AI ACT E PROTEZIONE DEI DIRITTI: ANALISI DEL RUOLO DELL'ARTICOLO 5 DEL REGOLAMENTO NELLA TUTELA DEI DIRITTI FONDAMENTALI *

di Alice Bertini**

Sommario. 1. Dall'origine dell'AI alla sfida giuridica: evoluzione tecnologica e tutela dei diritti fondamentali nell'era digitale – 2. L'evoluzione della disciplina europea in materia di intelligenza artificiale: dalle prime iniziative alla proposta di Regolamento – 3. *Artificial Intelligence Act*: l'avvento del primo Regolamento in materia di regolamentazione dell'intelligenza artificiale – 4. Le c.d. «pratiche vietate» e la tutela dei diritti fondamentali ai sensi dell'articolo 5 del Regolamento – 5. Le criticità normative e applicative dell'articolo 5 del Regolamento e il contributo offerto dalle recenti Linee guida della Commissione europea – 6. La reale efficacia dell'*AI Act* (e del suo articolo 5) nella tutela dei diritti fondamentali: una riflessione conclusiva.

1. Dall'origine dell'AI alla sfida giuridica: evoluzione tecnologica e tutela dei diritti fondamentali nell'era digitale. La storia dell'Intelligenza Artificiale, contrariamente a quanto si possa pensare, non è poi così recente. L'acronimo *«Artificial Intelligence»* (da cui il termine AI) è stato coniato nel 1956 durante un workshop al Dartmouth College di Hanover[1], dove i «padri dell'intelligenza artificiale»[2] avviarono i primi studi finalizzati alla creazione di una macchina o computer in grado di agire e pensare come un essere umano: lo scopo del seminario era infatti quello di «esaminare la congettura che ogni aspetto dell'apprendimento o ogni altra caratteristica dell'intelligenza possa essere, in linea di principio, descritto in modo tanto preciso che si possa far sì che una macchina lo simuli» [3]. Si è trattato di un evento di estrema rilevanza, che viene ormai pacificamente considerato quale momento fondativo dell'intelligenza artificiale come disciplina accademica, stimolo primo e primordiale che ha avviato i numerosi studi ed esperimenti degli anni successivi[4].
Gli anni che seguirono il seminario di Dartmouth possono essere definiti come gli anni delle

---

* *Sottoposto a referaggio*.

** Dottoranda in Sistemi Giuridici e Dimensione Sovranazionale – Università *Magna Graecia* di Catanzaro.

[1] Il c.d. *Darmouth Summer Research Project on Artificial Intelligence*: per sei settimane, un gruppo ristretto di ricercatori, matematici e scienziati si è riunito per discutere idee, definire problemi e riflettere sulla progettazione di algoritmi di intelligenza artificiale. Tale evento, che ha portato a concepire l'intelligenza artificiale come sapere accademico, ha riunito i pionieri dell'*AI* e creato la rete che avrebbe guidato lo sviluppo della disciplina nei decenni successivi.

[2] Tra cui è possibile ricordare, a titolo meramente esemplificativo, Claude Shannon, John McCarthy, Nathaniel Rochester e Marvin Minsky, gli organizzatori del workshop; così si legge in: P. Traverso, *Breve introduzione tecnica all'Intelligenza Artificiale* in *DPCEOnline,* 1, 2022, 155.

[3] S.J. Russell, P. Norving, J.F. Canny, *Artificial Intelligence: A Modern Approach*, Saddle River, 2010.

[4] A. Ballatore, S. Natale, *Fallimenti, controversie e il mito tecnologico dell'Intelligenza Artificiale*, in P. Magaudda e G. Balbi (a cura di) *Fallimenti digitali: un'archeologia dei «nuovi» media*, Milano, 2018, 137 – 149.

grandi aspettative, alimentate dai primi successi dell'AI: nel corso degli anni '60, infatti, grazie soprattutto ai primi ed ingenti finanziamenti ottenuti dalle istituzioni governative statunitensi, i ricercatori dell'epoca ottennero risultati promettenti in diversi settori. Ciò finì per sollevare un fervente ottimismo tra la comunità scientifica, circa le possibili ed immediate applicazioni di 'sistemi intelligenti' nei diversi settori sociali.

Tuttavia, soprattutto nei primi anni '70 del Novecento, l'AI iniziò ad affrontare i primi insuccessi e le prime delusioni, dovuti anche al mancato raggiungimento di obiettivi forse troppo ambiziosi per l'epoca. Ben presto l'ottimismo iniziale iniziò dunque a scontrarsi con la realtà: realizzare programmi in grado di comprendere e soprattutto replicare l'intelligenza umana diventa un obiettivo estremamente complesso da raggiungere, che necessita di tempo, lavoro e risorse[5].

