, siamo nel 2015 e, con l'appellativo di "intelligente", l'esecutivo europeo intende riferirsi solo ai servizi e alle reti concepite per sfruttare al meglio le potenzialità di un dispositivo ovvero di organizzare in maniera ottimale il carico di una rete energetica. A conferma di questo assunto, è agevole osservare che, nel testo inglese, il termine impiegato è, – banalmente – «smart»; e non quello di *intelligent*, abitualmente impiegato per riferirsi ai processi articolati di elaborazioni dati e produzione di output.

Di intelligenza artificiale, in senso stretto, si inizia a parlare solo nella revisione della Comunicazione adottata due anni prima. Nel corso del 2017, l'esecutivo europeo approccia,

---

* Professore ordinario di Diritto dell'Unione europea, Università degli Studi di Macerata.

[1] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, Bruxelles, 21.4.2021 COM(2021) 206 final 2021/0106 (COD).

[2] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa, {SWD(2015) 100 final}, Bruxelles, 6.5.2015, COM(2015) 192 final, p. 15.

per la prima volta, il tema della responsabilità civile discendente dall'uso di sistemi di intelligenza artificiale, avvicinandola alla disciplina – all'epoca già esistente [3] – della responsabilità per danno da prodotto[4].

Successivamente, nel mese di aprile del 2018, la Commissione ha iniziato ad accompagnare le trattazioni concernenti la responsabilità dell'uso dei sistemi di intelligenza artificiale con la protezione dei diritti umani e con la necessità di porre l'uomo al centro dei progressi tecnologici nel settore digitale. Nella comunicazione «Intelligenza artificiale per l'Europa», la Commissione si propone, infatti, di rafforzare la leadership dell'Unione europea nell'intelligenza artificiale. A tal fine, la Commissione prevede di stanziare i fondi necessari per prepararsi ai cambiamenti socio-economici che la diffusione di tale tecnologia comporta[5]. E ancor più chiaramente, nel corso del mese di dicembre 2018, afferma che lo sfruttamento delle tecnologie dell'intelligenza artificiale dovrà essere accompagnato da principi etici da elaborare[6]. Pertanto, già tre anni prima di formulare la proposta di regolamento l'organo esecutivo ha ben presente che il futuro atto normativo dovrà attuare un bilanciamento tra i principi della responsabilità oggettiva, tipica dei danni da prodotti, ed i diritti fondamentali[7].

In seguito, il processo legislativo ha subito un'accelerazione. Questa è stata indubbiamente determinata da una serie di fattori concomitanti. Innanzitutto, dallo scoppio della pandemia da COVID, la quale ha provocato un massiccio ricorso alle nuove tecnologie in diversi settori, quale strumento sostitutivo degli incontri e dei contatti personali. Si è così assistito, forse anche oltre le necessità dettate dalla pandemia, a una forte spinta verso la digitalizzazione e a un massiccio ricorso al «lavoro agile». Va poi menzionata la grave crisi economica e l'invasione dell'Ucraina da parte della Russia, che ha implicato la necessità di

---

[3] La prima disciplina della responsabilità per danno da prodotto difettoso era contenuta nella direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, in GUUE L 210 del 7.8.1985. Questa è stata ora abrogata dalla direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio, in GUUE L, 2024/2853, 18.11.2024, che è stata emanata proprio per adattare la disciplina originaria alle evoluzioni del mondo digitale.

[4] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti, {SWD(2017) 155 final}, Bruxelles, 10.5.2017, COM(2017) 228 final, p. 13: «La Commissione esaminerà l'eventuale opportunità di adeguare l'attuale quadro giuridico per tenere conto dei nuovi sviluppi tecnologici (ad esempio nei settori della robotica, dell'intelligenza artificiale e della stampa 3D), in particolare dal punto di vista della responsabilità civile, alla luce dei risultati della valutazione in corso sulla direttiva relativa alla responsabilità per danno da prodotti difettosi e sulla direttiva "macchine"».

[5] Comunicazione della Commissione, L'intelligenza artificiale per l'Europa, Bruxelles, 25.4.2018, COM(2018) 237 final: «Per gestire la trasformazione dell'IA, i lavoratori il cui impiego sta cambiando o può scomparire a causa dell'automazione devono avere tutte le opportunità di acquisire le competenze e le conoscenze necessarie per padroneggiare la nuova tecnologia e ricevere sostegno durante la transizione nel mercato del lavoro. Questo atteggiamento proattivo e incentrato sull'investire nelle persone è il fondamento di un approccio all'IA inclusivo e antropocentrico, che richiederà un investimento notevole».

[6] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Piano coordinato sull'intelligenza artificiale, Bruxelles, 7.12.2018, COM(2018) 795 final, p. 7.

[7] V. M. BASSINI, *Oggetto, campo di applicazione e ambito territoriale*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, Milano, 2025, p. 113 ss., spec. 114 ss.; M. ALMADA, N. PETIT, *The EU AI Act: between the Rock of Product Safety and the Hard Place of Fundamental Rights*, in *Common Market Law Review*, 2025, p. 85 ss., secondo i quali la regolamentazione dell'AI Act combina norme sulla sicurezza dei prodotti e tutela dei diritti fondamentali.

riconvertire le fonti di approvvigionamento. Pure la crisi climatica e la correlata necessità di ridurre l'impiego delle fonti fossili hanno contribuito a rendere necessaria una normativa sull'utilizzo delle nuove tecnologie.

In questo contesto, il ricorso all'intelligenza artificiale è stato sempre più considerato quale un volano per lo sviluppo delle economie moderne. La stessa Commissione, nel Libro bianco sull'intelligenza artificiale, ha riconosciuto che: «I progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati sono pertanto fattori determinanti per l'attuale crescita dell'IA. L'Europa può combinare i suoi punti di forza industriali e tecnologici con un'infrastruttura digitale di elevata qualità e un quadro normativo basato sui suoi valori fondamentali per diventare un leader mondiale nell'innovazione nell'economia dei dati e nelle sue applicazioni (…). Su questa base l'Europa può sviluppare un ecosistema di IA che consenta alla sua società e alla sua economia nel loro complesso di godere dei benefici apportati dalla tecnologia»[8].

Tutti questi fattori hanno dunque fatto maturare la necessità e la volontà di creare un ambiente favorevole allo sviluppo dell'intelligenza artificiale nell'Unione europea.

L'AI ACT è, pertanto, scaturito da queste molteplici esigenze. In definitiva, per una normativa così articolata e complessa, il procedimento legislativo è stato anche rapido. Rispetto ad una proposta della Commissione presentata in data 21 aprile 2021, il testo definitivo è stato approvato nel giro di tre anni, dal momento che lo stesso è stato licenziato dal Parlamento europeo e dal Consiglio, rispettivamente, nei mesi di marzo e maggio 2024[9].

L'AI Act è senza dubbio uno strumento legislativo di fondamentale importanza nella costruzione del mercato unico digitale[10]. Come ha affermato Mathieu Michel, all'epoca sottosegretario di Stato belga per la Digitalizzazione: «L'adozione del regolamento sull'IA rappresenta una pietra miliare per l'Unione europea. Questo atto legislativo storico (…) affronta una sfida tecnologica globale che crea anche opportunità per le nostre società ed economie. Con il regolamento sull'IA l'Europa pone l'accento sull'importanza della fiducia, della trasparenza e della responsabilità nell'utilizzo delle nuove tecnologie, insieme alla garanzia che questa tecnologia in rapida evoluzione possa prosperare e stimolare l'innovazione europea»[11]. In effetti, in questa dichiarazione, non a torto riportata da vari

---

[8] Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, Bruxelles, 19.2.2020, COM(2020) 65 final, p. 2.

[9] Più dettagliatamente: il 21 aprile 2021 la Commissione europea ha presentato la propria proposta (Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale), cit.; il 14 giugno 2023, il Parlamento Europeo ha proposto gli emendamenti; il 2 febbraio 2024 si è passati attraverso l'approvazione del COREPER; il 13 marzo 2024 c'è stato il via libera da parte del Parlamento Europeo; il 21 maggio 2024, il Consiglio approva la versione finale del regolamento. Il 12 luglio il regolamento 2024/1689 è pubblicato nella Gazzetta Ufficiale dell'Unione europea: Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), in GUUE L, 2024/1689, 12.7.2024. La nuova disciplina si applicherà a far data dal 2 agosto 2026 (per riferimenti più precisi, in relazione alle diverse parti del regolamento v. la nota 63).

[10] Cfr. B. NASCIMBENE, *Il mercato unico digitale è una nuova frontiera dell'integrazione europea?*, in *rivista.eurojus*, 3/2025, p. 1 ss., 10, nel decennio 2020-2030 individua tre atti come fondamentali per la costruzione del mercato unico digitale (il *Digital Markets Act*, il *Digital Services Act* e, appunto, l'*AI Act*).

[11] La dichiarazione riportata nel testo è desunta dal testo del comunicato stampa del Consiglio dell'Unione europea, al momento dell'approvazione da parte dell'istituzione del testo finale del regolamento (v. il sito: https://www.consilium.europa.eu/it/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/).

commentatori, viene sintetizzata, in poche parole, la volontà del legislatore europeo sia di adottare uno standard normativo globale, sia di creare un'opportunità di sviluppo economico e, al contempo, di dare vita ad un ambiente digitale sicuro ed affidabile.

Nonostante la centralità riconosciuta dell'AI Act occorre, tuttavia, chiedersi se sia sufficiente un atto normativo per conquistare un ruolo di primo piano nello sviluppo dell'intelligenza artificiale. In questo momento, infatti, si assiste ad una sorta di corsa alle tecnologie dell'intelligenza artificiale e ad un affannoso tentativo dei legislatori, nazionali ed internazionali, di fornire una regolamentazione che tenga conto non solo delle esigenze economiche, ma anche dell'impatto di questa tecnologia sul godimento dei diritti fondamentali.

2. *La base giuridica del regolamento*

Il regolamento si fonda su una duplice base giuridica[12]. Questa è composta, rispettivamente, dall'articolo 114 TFUE, che come è noto riguarda «le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno»; e dall'articolo 16 TFUE, che garantisce il diritto di ogni persona alla protezione dei dati di carattere personale.

La doppia base giuridica è sintomatica delle molteplici finalità perseguite dalle istituzioni europee: da un lato, lo sviluppo del mercato interno, teso a favorire una transizione digitale e ad affermare una sorta di sovranità europea sui dati; e, dall'altro, il rispetto dei diritti fondamentali ed in particolare quello alla tutela dei dati personali.

Tale duplice obiettivo emerge fin dal primo considerando, il quale prevede espressamente che: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme […] in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione. il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento».