La storia dell'AI è dunque fatta di luci ed ombre, di «primavere» ed «inverni», di scoperte e ambizioni, ma anche di delusioni e periodi di sconforto. Tanto che si arriva a parlare, tra la comunità scientifica, di vere e proprie «stagioni dell'*AI*» (*«AI seasons»*)[6].

Ed è proprio nel susseguirsi di queste stagioni – di entusiasmi e disillusioni, di scoperte e battute d'arresto – che prende forma una consapevolezza destinata a diventare ineludibile: lo sviluppo dell'*AI* non è neutro rispetto all'ordine giuridico. Ogni avanzamento tecnologico porta con sé ricadute concrete sui diritti degli individui – dalla *privacy*, alla non discriminazione, alla dignità ad un equo trattamento – e pone il diritto di fronte alla necessità di rispondere a domande per le quali non esistono ancora categorie consolidate. La questione non è più soltanto tecnica o scientifica, ma diventa profondamente giuridica e politica[7].

Recentemente si sta assistendo senz'altro al periodo più fecondo per tale materia, ad una delle «estati più roventi», in cui l'implementazione e lo sviluppo di sistemi di intelligenza artificiale si stanno diffondendo nei più disparati settori del vivere umano.

L'*AI* è diventata un «fatto sociale totale» come definito da Garapon e Lassègue[8] e la sensazione è che essa stia effettivamente cambiando il mondo, concretizzando quello che fino a pochi anni fa era proprio soltanto della *science fiction*: *driveless cars*, sistemi diagnostici e chirurgici ad autonomia crescente, robot umanoidi dotati di intelligenza artificiale. Tutte pratiche che generano quesiti antropologici riguardo al rapporto fra uomo e robot e, più in generale, fra uomo e *AI*[9].

Le implicazioni giuridiche di questa trasformazione sono molteplici. Sul piano dei diritti fondamentali, l'utilizzo di sistemi di *AI* solleva interrogativi di primaria importanza: i sistemi di riconoscimento facciale e di profilazione algoritmica mettono sotto pressione il diritto alla privacy e alla protezione dei dati personali; i meccanismi decisionali automatizzati incidono sul diritto ad un trattamento equo e non discriminatorio; la crescente autonomia dei sistemi *AI-based* erode infine le tradizionali categorie di responsabilità, rendendo difficile imputare ad un soggetto determinato le conseguenze di una scelta generata algoritmicamente.

La società è dunque oggi immersa in una vera e propria *«AI revolution»*[10] che ha sì grandi potenzialità, ma che presenta altresì la necessità di essere compresa, gestita e adeguatamente

---

[5] D. Crevier, *AI: The Tumultuous History of the Search for Artificial Intelligence*, New York, 1994.

[6] L. Portinale, *Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori*, in *MediaLaws*, 3, 2021, 13 – 20.

[7] Interessante, sul punto, M. Suleyman, *The Coming Wave: Technology, Power, and the Twanty-first Century's Greatest Dilemma*, New York, 2023. L'autore analizza l'impatto della diffusione dei sistemi *AI-based* sull'economica, la politica e la società, evidenziando le sfide e le opportunità che ciò comporta per il futuro dell'umanità stessa.

[8] A. Garapon, J. Lassègue, La *Giustizia digitale. Determinismo tecnologico e libertà*, Bologna, 2021, 79.

[9] M. Ferraris, *La pelle. Cosa significa pensare nell'epoca dell'intelligenza artificiale*, Bologna, 2025. L'autore esplora la differenza tra l'essere umano e le macchine intelligenti, concentrandosi sull'elemento della pelle come metafora e realtà incarnata dell'esistenza umana, contrapposta al silicio di cui sono composti i sistemi di *AI*.

[10] A. D'Aloia, *Il diritto verso «il nuovo mondo». Le sfide dell'Intelligenza Artificiale* in, A. D'Aloia (a cura di) *Il diritto e l'incerto del mestiere di vivere. Ricerche di biodiritto*, Padova, 2021, 228.

regolamentata. Infatti, se fino a pochi anni fa il tema del rapporto fra AI e sistemi sociali e giuridici era limitato ad una sfera ristretta di tematiche e specialisti di settore[11], oggi è esploso in tutta la sua complessità di implicazioni e sfide per il futuro, considerando, ormai, quale dato certo, il fatto che «l'AI non è più un'opzione disattivabile, un interruttore che avremo ancora possibilità di spegnere. È diventata indispensabile»[12].

Di fronte a tutto ciò, il diritto è come travolto da tale evoluzione che pone il giurista davanti a quesiti inediti e a nuove necessità. Pertanto, innanzitutto, il diritto deve essere in grado di dettare una regolamentazione di tale nuova «potenza cibernetica»[13], che sia quanto più possibilmente globale, o quanto meno sovrastatale: è necessario ragionare in una dimensione ampia, ricercando principi comuni, nella consapevolezza che approcci parziali siano inadeguati di fronte ad una tematica dal carattere così ampio e in grado di investire l'intera esistenza umana[14].

Date queste premesse, si veda come l'Unione europea sia da anni impegnata nel tentativo di regolare l'*AI* e le sue applicazioni, cercando di bilanciare l'esigenza di potenziare lo sviluppo tecnologico con quella di creare un sistema e una tecnologia sostenibile ed attenta alla tutela dei diritti fondamentali.

Per vero, l'attenzione dell'Unione europea al tema della regolamentazione dei sistemi di intelligenza artificiale comincia a concretizzarsi in modo sistematico negli ultimi dieci anni, in risposta alla crescente consapevolezza ed evidenza dell'impatto etico, economico e giuridico che questa tecnologia è in grado di generare[15].

Un primo concreto passo avanti nella regolamentazione europea in materia è stato fatto soltanto nel 2020 con la pubblicazione da parte della Commissione europea del Libro Bianco[16] sull'*AI*, elaborato con l'intento di indicare le opzioni politiche volte a garantire una crescente implementazione di sistemi *AI-based*, affrontando i rischi associati al loro utilizzo[17]. Viene chiarito fin dal subito che l'obiettivo principale deve essere quello di creare un'*AI* antropocentrica ed affidabile (*anthropocentric and trustworthy*) su cui i cittadini possano contare per incrementare il proprio benessere, pur sempre nel rispetto dei propri diritti fondamentali[18].

In seguito, nel corso del 2020 e del 2021, vengono adottate dal Parlamento europeo diverse risoluzioni (seppur non vincolanti) volte ad incentivare la Commissione ad attivarsi per

---

[11] A titolo esemplificativo, per lungo tempo, il confronto sull'intelligenza artificiale è rimasto confinato ad ambiti specialistici, interessando prevalentemente profili quali la protezione dei dati, la responsabilità algoritmica, l'automazione industriale, la cybersecurity e l'etica computazione, con il coinvolgimento quasi esclusivo di informatici, ingegneri, giuristi delle nuove tecnologie, *data scientist* ed esperti di etica digitale. Cfr., *ex multis*, U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2018; L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022.

[12] L. Alexandre, *La guerra delle intelligenze*, Torino, 2018, 295.

[13] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà* in *BioLaw Journal - rivista di biodiritto*, 1, 2019, 89.

[14] M. Coeckelbergh, *AI Ethics*, Cambridge, 2020.

[15] L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022. L'autore analizza l'impatto dell'AI nella trasformazione della società, dell'economia e della vita quotidiana, sottolineando l'importanza di governare tale crescente fenomeno in modo responsabile.

[16] Un Libro Bianco è un documento ufficiale della Commissione europea che presenta proposte di intervento in un determinato settore, delineando possibili strategie e opzioni normative da seguire. Non ha valore vincolante, tuttavia è un importante catalizzatore del dibattito istituzionale, in grado di attivare ed orientare future iniziative legislative sulle tematiche trattate.

[17] Cfr. *Libro Bianco sull'Intelligenza Artificiale – un approccio europeo all'eccellenza e alla fiducia*. COM(2020)65 *final*. Il testo ufficiale è consultabile sul sito web ufficiale della Commissione europea.

[18] G. Olivato, *UE – Commissione europea – Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, in *BioLaw Journal – Rivista di Biodiritto*, pubblicato il 19 febbraio 2020.

l'elaborazione di una proposta legislativa compiuta e completa in materia, al fine di introdurre una regolamentazione che consenta di sfruttare le opportunità e i benefici dell'AI e contestualmente di garantire la protezione dei principi etici e dei valori europei[19].
Arrivando ad oggi, l'ultima frontiera della «via europea all'IA»[20] è rappresentata dal cosiddetto *AI Act* o *Artificial Intelligence Act*, strumento normativo elaborato con l'intento di introdurre regole uniformi in materia di sviluppo, produzione e commercializzazione di sistemi di *AI* nel mercato unico dell'UE, in conformità con i valori ed i diritti fondamentali ivi promossi e tutelati[21].
La portata dell'*AI Act*, peraltro, non si esaurisce nel perimetro del mercato unico europeo: esso si candida a diventare, secondo la logica del cosiddetto «Effetto Bruxelles» (*Brussels Effect*)[22], un modello normativo di riferimento su scala globale. Con l'espressione «Effetto Bruxelles» si indica il fenomeno per cui la regolamentazione europea tende ad imporsi *de facto* come standard internazionale, poiché le imprese multinazionali, per accedere al mercato unico, adeguano i propri prodotti e processi alle norme europee, finendo per applicarle in modo uniforme anche al di fuori dell'UE[23]. Si tratta di un meccanismo già osservato con il GDPR in materia di protezione dei dati personali, e che l'*AI Act* potrebbe replicare nel settore dell'intelligenza artificiale, classificandosi quale primo quadro giuridico completo sull'IA a livello mondiale e ponendo l'Unione europea in una posizione di assoluta avanguardia nella definizione degli standard regolativi globali per queste nuove tecnologie.
Tutto ciò premesso, resta ora da comprendere se tale nuova regolamentazione, con la sua struttura incentrata su un approccio basato sul rischio (c.d. *risk based approach*) e il suo meccanismo di divieti ed eccezioni, sia realmente in grado di fornire una risposta concreta ed efficace al bisogno crescente di tutela dei nostri diritti fondamentali nell'era digitale, senza frenare lo sviluppo tecnologico.