Il contemperamento tra i due obiettivi che abbiamo sopra indicato (sviluppo del mercato interno e tutela dei diritti fondamentali) dovrebbe essere garantito dalla ricerca di una "via europea all'intelligenza artificiale", mediante la creazione di un ecosistema di fiducia. I principi di base del regolamento – e la stessa tassonomia del rischio – mirano evidentemente

[12] Sulla base giuridica e sugli obiettivi generali del regolamento v. C. SCHEPISI, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in V. SALVATORE (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, 2023, p. 29 ss.; M. CARTA, *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, in *rivista.eurojus.it*, n. 3/2024, p. 188 ss., 192; G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Bologna, 2024, p. 25 ss., 54 ss.

a rafforzare la fiducia dei cittadini nell'uso, che può essere garantita solo da un'assoluta trasparenza dei sistemi e da un costante controllo umano sul funzionamento degli stessi[13].

Per raggiungere tali obiettivi, il regolamento si basa sui principi di proporzionalità, trasparenza e sicurezza. Per proporzionalità si intende un approccio rapportato al rischio dei singoli sistemi, in funzione agli usi per i quali sono concepiti, in modo da non creare restrizioni eccessive al commercio. La trasparenza indica invece che i sistemi di IA devono essere progettati e sviluppati in modo da garantire il percorso logico che ha determinato l'assunzione delle decisioni. Infine, la sicurezza è il principio per cui i sistemi di IA devono essere progettati e sviluppati in modo da ridurre i rischi per la sicurezza e la salute delle persone, per i diritti fondamentali e per gli interessi pubblici.

Pur condividendo tale molteplicità di scopi, viene tuttavia da chiedersi se la base giuridica impiegata (artt. 114 e 16 TFUE) non finisca per essere, in un certo senso, limitativa a fronte della pluralità degli obiettivi perseguiti. In effetti, pur rappresentando i dati personali la base per lo sviluppo dei sistemi di intelligenza artificiale, sembra tuttavia criticabile limitare a tale aspetto le esigenze di protezione dei diritti fondamentali. Altri e non meno importanti diritti potrebbero infatti risultare pregiudicati da uno sviluppo incontrollato dell'intelligenza artificiale, quali il diritto di espressione, il principio di democrazia, il divieto di discriminazioni (quali possono essere quelle discendenti dai *bias* dei dati utilizzati per alimentare il sistema di intelligenza artificiale), la protezione dei minori e quella dei consumatori[14].

Non c'è, d'altro canto, alcun dubbio che il legislatore europeo fosse pienamente consapevole di questi rischi. Lo stesso Consiglio, nelle conclusioni della Presidenza nel corso del 2020 dirette ad incoraggiare la Commissione a presentare una proposta di atto legislativo, manifesta chiaramente l'esigenza che i sistemi di intelligenza artificiale siano rispettosi dei diritti fondamentali. Si può infatti leggere in dette conclusioni che: «Sottolineiamo che la progettazione, lo sviluppo, la diffusione e l'utilizzo dell'IA devono rispettare appieno i diritti fondamentali e le norme giuridiche vigenti. È opportuno applicare lo stesso livello di protezione al mondo digitale e a quello fisico. Sottolineiamo che, ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta possono essere apportate solo laddove siano necessarie e rispondano effettivamente a una finalità di interesse generale riconosciuta dall'UE o all'esigenza di tutelare i diritti e le libertà altrui, nel rispetto del principio di proporzionalità, e devono essere previste dalla legge e rispettare il contenuto essenziale dei diritti e delle libertà fondamentali. La normativa pertinente che dà attuazione ai diritti fondamentali potrebbe essere messa in discussione a causa della complessità e dell'opacità di talune applicazioni di IA, i cui risultati richiederebbero esperienza e processi specializzati per essere compresi e controllati»[15].

E la medesima Commissione europea, nella proposta presentata nel mese di aprile 2021, precisava che: «(l')utilizzo dell'IA con le sue caratteristiche specifiche (ad esempio

---

[13] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168 final, Bruxelles, 8.4.2019, spec. par. 2.2.

[14] Cfr. F. DONATI, *Diritti fondamentali e algoritmi nella Proposta di Regolamento sull'intelligenza artificiale*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, p. 111 ss.; A. ODDENINO, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune nozioni critiche sulla recente proposta di regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, ivi, p. 165 ss.; C. GRIECO, *Intelligenza artificiale e tutela degli utenti nel diritto dell'Unione europea*, Napoli, 2023.

[15] Consiglio dell'Unione europea, Conclusioni della presidenza - La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale, Bruxelles, 21 ottobre 2020, 11481/20, punti 10-11, p. 7 s.

opacità, complessità, dipendenza dai dati, comportamento autonomo) può incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea. La presente proposta mira ad assicurare un livello elevato di protezione di tali diritti fondamentali e ad affrontare varie fonti di rischio attraverso un approccio basato sul rischio chiaramente definito. Definendo una serie di requisiti per un'IA affidabile e di obblighi proporzionati per tutti i partecipanti alla catena del valore, la presente proposta migliorerà e promuoverà la protezione dei diritti tutelati dalla Carta: il diritto alla dignità umana (articolo 1), al rispetto della vita privata e alla protezione dei dati di carattere personale (articoli 7 e 8), alla non discriminazione (articolo 21) e alla parità tra donne e uomini (articolo 23). Essa mira a prevenire un effetto dissuasivo sui diritti alla libertà di espressione (articolo 11) e alla libertà di riunione (articolo 12), nonché ad assicurare la tutela del diritto a un ricorso effettivo e a un giudice imparziale, della presunzione di innocenza e dei diritti della difesa (articoli 47 e 48), così come il principio generale di buona amministrazione»[16].

Vista l'attenzione ai diritti fondamentali, vale la pena domandarsi se non sarebbero stati opportuni ulteriori normativi, per fornire una base giuridica specifica proprio alla parte relativa alla tutela di questi[17].

Il punto è tuttavia che, pur reperendo altre disposizioni all'interno del Trattato istitutivo che fanno chiaramente riferimento ai valori fondanti dell'Unione e ai diritti fondamentali, queste non sono tuttavia attributive di competenza. Non è, infatti, attributivo di competenza l'art. 2 TUE, il quale si limita a stabilire quali siano i valori fondanti dell'Unione. Né può essere attributivo di competenza l'art. 6, TUE, il quale, pur inserendo nel contesto del diritto primario, sia la Carta dei diritti fondamentali e le disposizioni in questa contenute (art. 6, par. 1), sia i diritti fondamentali desumibili dalla Convenzione europea dei

[16] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale), cit., p. 13.

[17] Tra i diritti fondamentali che potrebbero venire lesi dall'impiego di sistemi di intelligenza artificiale, dovrebbe includersi anche la proprietà intellettuale, anche se questa non è affatto menzionata nel passo sopra riportato della proposta della Commissione europea. Il problema si pone soprattutto per l'IA generativa, la quale raccoglie in via autonoma immagini e testi dal web, per poi elaborarne di nuovi. Sotto questo aspetto, la tutela del diritto d'autore sovviene in una duplice prospettiva. Il primo aspetto concerne la tutela del diritto d'autore a fronte di testi ed immagini diffuse sul web, che potrebbero essere tutelati dalle norme sulla proprietà intellettuale. In secondo luogo, c'è il problema di capire in quale misura le opere create con sistemi di IA generativa possano, a propria volta, accedere alla tutela autoriale. Il regolamento, nella misura in cui disciplina i sistemi di intelligenza artificiale generativa (denominati modelli di IA per finalità generali), prende posizione sul primo aspetto; v., in particolare, il considerando 106: «A tal fine, i fornitori di modelli di IA per finalità generali dovrebbero mettere in atto una politica volta a rispettare il diritto dell'Unione in materia di diritto d'autore e diritti connessi, in particolare per individuare e rispettare la riserva dei diritti espresse dai titolari dei diritti a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790. Qualsiasi fornitore che immetta sul mercato dell'Unione un modello di IA per finalità generali dovrebbe rispettare tale obbligo, indipendentemente dalla giurisdizione in cui hanno luogo gli atti pertinenti in materia di diritto d'autore alla base dell'addestramento di tali modelli di IA per finalità generali». Al contrario, il regolamento non si occupa per nulla del secondo tema ovvero della tutela del diritto di autore per le opere generate da sistemi di IA. In dottrina, cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, cit., p. 121 ss.; C. GRIECO, *Intelligenza artificiale e diritto d'autore: riflessioni a partire dalla recente prassi interna ed europea*, in *Studi sull'integrazione europea*, 2024, p. 239 ss.; A. AMIDEI, *La "creatività computazionale"? Quale tutela autoriale per le opere dell'ingegno AI-generated?*, in U. RUFFOLO, A. AMIDEI, *Diritto dell'intelligenza artificiale*, Vol. II, *Proprietà industriale e intellettuale. Corp Techh. Giustizia predittiva. Transumanesimo. AI generativa. Metaverso*, Roma, 2024, p. 79 ss.; ID., *AI generativa, libertà di manifestazione del pensiero e diritto d'autore*, ivi, p. 139 ss.

diritti dell'uomo e dalle tradizioni costituzionali comuni (art. 6, par. 3), è tuttavia esplicito nel precisare che dette fonti non sono attributive di competenza[18].

Neppure possono essere ritenute disposizioni attributive di competenza l'art. 19 TUE, che si limita a descrivere il sistema giurisdizionale europeo, ma risulta, di per sé, privo di attribuzione di poteri normativi specifici alle istituzioni europee[19] e l'art. 8 TFUE, che pure sancisce il principio di non discriminazione, da tenere indubbiamente presente nella conformazione degli algoritmi, senza tuttavia apprestare alcun procedimento legislativo per l'adozione di atti a tutela dello stesso[20].

Quindi, il riferimento alle disposizioni sopra menzionate, che trattano rispettivamente dell'armonizzazione necessaria per il funzionamento del mercato interno e della tutela dei dati personali, è chiaramente limitativo rispetto all'obiettivo prefissato dal legislatore europeo; ma lo stesso risulta chiaramente non superabile, data l'assenza di altre previsioni attributive di competenza all'interno del Trattato istitutivo.

3. *La definizione di intelligenza artificiale e l'ambito di applicazione della normativa europea*

Il regolamento adotta una nozione di intelligenza artificiale che, per certi versi, è più descrittiva dei caratteri dei sistemi che vi fanno ricorso, che realmente definitoria della tecnologia stessa.

---

[18] Per la precisione, l'art. 6, par. 2, secondo comma, TUE, precisa che «Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati». Viceversa, la circostanza che l'art. 6, par. 3, del Trattato non sia una disposizione attributiva di competenza è stata esplicitata dalla Corte di giustizia nel noto parere 2/94, *Adesione della Comunità alla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, ECLI:EU:C:1996:140, punti 32-34: «Si deve anzitutto ricordare che la rilevanza del rispetto dei diritti dell'uomo è stata sottolineata in varie dichiarazioni degli Stati membri e delle istituzioni comunitarie (richiamate al punto III.5 della parte in fatto). Un riferimento al rispetto di tali diritti è contenuto anche nel preambolo dell'Atto unico europeo, nonché nel preambolo e negli artt. F, n. 2, J.1, n. 2, quinto trattino, e K.2, n. 1, del Trattato sull'Unione europea. L'art. F precisa, inoltre, che l'Unione rispetta i diritti fondamentali quali sono garantiti, in particolare, dalla Convenzione. L'art. 130 U del Trattato prevede, al n. 2, che la politica della Comunità nel settore della cooperazione allo sviluppo contribuisce all'obiettivo del rispetto dei diritti dell'uomo e delle libertà fondamentali. Si deve rilevare inoltre che, secondo costante giurisprudenza, i diritti fondamentali fanno parte integrante dei principi generali del diritto dei quali la Corte garantisce l'osservanza. A tal fine la Corte si ispira alle tradizioni costituzionali comuni agli Stati membri e alle indicazioni fornite dai trattati internazionali relativi alla tutela dei diritti dell'uomo a cui gli Stati membri hanno cooperato e aderito. In tale contesto la Corte ha precisato che la Convenzione riveste un significato particolare. Se il rispetto dei diritti dell'uomo costituisce, quindi, un requisito di legittimità degli atti comunitari, si deve tuttavia rilevare che l'adesione alla Convenzione determinerebbe una modificazione sostanziale dell'attuale regime comunitario di tutela dei diritti dell'uomo, in quanto comporterebbe l'inserimento della Comunità in un sistema istituzionale internazionale distinto, nonché l'integrazione del complesso delle disposizioni della Convenzione nell'ordinamento giuridico comunitario».

[19] Pur essendo indubbio il ruolo della Corte di giustizia nell'introduzione e nella tutela dei diritti fondamentali nell'ordinamento giuridico dell'Unione europea: cfr. F. CAPOTORTI, *Il diritto comunitario non scritto*, in *Dir. com. sc. int.*, 1983, p. 409 ss.; A. DAVÌ, *Comunità europee e sanzioni economiche internazionali*, Napoli, 1993, p. 332 ss.; C. CURTI GIALDINO, *Art. 19 TUE*, in C. CURTI GIALDINO (a cura di), *Codice dell'Unione europea operativo*, Roma, 2012, p. 226 ss., 236 s.

[20] Per questa riflessione sull'art. 8 TFUE cfr. A. ADINOLFI, *Processi decisionali automatizzati e diritto antidiscriminatorio dell'Unione europea*, in A. ADINOLFI, A. SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze*, Napoli, 2022, p. 31 ss., 51.

L'art. 3, n. 1, infatti definisce un sistema di intelligenza artificiale come «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».

In prima battuta la Commissione europea aveva ipotizzato una definizione flessibile di "sistema di IA" come di «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

Successivamente, però, tale nozione è stata rimeditata al fine di conformarsi alla definizione desumibile dalla Raccomandazione predisposta dall'OCSE, anch'essa, a propria volta, modificata nel corso del 2023[21]. Secondo questa raccomandazione, un sistema di intelligenza artificiale «is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment»[22].

Una definizione assolutamente identica è stata poi adottata, nel medesimo lasso temporale, dagli Stati membri del Consiglio d'Europa nella Convenzione quadro sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto[23].

Volendo identificare il punto fondamentale nelle definizioni adottate dal regolamento, dalla Raccomandazione dell'OCSE e, infine, dalla Convenzione del Consiglio d'Europa, potremmo affermare che è la capacità di imparare che contraddistingue un sistema di IA. Questo, in definitiva, ci riporta alla mente le parole di Alan Turing che già nel 1950, ipotizzava che in futuro prossimo sarebbero stati inventati dei calcolatori in grado di apprendere e di assumere decisioni conseguenti, quasi come se stessero realmente pensando e non semplicemente mettendo in ordine i dati desunti dall'osservazione della realtà[24].

In tal modo il legislatore europeo ha voluto ricomprendere in tale definizione anche la c.d. intelligenza artificiale generativa, ovvero quella che muovendo da dati immessi durante

---

[21] Sull'evoluzione della nozione di IA cfr. G. PROIETTI, *Definire l'indefinibile? i sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico*, in *Contratto e impresa*, 2024, p. 882 ss., 901 ss.

[22] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449. La raccomandazione è stata adottata il 22 maggio 2019. Tale versione è stata modificata in data 8 novembre 2023 e successivamente approvata il 3 maggio 2024.

[23] CM(2024)52-final - Committee on Artificial Intelligence (CAI) - Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 17/05/2024. Il testo del Rapporto esplicativo, al punto 23, riporta infatti che la definizione adottata dalla Convenzione è ripresa da quella della Raccomandazione dell'OCSE, come modificata nel corso del 2023 («The definition of an artificial intelligence system prescribed in this Article is drawn from the latest revised definition adopted by the OECD on 8 November 2023»). Per il rapporto v. il documento: CM(2024)52-addfinal - Committee on Artificial Intelligence (CAI) - Framework Convention on artificial intelligence, human rights, democracy and the rule of law - Explanatory Report. Tutti i documenti riportati in questa nota sono reperibili sul sito del Consiglio d'Europa (www.coe.int). Per un primo commento cfr. F. SEATZU, *Assessing the Council of Europe's AI Convention: Challenges and Prospects for Protecting Human Rights and Democracy in the Age of AI*, in *Studi sull'integrazione europea*, 2025, p. 9 ss.

[24] A.M. TURING, *Macchine calcolatrici e intelligenza*, trad. it. a cura di D. Mauri, Torino, 2025 (il testo originale è del 1950): «Io credo che la domanda "le macchine sono in grado di pensare?", sia troppo insensata perché valga la pena discuterne. E tuttavia, credo anche che alla fine di questo secolo l'uso delle parole e l'opinione diffusa delle persone colte avranno subito un cambiamento tale che si potrà parlare di macchine che pensano senza aspettarsi di essere contraddetti».

il periodo di addestramento è, a propria volta, capace di reperire le risorse sul web e di elaborare dei testi autonomi[25].

Nonostante la definizione di intelligenza artificiale sia estremamente comprensiva, il regolamento prevede talune esclusioni dal proprio ambito di applicazione, in funzione di specifici usi di tale tecnologia. Le principali di dette esclusioni sono le seguenti: *i*) i sistemi di IA sviluppati o utilizzati per scopi esclusivamente *militari o di difesa*; *ii*) i sistemi di IA utilizzati solo a scopo di *ricerca e innovazione*; *iii*) nel caso in cui l'intelligenza artificiale venga utilizzata nel corso di un'*attività personale* a carattere non professionale. Ognuna di queste, evidentemente, risponde ad una ratio specifica. Quella per scopi militari dipende dalla circostanza che il regolamento impone una serie di requisiti di trasparenza e di responsabilità in capo ai fornitori ovvero agli utilizzatori, che sono incompatibili con lo sviluppo delle tecnologie in ambito bellico. D'altro canto, le attività militari si svolgono essenzialmente all'interno di una cornice dettata dal diritto internazionale e, più in particolare, del diritto dei conflitti armati; con la conseguenza che un regolamento europeo mal si presta a circoscriverne l'impiego della tecnologia in esame in tale ambito[26]. L'eccezione per scopo di ricerca è dovuta al fatto che l'attività scientifica mira esclusivamente a porre in essere sistemi più evoluti: essa stessa ha bisogno di una certa libertà di azione che evidentemente non si concilia con prescrizioni così stringenti quali quelle contenute nel regolamento[27]. Infine, l'esclusione dei sistemi di IA per meri motivi personali si giustifica per il fatto che questi sistemi hanno un impiego circoscritto all'utilizzatore: non essendo destinati ad uscire dalla sfera di discrezionalità di costui, essi non possono comunque produrre effetti di larga scala, né provocare impatti rilevanti sul godimento dei diritti fondamentali da parte dei terzi.

Infine, per concludere l'introduzione del regolamento, è opportuno chiarire chi ne sono i principali destinatari ovvero i sono i soggetti tenuti ad osservare gli obblighi prescritti dal regolamento stesso[28]. Il regolamento si applica: *a*) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che siano stabiliti nell'unione o in un paese terzo; b) agli operatori di sistemi di IA che hanno il loro luogo di stabilimento o che sono ubicati nell'Unione; c) ai fornitori e agli operatori di sistemi di IA situati in un paese terzo, laddove l'*output* prodotto dal sistema sia utilizzato nell'Unione; d) agli importatori e ai distributori dei sistemi di IA.

Definendo in tal modo il proprio ambito di applicazione, il legislatore dell'Unione europeo rende manifesta l'aspirazione a porre in essere delle regole "globali"[29] ovvero a

---

[25] Per questi sistemi, la versione finale del regolamento ha previsto la regolamentazione dei modelli di IA per finalità generali, sui quali v., *infra*, nota 58.

[26] Considerando n. 24, reg. 2024/1689: «Per quanto riguarda gli scopi militari e di difesa, tale esclusione è giustificata sia dall'articolo 4, paragrafo 2, TUE sia dalle specificità della politica di difesa comune degli Stati membri e dell'Unione di cui al titolo V, capo 2, TUE che sono soggette al diritto internazionale pubblico, che costituisce pertanto il quadro giuridico più appropriato per la regolamentazione dei sistemi di IA nel contesto dell'uso letale della forza e di altri sistemi di IA nel contesto delle attività militari e di difesa».

[27] Considerando n. 25, reg. 2024/1689: «Il presente regolamento dovrebbe sostenere l'innovazione, rispettare la libertà della scienza e non dovrebbe pregiudicare le attività di ricerca e sviluppo. È pertanto necessario escludere dal suo ambito di applicazione i sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici».

[28] Sul tema v., più diffusamente, L. GATT, M.T. LO CONTE, M.E. MAZZARELLA, *L'ambito di applicazione, soggettivo e oggettivo, dell'AI Act*, in U. RUFFOLO (a cura di), *AI Act. La regolamentazione europea dell'intelligenza artificiale*, Roma, 2025, p. 49 ss.

[29] Obiettivo abitualmente denominato come "sovranità digitale esterna". V. M. CARTA, *Il Regolamento UE sull'Intelligenza Artificiale*, cit., p. 190; G. FINOCCHIARO, *I molteplici obiettivi perseguiti dal regolamento*, in O.

stabilire degli standard che hanno vocazione ad applicarsi anche a soggetti situati in Stati terzi, ma che comunque producono sistemi di intelligenza artificiale destinati ad essere immessi nel mercato interno. Si tratta, evidentemente, di uno scopo non sempre chiaramente esplicitato negli atti che hanno preceduto l'adozione del regolamento, ma che risulta evidentemente ben presente e che, appunto, consiste nell'aspirazione a configurare l'Unione europea come un leader normativo e tecnologico in materia, in grado di definire gli standard globali per l'impiego dell'intelligenza artificiale[30].

4. *La piramide del rischio*

Per contemperare il corretto funzionamento del mercato interno con le esigenze di sicurezza dei sistemi di intelligenza artificiale, il regolamento si fonda su una sorta di «tassonomia del rischio». L'AI Act adotta, infatti, un approccio cosiddetto "*risk-based*", nel senso che maggiore è il rischio che discende dall'immissione in commercio di un determinato sistema di intelligenza artificiale, più rigorose sono le previsioni che i soggetti coinvolti e, soprattutto i fornitori, devono osservare.

In questa scelta è, peraltro, ravvisabile uno dei limiti di operatività del regolamento. Il sistema finisce, infatti, per assumere una certa rigidità[31]. L'inserimento dell'uno e dell'altro livello rischio è infatti determinato da una scelta a monte effettuata dalla Commissione sulla base delle tipologie di sistemi esistenti e della reportistica degli incidenti in relazione a ciascun utilizzo. Data la rapidità dell'evoluzione tecnologica è inevitabile che sorgano nuovi sistemi capaci di svolgere funzioni ulteriori, che risulteranno difficilmente inquadrabili in una delle categorie regolamentate[32].

In base a questo approccio è possibile rintracciare quattro diversi livelli di rischio che vanno dal minore al maggiore. Ciascun livello di rischio prevede specifici permessi e/o restrizioni.

Questa "piramide del rischio" comprende al livello più basso un rischio "minimo" o assente, al quale corrisponde un permesso all'immissione in commercio senza restrizioni. In tale ambito, viene tuttavia raccomandata l'adozione di un Codice di Condotta a fornitori ed utilizzatori.

Il secondo livello di rischio è quello dei testi o filmati elaborati da sistemi di intelligenza artificiale (ad es., i *chatbot*), per il quale è previsto un permesso generale alla loro diffusione a condizione che siano rispettati gli obblighi di informazione e trasparenza. Per detti sistemi, infatti, l'obbligo principale consiste, infatti, nel garantire «che i sistemi di IA destinati a interagire direttamente con le persone fisiche s(ia)no progettati e sviluppati in modo tale che

---

POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, cit., p. 101 ss.

[30] Si tratta del noto effetto Bruxelles, come teorizzato da A. BRADFORD, *Effetto Bruxelles. Come l'Unione europea regola il mondo,* Milano, 2021; ID., *Digital Empires: The Global Battle to Regulate Technology*, USA, 2023.

[31] V. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, cit., p. 15.

[32] Per questo il regolamento, all'art. 97, prevede una delega alla Commissione per adottare un atto delegato ed emendare l'allegato III, concernente i c.d. sistemi ad alto rischio.

le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA»[33].

Al terzo livello corrisponde il c.d. *rischio alto* e l'autorizzazione all'immissione in commercio è concesso solo a condizione che il fornitore abbia rispettato i requisiti dell'AI Act e abbia adeguatemente svolto una valutazione di conformità *ex-ante*.

Infine il quarto e ultimo livello indica un rischio *inaccettabile*: qui siamo nelle ipotesi nelle quali, secondo la Commissione, ricorrono i maggiori rischi per la tutela delle persone ovvero per i diritti fondamentali. I sistemi di intelligenza artificiale che mirano ad introdurre dei sistemi classificati in questo ambito sono, in linea di principio, vietati. Per ragioni espositive conviene iniziare da questi ultimi.

5. *Il rischio inaccettabile*

I sistemi di intelligenza artificiale a rischio inaccettabile sono disciplinati dal solo art. 5. Questa previsione ha eminentemente la funzione di vietare l'immissione in commercio di sistemi di intelligenza artificiale riconducibili nelle categorie menzionate nella disposizione. Anche se, come vedremo tra breve, i divieti sono estremamente circostanziati e suscettibili di svariate deroghe.

Il primo divieto concerne i sistemi che determinano una manipolazione comportamentale cognitiva, eventualmente attraverso lo sfruttamento di specifiche vulnerabilità (quali età, disabilità o situazione socioeconomica) del soggetto[34]. In questo caso siamo in presenza di un divieto assoluto, non suscettibile di deroghe. Tuttavia, dalla formulazione delle previsioni normative inerenti, emerge chiaramente che il divieto colpisce non tanto la produzione, quanto piuttosto la commercializzazione ovvero l'uso del sistema diretto a distorcere il comportamento di un determinato soggetto («l'immissione sul mercato, la messa in servizio o l'uso»). Inoltre, per incorrere nel divieto occorre che tali tecniche facciano uso di tecniche subliminali («che utilizza tecniche subliminali») ovvero che sfruttino le debolezze specifiche del soggetto («che sfrutta le vulnerabilità di una persona fisica»); e che si prefiggano, quale scopo specifico, di distorcere il comportamento («aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone»). In quarto luogo occorre che la manipolazione abbia l'effetto di indurre una persona o un gruppo di persone a prendere una decisione che le provochi un danno

[33] Art. 50, reg. 2024/1689. In dottrina v. E. LONGO, F. PAOLUCCI, *The Article 50 of the AI Act and the Transparency obligations: The Model and Its Limitations*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, cit., p. 275 ss.

[34] Art. 5, reg. 2024/1689: «1. Sono vietate le pratiche di IA seguenti: a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo; b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo».

significativo («inducendole …a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare… un danno significativo»).

Sulla base della formulazione delle disposizioni in esame, è agevole affermare che le condizioni previste sono cumulative: ne discende che devono ricorrere tutte e quattro le condizioni per incorrere nel divieto[35]. In questo contesto, l'interprete non potrebbe fare ricorso al disposto dell'art. art. 5, par. 1, lett. a) e b), per vietare l'attività di società quali Neuralink, che elabora supporti per sopperire alle disabilità di specifici soggetti (quali, ad esempio, computer che creano parole dal movimento degli occhi) oppure di chatGPT, che pure può essere utilizzato per creare testi ed immagini molto simili a quelli concepiti dall'intelletto umano[36], perché mancano sia dell'elemento oggettivo, sia di quello finalistico: essi non sono, infatti, diretti a indurre un certo comportamento, attraverso tecniche subliminali, per arrecare un danno significativo.

Il secondo divieto concerne il c.d. *social scoring*, ovvero la valutazione del comportamento sociale di determinati soggetti o di talune caratteristiche (in genere, al fine di desumerne elementi per l'accesso a determinati servizi, quali possono essere i servizi socio-assistenziali)[37]. Tale disposizione rafforza, in definitiva, la previsione già contenuta nell'art. 22 GDPR[38]. Questo articolo, come è noto, stabilisce il diritto dell'interessato a non essere sottoposto a trattamento automatizzato, a meno che non vi abbia acconsentito ovvero il trattamento sia previsto da una norma nazionale o di diritto dell'Unione. Sia il divieto di *social scoring* previsto dal regolamento sull'intelligenza artificiale, sia il diritto a non essere sottoposto ad un trattamento automatizzato disciplinato dal GDPR richiedono che il trattamento sia produttivo di un danno per l'interessato. La Corte di giustizia, nella nota sentenza *Schufa* ha stabilito che è sufficiente la mera eventualità per l'interessato di ricevere un trattamento

---

[35] Comunicazione della Commissione europea, *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, Brussels, 29.7.2025, C(2025) 5052 final, p. 18, punto 61: «For the prohibition to apply, *all four conditions must be simultaneously fulfilled* and there must be a plausible causal link between the techniques deployed, the material distortion of the behaviour of the person, and the significant harm that has resulted or is reasonably likely to result from that behaviour» (corsivo aggiunto).

[36] V. F. DONATI, *Le pratiche di AI vietate*, in U. RUFFOLO (a cura di), *AI Act*, cit., p. 119 ss., 121; F.P. LEVANTINO, I NERONI REZENDE, *Rischio inaccettabile: usi proibiti*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, cit., p. 159 ss., 163.

[37] Art. 5, par. 1, lett. c), reg. 2024/1689: «l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità».

[38] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). In dottrina, v., anche per ulteriori citazioni; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, vol. I (*Dalla dir. 95/46 al nuovo regolamento europeo*) e vol. II (*Il regolamento europeo 2016/679*), Torino, 2016; G. RESTA, V. ZENO ZENCHOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ.*, 2018, p. 411 ss.; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa*, 2018, 3, p. 1098 ss.; C. CALIFANO, L. COLAPIETRO (a cura di), *Innovazione tecnologica e persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, Napoli, 2018; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; G. FINOCCHIARO, *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019.

deteriore a seguito del trattamento automatizzato[39]. Se trasponiamo i principi desumibili dall'interpretazione che la Corte di giustizia ha dato dell'art. 22 del regolamento sulla protezione dei dati personali al regolamento sull'intelligenza artificiale, ne discende che, a differenza della prima fattispecie prevista dall'art. 5 (trattamento subliminale per distorcere il comportamento), in questo caso il danno può anche essere meramente eventuale: ovvero discendere dalla circostanza che, per effetto degli elementi utilizzati dal sistema di intelligenza artificiale, ne possa ipoteticamente derivare la privazione di una possibilità per l'interessato (quale può essere, per l'appunto, il mancato accesso ad un contributo sociale o ad un alloggio a costi contenuti, ecc.).

La terza ipotesi concerne la c.d. polizia predittiva ovvero l'uso dei sistemi di intelligenza artificiale «al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità»[40]. Si tratta, in altri termini, del ricorso ai sistemi di intelligenza artificiale al fine di impedire o prevenire la commissione di reati ovvero calcolare una pena detentiva. Il divieto trae origine dal noto caso COMPAS (*Correctional offender management profiling for alternative sanctions*), nel quale una corte americana[41] determinò la pena detentiva facendo ricorso ad un sistema di intelligenza artificiale artatamente capace di valutare la propensione ad incorrere in recidiva sulla base di determinati parametri, quali la storia pregressa, l'ambiente sociale di provenienza, la condizione economica, il livello di istruzione. In altri termini: è evidente che una valutazione siffatta presenti un elevato rischio di discriminazioni fondate su preconcetti statistici.

Tale disposizione va coordinata con quella contenuta al punto 8 dell'Allegato III, del regolamento il quale ricomprende, tra i sistemi ad alto rischio, quelli che fanno uso dei sistemi di intelligenza artificiale nell'ambito di un processo «per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie». Sulla base del combinato disposto dell'art. 5, par. 1, lett. *c*, e dell'Allegato III, sembrerebbe possibile adombrare la seguente conclusione: mentre è possibile il ricorso ad un sistema automatizzato per ricercare fatti o elementi ermeneutici, lo stesso non sarebbe ammissibile per calcolare la pena o, addirittura, scrivere una sentenza[42]. In questi casi, infatti,

---

[39] Corte di giustizia, 7 dicembre 2023, causa C- 634/21, *OQ c. Land Hessen e SCHUFA Holding AG*, ECLI:EU:C:2023:957, spec. punti 48-50.

[40] Art. 5, par. 1, lett. d), reg. 2024/1689.

[41] Corte Suprema del Wisconsin, 13 July 2016, *State v. Loomis, Case no. 2015AP157-CR* (la decisione è consultabile al sito https://law.justia.com/). Il caso *Loomis* è talmente conosciuto da venire richiamato anche in una sentenza del Consiglio di Stato (Cons. Stato, sez. VI, 13 dicembre 2019, n. 8474, par. 15.2, seppure in relazione all'uso dei procedimenti automatizzati per l'immissione in ruolo dei docenti). In dottrina v. K. FREEMAN, *Algorithmic injustice: how the Wisconsin Supreme Court failed to protect due process rights in State v. Loomis*, in *North Carolina Journal of Law and Technology*, 2018, p. 75 ss.; F. LAGIOIA, G. SARTOR, *Il sistema COMPAS: algoritmi, previsioni, iniquità*, in U. RUFFOLO (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino, Giappichelli, 2021, p. 226 e ss.; G. GALLONE, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Padova, 2023, 117 s.; C. PAPPALARDO, *Le applicazioni e le pratiche proibite di IA*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il regolamento europeo sull'intelligenza artificiale. Commento al Reg. UE n. 1689/2024*, Sant'Arcangelo di Romagna, 2024, p. 441 ss., 460.

[42] In tal senso v. anche la raccomandazione approvata dal plenum del Consiglio superiore della magistratura, in data 8 ottobre 2025, 118/VV/2024: «Riaffermare la centralità dell'esperienza processuale. Il processo e la valutazione giudiziale sono un'esperienza umana insostituibile, fondata su presenza, oralità, immediatezza percettiva e contraddittorio in uno spazio condiviso. Il Consiglio si adopererà, pertanto, per impedire la "despazializzazione del giudizio", ossia la riduzione del processo a mera interazione digitale, riaffermando che

dovrebbe essere sempre necessario l'intervento umano, per non incorrere nel divieto assoluto di immissione in commercio e di impiego[43].

Il quarto divieto riguarda i sistemi di IA che creano immagini ovvero ampliano banche dati mediante tecniche di «*scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso» (art. 5, par. 1, lett. *e*). Le tecniche di *scraping* consistono nel raccogliere immagini da telecamere ovvero da siti internet e *social network*, al fine di modificarle ovvero di ampliare i *data base*. La *ratio* del divieto risiede nel fatto che queste tecniche possono facilmente violare la *privacy* degli individui e «accresce il senso di sorveglianza»[44] da parte della collettività.

Tale divieto va tuttavia distinto da quello concernente la «categorizzazione biometrica» in tempo reale, per dedurre dati sensibili e la «identificazione biometrica», che costituiscono le ipotesi previste dalle lettere *h*) e *g*) della medesima disposizione[45]. In questo caso si possono, quindi, determinare due situazioni parallele dal punto di vista delle tecniche impiegate, ma assai diverse quanto ad estensione del divieto. La differenza risiede nel fatto che, mentre nel caso di *scraping* le immagini di un individuo vengono utilizzate per inferirne determinati caratteri o l'appartenenza a specifici gruppi (quali, in via esemplificativa, partiti politici, credenze religiose, orientamenti sessuali), nel secondo caso le tecniche di categorizzazione biometrica sono utilizzate al mero fine di riconoscere una persona (che magari sta volutamente celando la propria identità) [46].

È poi necessario introdurre un'ulteriore distinzione tra le due ipotesi prese in considerazione dalle lettere *h*) e *g*). Mentre nel primo caso (la categorizzazione biometrica) il divieto è assoluto, perché si scontra soprattutto con il divieto di trattamento di dati personali

---

la decisione nasce da una relazione viva tra giudice, parti e prove, in un tempo e in uno spazio che ne garantiscano serietà, pubblicità e responsabilità».

43 Sul tema v. R.E. KOSTORIS, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *Cass. pen.*, 2024, p. 1642 ss.; U. RUFFOLO, *Sentenza robotica e giustizia predittiva*, in U. RUFFOLO, A. AMIDEI, *Diritto dell'intelligenza artificiale*, cit., p. 15 ss.; E. PIETROCARLO, *Predictive policing e giustizia predittiva nel Regolamento europeo sull'IA*, in U. RUFFOLO (a cura di), *AI Act*, cit., p. 231 ss.

44 Considerando n. 43, reg. 2024/1689.

45 V. art. 5, par. 1, rispettivamente lett. g) e h): «g) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di *categorizzazione biometrica* che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto; h) l'uso di sistemi di *identificazione biometrica* remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti: i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni» (corsivi aggiunti).

46 Per la distinzione tra categorizzazione e individuazione biometrica attraverso tecniche di riconoscimento facciale v. Art. 29, Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Brussels, 22 March 2012; S. DEL GATTO, *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation. il caso del riconoscimento facciale*, in *Riv. ital. dir. pubbl. com.*, 2023, p. 37 ss., 41 s.; N. MENÉNDEZ GONZÀLEZ, G. MOBILIO, *Between Prohibited Risks and High Risks: The Regulation of Facial Recognition Technology*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, cit., p. 199 ss.

che «rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose» di cui all'art. 9 GDPR, nel secondo caso («l'identificazione biometrica») il divieto è, al contrario, derogabile se ricorrono determinate condizioni[47]. In questa seconda ipotesi, infatti, il sistema di intelligenza artificiale interviene solo per agevolare l'individuazione di determinate persone: in questo caso, vista l'esigenza di sicurezza della collettività, il divieto è derogabile se serve per identificare persone che siano collegate (in quanto vittime o sospetti autori) con determinati reati, particolarmente gravi e potenzialmente lesivi dell'ordine pubblico.

Da ultimo, la disposizione in esame vieta il riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione (art. 5, par. 1, lett. *f*). Sono infatti noti gli impieghi di sistemi di intelligenza artificiale al fine di individuare le emozioni in questi luoghi. Il considerando n. 44, del regolamento 2024/1689 giustifica tale divieto sulla base delle differenze rilevabili tra le varie popolazioni. Si può infatti leggere in detto considerando che: «Sussistono serie preoccupazioni in merito alla base scientifica dei sistemi di IA diretti ad identificare o inferire emozioni, in particolare perchè l'espressione delle emozioni varia notevolmente in base alle culture e alle situazioni e persino in relazione a una stessa persona… Pertanto, i sistemi di IA che identificano o inferiscono emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici possono portare a risultati discriminatori e possono essere invasivi dei diritti e delle libertà delle persone interessate».

Quindi, la preoccupazione verso i sistemi di riconoscimento delle emozioni, concerne la circostanza che detti sistemi risultano gravemente pregiudizievoli per i diritti fondamentali[48]. Siffatti impieghi dei sistemi di intelligenza artificiale, peraltro diffusi in taluni paesi asiatici (ad esempio in Cina), in quanto si pongono in aperta violazione della privacy e della vita privata degli individui soggetti al controllo e, come tali, si pongono in aperto contrasto con gli articoli 7 e 8 della Carta dei diritti fondamentali.

Tale divieto, peraltro, consente un'eccezione, nella misura in cui il riconoscimento delle emozioni possa produrre effetti positivi per l'individuo, quali la diagnosi e l'individuazione del trattamento sanitario (specie nei casi di malattie mentali) ovvero di sicurezza[49].

6. *I sistemi ad alto rischio*

Il terzo livello della piramide è occupato dai sistemi di intelligenza artificiale ad alto rischio. Si tratta, peraltro, della fattispecie alla quale sono destinate la maggior parte delle disposizioni del regolamento europeo.

---

[47] L'attività di *web scraping* è stata una delle violazioni commesse dalla società statunitense Clearview AI, la quale scandaglia il web al fine di individuare di individuare elementi biometrici di identificazione, che successivamente trasforma in algoritmi, al fine di procedere all'identificazione dei soggetti, senza acquisire il previo consenso di questi. V. il caso deciso dal Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022, 9751362; in dottrina v. N. ZORZI GALGANO, *Il regolamento UE 2024/1689 del 13 giugno 2024 sul c.d. alto rischio inaccettabile: le pratiche inerenti sistemi di intelligenza artificiale vietate dal legislatore europeo*, in *Contratto e impresa*, 2025, p. 41 ss., 71 s.

[48] E. M. RENIERIS, *Beyond Data. Reclaiming Human Rights at the Dawn of the Metaverse*, MIT Press, 2023, 102, riporta che in Cina se ne fa uso anche per accertare se gli studenti in età scolare siano effettivamente felici.

[49] Non rientrano evidentemente nel divieto i sistemi di controllo che non servono per desumere le emozioni del soggetto. Le linee guida elaborate dalla Commissione, al riguardo, riporta quale esempio il caso di impiego di sistemi di IA che seguono gli occhi degli studenti durante un esame, per evitare casi di falso ovvero di plagio (*Commission Guidelines on prohibited artificial intelligence practices*, cit., p. 86 s.).

Ai sensi dell'art. 6 ricorre un'ipotesi di sistema di IA ad alto rischio in presenza di due situazioni eterogenee.

Innanzitutto, allorché il sistema di intelligenza artificiale costituisce uno dei prodotti (ovvero una componente di questi) oggetto della normativa armonizzata a livello dell'Unione e ricompresa nell'allegato I al regolamento. Detto allegato è estremamente ampio e include un lungo elenco di normative di armonizzazione. È impossibile, nell'economia di questo scritto, elencarle se non in maniera sintetica. Le principali riguardano: la sicurezza dei giocattoli; gli ascensori; le apparecchiature radio; gli impianti a fune; i dispositivi di protezione individuale; i dispositivi medici; la sicurezza dell'aviazione civile; i mezzi a due o tre ruote; l'equipaggiamento marittimo; l'interoperabilità del sistema ferroviario[50].

Nel caso in cui il sistema di IA, pur non rientrando nell'ambito della normativa armonizzata elencata nell'allegato I, è destinato a particolari fini, allora l'interprete deve verificare se l'ipotesi rientri comunque in una di quelle previste dall'allegato III. Detto allegato menziona diversi impieghi dei sistemi di intelligenza artificiale, che riguardano, rispettivamente: l'identificazione biometrica a posteriori; il riconoscimento delle emozioni; la formazione professionale; la valutazione e l'apprendimento; la selezione personale; l'accesso ai servizi essenziali; il controllo delle frontiere; l'uso, da parte dell'autorità giudiziaria per la ricerca dei fatti o del diritto ovvero quale strumento nella risoluzione alternativa delle controversie[51].

In definitiva, la Commissione europea ha optato per una soluzione definitoria rigida dei sistemi ad alto rischio. Essa si è, infatti, basata su meri dati statistici ovvero sul calcolo delle probabilità che si verifichino degli incidenti nell'uso di detti sistemi; e, sulla base di detto riscontro, ne ha poi previsto l'inclusione nella categoria in esame[52]. Rispetto a detta rigidità sono, tuttavia, ammessi due temperamenti. Il primo è che la Commissione può modificare l'Allegato III, attraverso atti delegati, che può esercitare «aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio»[53]. In secondo luogo, un sistema di IA, pur rientrando in uno degli usi di cui all'Allegato III, non è considerato ad alto rischio se lo stesso è utilizzato solo per svolgere «un compito procedurale limitato» ovvero a «migliorare un'attività umana precedentemente completata», senza sostituire o influenzare la valutazione umana[54].

Gli obblighi principali che incombono sui fornitori dei sistemi ad alto rischio sono disciplinati dagli articoli 9 a 15. Questi, sulla falsariga delle norme sulla sicurezza dei prodotti, comprendono sia obblighi di documentazione, tracciabilità e trasparenza; sia obblighi che attengono ai dati che devono essere utilizzati per addestrare il sistema; sia, infine, obblighi di

---

[50] Omettiamo di riportare in nota l'elenco (piuttosto esteso) dei singoli atti normativi compresi nell'Allegato I. Ciò che conta è siano disposizioni di armonizzazione recenti: quelle correntemente definite come appartenenti alla nuova cornice legislativa (NFL – New Legislative Framework). V. F. GALLI, G. CONTISSA, G. SARTOR, *I sistemi ad alto rischio*, in U. RUFFOLO (a cura di), *AI Act. La regolamentazione europea dell'intelligenza artificiale*, cit., p. 155 ss., 157; T. RODRÍGUEZ DE LAS HERAS BALLEL, *High-Risk AI Systems in the European AI Act*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, cit., p. 228 ss., 239.

[51] L'Allegato III, pertanto, non sta legittimando un uso dell'intelligenza artificiale quale sostitutivo delle parti, degli Avvocati ovvero dei Giudici, ma solo quale ausilio allo stesso. V. U. RUFFOLO, *I due volti della giustizia predittiva: decisoria e consultiva*, in U. RUFFOLO (a cura di), *AI Act*, cit., p. 193 ss.; M. BOLOGNESE, *La funzione giurisdizionale nel diritto europeo dell'intelligenza artificiale*, in *rivista.eurojus.it*, 3/2025, p. 207 ss.

[52] Le ipotesi previste in maniera generale ed astratta dal regolamento, discendono dalla combinazione della probabilità statistica che si verifichi un danno, con la gravità del danno stesso. V. T. RODRÍGUEZ DE LAS HERAS BALLEL, *High-Risk AI Systems in the European AI Act*, cit., p. 237.

[53] Art. 7, par. 1, reg. 2024/1689.

[54] Art. 6, par. 3, reg. 2024/1689.

introdurre sistemi resilienti. In definitiva si tratta di una serie di regole di prudenza, che assolvono eminentemente alla funzione di «ricondurre i rischi posti dai sistemi di IA ad alto rischio entro livelli ritenuti "accettabili"»[55].

Più specificamente gli oneri di documentazione concernono: l'obbligo dei fornitori di mettere in piedi e aggiornare costantemente un sistema di monitoraggio e gestione dei rischi (art. 9); l'obbligo di redigere una documentazione tecnica prima dell'immissione nel mercato (art. 11); l'obbligo di tracciare gli eventi che riguardano il sistema e di conservarne la relativa documentazione durante tutta la vita dello stesso (art. 12); l'obbligo, infine, di garantire che le informazioni siano chiare, trasparenti e facilmente accessibili per gli utilizzatori (art. 13). Detti obblighi sono completati da una disposizione, introdotta solo in occasione dell'ultima versione del regolamento, che concerne il diritto di ogni interessato, in ipotesi di decisione assunta da un utilizzatore attraverso un sistema di intelligenza artificiale ad alto rischio, di agire per ottenere una spiegazione dall'utilizzatore del sistema, circa il «ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata» (art. 86).

Per quanto riguarda l'addestramento del sistema, il fornitore deve garantire che questo avvenga solo con dati di alta qualità: questi sono i dati adeguati alla finalità specifica, rispetto ai quali è adeguatamente documentata la prestazione del consenso del titolare, in ossequio alle previsioni del citato regolamento sulla tutela dei dati personali (art. 10).

Il fornitore deve poi garantire che i sistemi ad alto rischio siano «progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita» (art. 15).

Ulteriori obblighi specifici per i fornitori riguardano quello di apporre il proprio segno distintivo; creare dei punti di contatto; mettere in piedi un sistema di gestione della qualità (art. 17); conservare la documentazione per dieci anni (art. 18); apporre la marcatura CE per indicare la conformità alla normativa unionale (48).

Un obbligo specifico per gli utilizzatori, riguarda, invece, quello di valutare l'impatto del sistema di IA ad alto rischio sui diritti fondamentali (art. 27).

Superiore e di portata tale da contraddistinguere l'approccio di tutto il regolamento ai sistemi ad alto rischio è poi l'obbligo che incombe sia ai fornitori (art. 14), sia agli utilizzatori (art. 26), di garantire la possibilità di una sorveglianza umana in ogni fase del processo di funzionamento. Tale obbligo, che fa il palio con la previsione del GDPR che prevede il diritto di ogni interessato a non essere sottoposto ad una decisione automatizzata (il citato art. 22, del reg. 2016/679), è, in qualche modo, il centro normativo intorno al quale ruotano tutte le previsioni del regolamento e che è atto a caratterizzare l'AI Act come un sistema effettivamente antropocentrico, in quanto diretto a porre al centro la persona umana e a considerare quest'ultima come ultimo ed effettivo responsabile di ogni violazione.

7. *La governance dell'IA*

Al fine di garantirne una corretta applicazione il legislatore europeo ha previsto l'istituzione di vari organi che svolgono compiti consultivi o di controllo che danno vita a

[55] R. PETRUSO, G. SMORTO, *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *Nuova giur. civ. comm.*, 2024, II, p. 989 ss., 996.

una nuova architettura di governance. Tale sistema è estremamente complesso ed articolato[56]. Il quadro generale che ne discende non risulta affatto di agevole lettura, dal momento che prevede frequenti interrelazioni e sovrapposizioni di competenze.

Per comodità espositiva, conviene distinguere il livello europeo da quello nazionale. Per quanto concerne l'ordinamento sovranazionale, il regolamento prevede l'istituzione di ben cinque autorità. Alcune di queste sono già esistenti, ma – per effetto del regolamento – divengono tributarie di nuove funzioni.

La prima delle autorità europee ha compiti esecutivi: si tratta, nella specie, dell'Ufficio per l'intelligenza artificiale, istituito all'interno della Commissione per far rispettare le regole stabilire dal regolamento all'interno dell'Unione europea[57]. Questo ufficio monitora l'efficace attuazione del regolamento e, a tal fine, può: chiedere documentazione sui modelli di IA, valutare la conformità del fornitore dei modelli di IA agli obblighi previsti dal regolamento; richiedere l'accesso al modello stesso[58].

Vi sono, poi, tre organi che assolvono eminentemente a funzioni consultive. Il primo di questi è il Consiglio per l'intelligenza artificiale (art. 65-66). Esso è composto da rappresentanti degli Stati membri ed è incaricato di fornire consulenza e assistenza alla Commissione e agli Stati membri ai fini di un'applicazione coerente ed efficace del regolamento sull'intelligenza artificiale. Il secondo è un Forum consultivo (art. 67) per i portatori di interessi volto a fornire competenze tecniche al Consiglio per l'intelligenza artificiale e alla stessa Commissione europea. Da ultimo, il regolamento prevede l'istituzione del Gruppo di esperti scientifici indipendenti (art. 68), selezionati dalla Commissione europea per le loro competenze specifiche, a sostegno delle attività di esecuzione, che assistono la

---

[56] Sul sistema di *governance* v. M. RABITTI, F. BASSAN, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti*, in *Federalismi*, n. 30/2024, p. 250 ss.; S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in *Quaderni AISDUE*, Fascicolo speciale n. 2/2024, *La nuova disciplina UE sull'intelligenza artificiale*, p. 1 ss.; C. CALENDA, *La governance a livello dell'Unione europea. Il Comitato europeo per l'intelligenza artificiale e gli altri organismi di supporto*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il regolamento europeo sull'intelligenza artificiale*, cit., p. 743 ss.; A. PAJNO, *La governance dell'Intelligenza artificiale fra Regolamento europeo e disciplina nazionale*, in U. RUFFOLO (a cura di), *AI Act. La regolamentazione europea dell'intelligenza artificiale*, Roma, 2025, p. 353 ss.; G. NATALE, *il ruolo delle autorità amministrative indipendenti in materia di AI*, ivi, p. 385 ss.

[57] Art. 64 del regolamento 2024/1689. L'ufficio è stato istituito con decisione della Commissione, prima che venisse licenziato il testo definitivo del regolamento con la decisione C/2024/1459, del 24 gennaio 2024, che istituisce l'ufficio europeo per l'Intelligenza Artificiale, in GUUE, C/2024/1459, del 14 febbraio 2024.

[58] L'Ufficio per l'IA si occupa anche della supervisione sui modelli di IA per finalità generali (v. considerando 151 e art. 64, del regolamento 2024/1689). Tali sono quei sistemi che siano allenati «su un largo insieme di dati (generalmente usando auto-supervisione ad ampia scala) e che può essere adattato (per esempio, accordato a un ampio insieme di compiti a valle)». In concreto, sarebbero i sistemi di IA c.d. generativa, che hanno una grande flessibilità e una capacità di fornire risposte, elaborare testi e immagini in maniera autonoma, sulla base dei dati elaborati durante il processo di addestramento. Il regolamento prevede obblighi specifici per i fornitori di modelli di IA per finalità generali e obblighi più stringenti per i sistemi di IA che prevedono rischi sistemici: v., rispettivamente, gli articoli 53 e 55. In dottrina v. G. SARTOR, G. DE GREGORIO, G. MUTO, *Large Language Models, Intelligenza artificiale generativa e Artificial Intelligence Act*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, cit., p. 248 ss., spec. 254 s.; U. RUFFOLO, *AI Act e AI generativa*, in U. RUFFOLO (a cura di), *AI Act. La regolamentazione europea dell'intelligenza artificiale*, cit., p. 303 ss.; M. UNFER, *L'IA generativa per finalità generali*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il regolamento europeo sull'intelligenza artificiale*, cit., p. 653 ss.; ID., *Segue: ChatGPT e sistemi similari*, ivi, p. 679 ss.; L. CHIMENTI, *L'IA che genera immagini e video*, ivi, p. 687 ss.

Commissione europea e le autorità di vigilanza nazionali soprattutto per quanto concerne i modelli di intelligenza artificiale per finalità generali[59].

Infine, l'ultimo organo europeo che ha assunto nuove funzioni per effetto del regolamento è il Garante europeo della protezione dei dati, che assolve al ruolo di autorità di vigilanza nei confronti delle istituzioni europee, ipotesi che ricorrerà soprattutto nel caso in cui queste svolgano il ruolo di utilizzatrici di sistemi di intelligenza artificiale (art. 70, par. 9).

Focalizzando ora l'attenzione sul piano dell'ordinamento interno, gli Stati membri devono designare due autorità nazionali competenti: una per la vigilanza del mercato e una per la ricezione delle notifiche (art. 70); l'altra, per garantire il rispetto dei diritti fondamentali (art. 77).

Sul piano dell'ordinamento italiano[60], le autorità competenti per garantire il rispetto dei diritti fondamentali sono l'AGCOM per quanto concerne l'informazione, i contenuti (testuali, fotografici, audiovisivi e radiofonici), nonché il diritto d'autore; il garante protezione dati personali per la protezione dei dati personali; i giudici nazionali.

Inoltre la legge 132/2025[61], in attuazione del regolamento, ha così ripartito i compiti alle varie strutture interne. Innanzitutto, il legislatore ha istituito una struttura presso la Presidenza del Consiglio dei ministri, che deve provvedere alla predisposizione della strategia nazionale per l'intelligenza artificiale. Questa serve per favorire «la collaborazione tra le amministrazioni pubbliche e i soggetti privati relativamente allo sviluppo e all'adozione di sistemi di intelligenza artificiale, coordina(re) l'attività della pubblica amministrazione in materia, promuovere la ricerca e la diffusione della conoscenza in materia di intelligenza artificiale e indirizza le misure e gli incentivi finalizzati allo sviluppo imprenditoriale e industriale dell'intelligenza artificiale» (art. 19, secondo comma, l. 132/2025).

La struttura presso la Presidenza del Consiglio dei ministri «provvede al coordinamento e al monitoraggio dell'attuazione della strategia (…), avvalendosi dell'Agenzia per l'Italia digitale, d'intesa, per gli aspetti di competenza, con l'Agenzia per la cybersicurezza nazionale e sentiti la Banca d'Italia, la Commissione nazionale per le società e la borsa (CONSOB) e l'Istituto per la vigilanza sulle assicurazioni (IVASS) in qualità di autorità di vigilanza del mercato» (art. 19, quarto comma, l. 132/2025).

In sintesi: la principale autorità di vigilanza nazionale è l'ACN (Agenzia Nazionale per la Cybersicurezza), la quale si occupa della vigilanza, nonché delle attività ispettive e

---

[59] In questo ambito il Gruppo di esperti ha anche limitati poteri esecutivi. Il considerando 163 prevede, infatti che: «Al fine di integrare i sistemi di governance per i modelli di IA per finalità generali, il gruppo di esperti scientifici dovrebbe sostenere le attività di monitoraggio dell'ufficio per l'IA e può, in alcuni casi, fornire segnalazioni qualificate all'ufficio per l'IA che avviano attività di follow-up quali indagini. Ciò dovrebbe valere quando il gruppo di esperti scientifici ha motivo di sospettare che un modello di IA per finalità generali rappresenti un rischio concreto e identificabile a livello dell'Unione. Inoltre, ciò dovrebbe verificarsi nel caso in cui il gruppo di esperti scientifici abbia motivo di sospettare che un modello di IA per finalità generali soddisfa i criteri che comporterebbero una classificazione come modello di IA per finalità generali con rischio sistemico. Per dotare il gruppo di esperti scientifici delle informazioni necessarie per lo svolgimento di tali compiti, è opportuno prevedere un meccanismo in base al quale il gruppo di esperti scientifici può chiedere alla Commissione di esigere da un fornitore documentazione o informazioni».

[60] Sul sistema italiano v. E. GUARNACCIA, *Le autorità nazionali competenti*, in G. CASSANO, E.M. TRIPODI (a cura di), *Il regolamento europeo sull'intelligenza artificiale*, cit., p. 743 ss.; R. LATTANZI, *AI Act e autorità di protezione dei dati personali*, in O. POLLICINO, F. DONATI, G. FINOCCHIARO, F. PAOLUCCI (a cura di), *La disciplina dell'intelligenza artificiale*, cit., p. 367 ss.; A. DE TOMMASO, M.L. MARINELLO, *Il ruolo di AGCOM nella regolazione dell'intelligenza artificiale*, ivi, p. 399 ss.

[61] L. 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, in GU n. 223, del 25 settembre 2025.

sanzionatorie dei sistemi di intelligenza artificiale, oltre, ovviamente, a curare i profili della sicurezza. Inoltre la legge ha istituito l'AgID, l'Agenzia per l'Italia Digitale, quale autorità di notifica e per effettuare i compiti di valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale (art. 20, l. 132/2025).

Vi è infine anche un Comitato per il coordinamento presso Presidenza Consiglio dei Ministri, presieduto dal Presidente del Consiglio dei ministri, che «svolge funzioni di coordinamento dell'azione di indirizzo e di promozione delle attività di ricerca, di sperimentazione, di sviluppo, di adozione e di applicazione di sistemi e modelli di intelligenza artificiale svolte da enti e organismi nazionali pubblici o privati soggetti a vigilanza o destinatari di finanziamento pubblico, ivi comprese le fondazioni pubbliche o private vigilate o finanziate dallo Stato, che operano nel campo dell'innovazione digitale e dell'intelligenza artificiale».

In conclusione, vi è una congerie di autorità sia europee, sia nazionali, ognuna teoricamente competente per compiti specifici, ma che in realtà dovrà necessariamente coordinarsi e tenere conto delle attività poste in essere dalle altre autorità.

A questo punto viene spontaneo chiedersi sulla base di quali principi debba operarsi il coordinamento. Non può infatti liquidarsi, in maniera semplicistica, il tema del coordinamento, limitandoci a stabilire la prevalenza delle autorità europee su quelle nazionali, come si verifica, ad esempio in materia di concorrenza, nei rapporti tra la Commissione europea e le autorità nazionali incaricate del controllo sull'applicazione dei divieti in materia antitrust. Il principio della prevalenza del diritto dell'Unione europea, infatti, non risolve il problema del coordinamento, perché i compiti delle varie autorità coinvolte nell'applicazione del regolamento sull'intelligenza artificiale si assestano su piani paralleli, tra di loro non coincidenti: mentre quelle europee esercitano funzioni esecutive e consultive; quelle nazionali esercitano compiti di vigilanza e di controllo. Non ha pertanto senso a ribadire la prevalenza dell'ordinamento sovranazionale su quello nazionale, perché questo principio non apporta elementi utili, stante le evidenti diversità di ruoli.

L'unico caso nel quale la Corte di giustizia ha affrontato il problema del coordinamento tra autorità tributarie di funzioni differenti si è posto nella sentenza *Meta c. Bundeskartellamt*. In detta occasione la Corte di Lussemburgo affermò l'esistenza di un obbligo di coordinamento tra le autorità. Si può, infatti, leggere in detta sentenza che: «se è vero che… né il GDPR né alcun altro strumento del diritto dell'Unione prevedono norme specifiche a tal riguardo, ciò non toglie che… quando applicano il GDPR, le diverse autorità nazionali coinvolte sono tutte vincolate dal principio di leale cooperazione sancito all'articolo 4, paragrafo 3, TUE. …in forza di tale principio, nelle materie rientranti nel diritto dell'Unione, gli Stati membri, *ivi incluse le loro autorità amministrative, devono rispettarsi ed assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati*, adottare ogni misura atta ad assicurare l'esecuzione degli obblighi conseguenti, in particolare, agli atti delle istituzioni dell'Unione, nonché astenersi da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione»[62].

[62] Corte di giustizia, 23 luglio 2023, causa C-252/21, *Meta c. Bundeskartellamt*, ECLI:EU:C:2023:537, punto 53. Sul caso v., anche per ulteriori riferimenti, F. BATTAGLIA, *Il consumatore digitale nel diritto dell'Unione europea*, Napoli, 2023, p. 267 ss.; ID., *La sentenza Meta platforms. Riflessioni in materia di valore dei dati e libera espressione del consenso*, in *OIDU*, 2023, p. 723 ss.; P. MANZINI, *Antitrust e privacy: la strana coppia*, in *Quaderni AISDUE*, 2023, p. 196 ss.; P.J. VAN DE WAERDT, *Meta v Bundeskartellamt: Something Old, Something New*, in *European Papers*, 2023, p. 1077 ss.; A. LICASTRO, *Meta Platforms Inc., già Facebook Inc. v. Bundeskartellamt: la Corte di Giustizia dell'Unione Europea apre (finalmente) all'integrazione fra diritto antitrust e data protection*, in *Rivista della Regolazione dei mercati*, 2023, p. 503 ss.;

In sintesi, la Corte estese il principio di leale cooperazione, che per espressa previsione è destinato ad operare tra Stati membri ed istituzioni europee ovvero nei rapporti orizzontali tra queste ultime, anche ai rapporti intercorrenti tra autorità amministrative nazionali, allorché esse applicano il diritto dell'Unione europea.

Occorre tuttavia chiedersi, se un siffatto principio sia sufficiente nella materia oggetto delle riflessioni che stiamo svolgendo in questo paragrafo. È infatti ovvio che un conto è coordinare l'attività di due autorità che si occupano di materie eterogenee, come si verificava, per l'appunto nel caso *Meta* (rispettivamente: l'autorità garante della concorrenza e quella dedita alla protezione dei dati personali); mentre cosa ben diversa è coordinare l'attività di una pluralità di enti diversi con competenze non definite in maniera precisa e che appaiono parzialmente sovrapponibili. Ci sembra, infatti, che il legislatore europeo e quello nazionale dovranno escogitare, in questa materia, dei principi nuovi ed ulteriori, oltre a quello della prevalenza del diritto dell'Unione europea e del principio di cooperazione, per consentire all'interprete di stabilire di volta in volta come si possano svolgere tutte le attività di sorveglianza e deliberative in maniera coordinata.

Il regolamento 2024/1689 prevede, infine, un esteso apparato sanzionatorio. La violazione delle previsioni del regolamento è punita con un sistema di sanzioni pecuniarie commisurate, in misura proporzionale alla tipologia e alla gravità delle violazioni, in una percentuale variabile dal 3% al 7% del fatturato annuo globale dell'impresa autrice dell'illecito. Il regolamento stabilisce massimali più equi per PMI e Start-up al fine di assicurare che i sistemi di IA siano sviluppati ed impiegati in modo etico e legale.

8. *Un approccio timido del legislatore europeo?*

Le regole dell'AI ACT, similmente a quanto accaduto per il GDPR, entreranno in vigore in maniera scaglionata nel tempo, in tal modo consentendo alle imprese e alle pubbliche amministrazioni di adeguarsi progressivamente al nuovo quadro normativo[63].

Alla conclusione di tale sommaria disamina del regolamento permangono, tuttavia, diversi dubbi circa la sua reale efficacia e l'idoneità dello stesso a rafforzare un'effettiva sovranità digitale dell'Unione europea. Tale conclusione, infatti, discende da una serie di considerazioni.

In primo luogo, il legislatore europeo non intende affrontare tutti i problemi giuridici posti da detta tecnologia: egli, consapevolmente, mira essenzialmente a disciplinare l'accesso al mercato dei fornitori dei sistemi di intelligenza artificiale. Questa scelta, tuttavia, presenta dei costi ben precisi, in termini di assenza di regolamentazione. Innanzitutto non sono presenti regole uniformi di responsabilità, per i danni provocati dall'uso di sistemi di

A.C. WITT, *Meta v Bundeskartellamt–data-based Conduct between Antitrust Law and Regulation*, in *Journal of Antitrust Enforcement*, 2024, p. 345 ss.; M. PREVIATELLO, *The Duty of Sincere Cooperation between National Competition Authorities and Supervisory Authorities Established by the GDPR: Meta Platforms and Others*, in *BlogAISDUE*, 2024.

[63] Nello specifico, il regolamento è entrato in vigore 20 giorni dopo la pubblicazione nella Gazzetta ufficiale UE; esso si applicherà a far data dal 2 agosto 2026. Tuttavia, mentre i divieti relativi alle pratiche vietate (il c.d. rischio inaccettabile, di cui all'art. 5), si applicano a partire da sei mesi dopo l'entrata in vigore (quindi, già dal 2 febbraio 2025), i codici di buone pratiche, le norme sui sistemi di IA per finalità generali ed il sistema di *governance* si applicheranno solo a partire dal 2 agosto 2026. Infine, gli obblighi per i sistemi ad alto rischio trentasei mesi dopo l'entrata in vigore (2 agosto 2027).

intelligenza artificiale[64], con la conseguenza che le stesse finiranno per dipendere essenzialmente e dalle regole di diritto internazionale privato contenute nel regolamento c.d. Roma II, sulla legge applicabile alle obbligazioni non contrattuali[65].

Ma soprattutto, cosa assai più grave, il legislatore europeo ha omesso di prevedere specifiche misure di protezione dei diritti fondamentali. Infatti, al di là dell'affermazione di principio, secondo cui il legislatore europeo intende proteggere di diritti fondamentali, nel regolamento sull'intelligenza artificiale mancano, in realtà, specifiche forme di tutela per i singoli, con la conseguenza che queste sono eminentemente quelle previste dal regolamento sulla protezione dei dati[66]. Viene dunque da domandarsi se l'AI Act sia effettivamente protettivo per i diritti fondamentali[67]. Tanto più che la valutazione dell'impatto sui diritti fondamentali è, ai sensi dell'art. 26, rimesso agli stessi *deployer*: è agevole pensare che gli utilizzatori del sistema finiranno, nella maggior parte dei casi, con il minimizzare i rischi.

In secondo luogo l'AI Act lascia forse troppo margine agli Stati membri. Molte norme, infatti, non sono *self-executing* e necessitano, pertanto, di ulteriori provvedimenti legislativi da parte degli Stati membri per avere effetto diretto ed essere applicabili.

Un'altra criticità concerne il rischio di mancato coordinamento e le sovrapposizioni, finanche nella formulazione di talune disposizioni, con altri atti normativi adottati dalle istituzioni europee. Il problema si pone, in particolar modo, con il citato Regolamento sulla protezione dei dati personali. Alle volte, la circostanza che determinati diritti siano previsti da entrambe le fonti, come avviene ad esempio con il diritto a non essere sottoposto ad una decisione integralmente automatizzata, potrebbe finanche far sorgere dei dubbi su quale sia la reale portata del diritto che viene concretamente invocato in giudizio.

Inoltre il legislatore ha omesso di disciplinare aspetti rilevanti nel funzionamento dei sistemi di intelligenza artificiale, quali, in particolare, la tutela dell'ambiente. Questa è sì menzionata in vari considerando[68], ma di fatto non è affatto regolamentata se non in misura estremamente marginale[69]. In tal modo il regolamento finisce per lasciare scoperto proprio

---

[64] È noto, infatti, che il Parlamento europeo aveva a suo tempo emanato una risoluzione diretta alla Commissione europea affinché questa presentasse una proposta su regole armonizzate di responsabilità per l'uso dei sistemi di intelligenza artificiale (Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 2020/2014(INL)). Questa, tuttavia, non ha avuto seguito, preferendo la Commissione adottare la proposta che poi ha condotto all'adozione del regolamento 2024/1689. In assenza di una normativa uniforme, sono state sostenute eminentemente due tesi, in entrambi i casi tendenti ad ipotizzare una sorta di regime di responsabilità aggravata in capo al fornitore. Secondo il primo orientamento la responsabilità costituirebbe un regime da "colpa presunta". Secondo un altro orientamento, la responsabilità del fornitore sarebbe assimilabile alla categoria della responsabilità oggettiva, sulla falsariga della responsabilità del produttore nella direttiva da danno da prodotto. In dottrina v., quali esponenti delle due tesi, E. BOCCHINI, *La regolazione giuridica dell'intelligenza artificiale*, Torino, 2024, p. 101 ss.; A. ALBANESE, *La responsabilità extracontrattuale per l'utilizzo dei sistemi di I.A.*, in R. BOCCHINI (a cura di), *Trattato. Le Piattaforme digitali e-Agorà*, Torino, 2025, p. 506 ss., 519.

[65] Regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali (Roma II), in GUUE L 199 del 31.7.2007, pp. 40–49. In dottrina v. B. CAPPIELLO, *AI-systems and Non-Contractual Liability*, Torino, 2022.

[66] V. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, cit., p. 16.

[67] V. F. PAOLUCCI, *Shortcomings of the AI Act. Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights*, in *Verfassungsblog*, 14 marzo 2024; E. CIRONE, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in *Quaderni AISDUE*, Fascicolo speciale n. 2/2024, *La nuova disciplina UE sull'intelligenza artificiale.*

[68] V., ad es., i considerando n. 1, 2, 8, 27, 48, 130, 142, 155, 176.

[69] V., in particolare, l'art. 40, par. 1, del regolamento: «La richiesta di normazione chiede inoltre prodotti relativi a processi di comunicazione e documentazione *intesi a migliorare le prestazioni dei sistemi di IA in termini di risorse,*

uno degli aspetti negativi maggiormente impattanti dell'uso dei sistemi di intelligenza artificiale: ovvero le conseguenze che questo apporterà sul pianeta. Si tratta di un tema tuttora assai controverso, sia nella letteratura scientifica, che in quella specificamente giuridica; e che è sovente fonte di dibattito e di visioni contrastanti[70], rispetto al quale, il legislatore europeo – così attento alla tutela dell'ambiente in altri settori normativi (non fosse altro per il disposto dell'art. 11 TFUE) – bene avrebbe potuto introdurre previsioni rilevanti anche in questa materia.

Dal punto di vista economico, poi, occorre chiedersi se questo atto, piuttosto che rafforzare la c.d. sovranità digitale dell'Unione europea, non finisca con il minare la competitività delle imprese europee, le quali sono destinatarie di una serie molto nutrita di obblighi. Parrebbe quindi legittimo porre il dubbio se tale sistema normativo non finisca con il produrre il risultato opposto ovvero quello di aumentare il rischio di delocalizzazione.

L'ultima questione è cercare comprendere se l'AI Act sia in grado duplicare il successo del GDPR e rappresentare uno standard anche per Stati terzi. Capire, in altri termini, se questo regolamento possa effettivamente produrre un "effetto Bruxelles".

In realtà, la risposta, almeno allo stato, sembrerebbe negativa, perché lo stesso regolamento lascia troppo spazio alla regolamentazione privata, con ciò stesso diminuendone la portata e l'efficacia normativa. Inoltre esso affida un ruolo eccessivamente rilevante alla normativa delegata da parte della Commissione. L'organo esecutivo potrà infatti adottare atti delegati entro cinque anni dall'entrata in vigore (ed anche in futuro, se i colegislatori non revocheranno la delega), per: *i*) escludere che taluni sistemi, che non presentano rischi significativi per la salute ed i diritti fondamentali, siano ad alto rischio (6, par. 6); *ii*) aggiungere o modificare i casi d'uso dei sistemi ad alto rischio (7, par.1); *iii*) stabilire gli obblighi di conservazione della documentazione tecnica per aggiornarla al progresso tecnico; *iv*) adeguare i requisiti di conformità al progresso tecnico (43, parr. 5 e 6); stabilire il contenuto della dichiarazione di conformità (art. 47, par. 5).

In breve, vi sono margini di discrezionalità particolarmente ampi per gli Stati membri; troppa autonomia per i privati; eccessivi poteri normativi, su punti fondamentali della normativa regolamentare, in capo all'esecutivo europeo. Infine, decisamente numerose sono le autorità di *governance*, a vari livelli (europeo e nazionale), chiamate a vigilarne l'applicazione: esse assai difficilmente riusciranno ad operare in maniera fluida e condivisa, soprattutto perché nei rapporti reciproci manca un'autorità sovraordinata, come invece si verifica in materia di concorrenza. Sulla base di questi elementi, sembra necessario concludere che appare assai improbabile che il regolamento possa effettivamente rappresentare uno standard normativo suscettibile di imporsi a livello mondiale[71].

---

come la riduzione del consumo di energia e di altre risorse del sistema di IA ad alto rischio durante il suo ciclo di vita, e allo sviluppo efficiente sotto il profilo energetico dei modelli di IA per finalità generali» (corsivo aggiunto).

[70] V. K. CRAWFORD, *Né intelligente, né artificiale. Il lato oscuro dell'IA*, Bologna, 2021, p. 49 ss.; M.A. ALLOGHANI, *Artificial Intelligence and Sustainability*, London, 2023, spec. p. 65 ss.; nonché gli scritti pubblicati nel volume C. UBALDO, K. ALEXANDER (a cura di), *Sostenibilità e intelligenza artificiale: resilienza o panacea?*, Milano, 2025. Per gli aspetti giuridici v. C. DI FRANCESCO MAESA, *Economia circolare e IA: a che condizioni è una sfida possibile per l'UE?*, in *Quaderni AISDUE*, Convegno di Siena 4 e 5 dicembre 2024.

[71] V. anche i dubbi di M. BASSINI, *Oggetto, campo di applicazione e ambito territoriale*, cit., p. 139 s.; U. PAGALLO, *Why the AI Act Won't Trigger a Brussels Effect*, in corso di pubblicazione nel volume *AI Approaches to the Complexity of Legal Systems*, Springer, ma già consultabile al sito https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4696148