2. L'evoluzione della disciplina europea in materia di intelligenza artificiale: dalle prime iniziative alla proposta di Regolamento. Come già esposto *supra*, l'Unione europea si è da anni attivata per cercare di elaborare una risposta legislativa coerente e mirata di fronte al crescente bisogno di regolamentare la rapida diffusione dei sistemi di intelligenza artificiale. Tale impegno si è concretizzato, dapprima, in due importanti Comunicazioni adottate dalla Commissione europea nell'aprile e dicembre 2018[24], con l'intento di iniziare a delineare una

[19] Tali risoluzioni si sono rivelate essere centrali nell'orientare la legislazione europea successiva in materia di intelligenza artificiale. Tali provvedimenti hanno affrontato una pluralità di tematiche, fra cui l'etica dell'AI, la responsabilità civile, la proprietà intellettuale, l'uso militare e penale dell'AI, richiamando sempre la necessità di tutelare i diritti fondamentali e garantire trasparenza e controllo umano.
[20] M. Zanichelli, *Ecosistemi, opacità, autonomia: le sfide dell'intelligenza artificiale in alcune proposte recenti della Commissione europea*, in A. D'Aloia (a cura di) *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2020, 70.
[21] Si tratta del Regolamento del Parlamento europeo e del Consiglio, Reg. UE 1689/2024 del 13/06/2024, che stabilisce regole armonizzate sull'intelligenza artificiale.
[22] L'espressione *Brussels Effect* è stata resa celebre dalla giurista danese Anu Bradford, principalmente nella sua monografia *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020. Con tale locuzione si indica il fenomeno per cui l'Unione europea, in virtù delle dimensioni del proprio mercato interno e della solidità del proprio apparato regolatorio. È in grado di imporre i propri standard normativi a livello globale, senza ricorrere a strumenti di diritto internazionale né a meccanismi coercitivi di natura extraterritoriale.
[23] Per un approfondimento sul concetto di *Brussels Effect* e sulle sue applicazioni anche nel settore della regolamentazione digitale, si vedano, oltre al già citato lavoro di A. Bradford, *ex multis*: K. Bamberger, D. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, Cambridge, 2015; A. Bradford, J.N. Herrera, V. Rotaru, *The European Union in a globalised world: the Brussels effect*, in *RED*, 2, 2021, 75-79; M. Ylonen, *Reconceptualising the Brussels Effect*, in *Journal Common Market Studies*, vol. 64, 1, 2026, 100-124.
[24] Si tratta, da un lato, della COM(2018)237 dal titolo *Intelligenza artificiale per l'Europa* adottata nell'aprile del 2018, con cui la Commissione ha presentato una prima strategia europea sull'IA; e, dall'altro lato, della

strategia europea per la creazione di un mercato unico digitale. In particolare, nella Comunicazione del dicembre 2018 – COM (2018)795 – la Commissione europea e gli Stati membri hanno presentato un *Piano coordinato sull'intelligenza artificiale* con l'obiettivo di allineare strategie nazionali, investimenti e priorità politiche in un settore in rapida evoluzione, come quello ICT[25].

Un passo successivo di grande importanza è stato fatto poi nel 2019, quando la Commissione europea – con il contributo di organismi di esperti come lo *High-Level Expert Group on Artificial Intelligence*[26] – ha elaborato una serie di linee guida etiche per uno sviluppo tecnologico conforme ai valori europei e finalizzato alla predisposizione di un'*AI* affidabile. Tali linee guida[27] elencano i sette requisiti chiave che i sistemi *AI-based* devono soddisfare per essere realmente considerati affidabili: supervisione umana, robustezza tecnica e sicurezza, *privacy* e *governance* dei dati, trasparenza, non discriminazione ed equità, benessere sociale e ambientale e, infine, responsabilità.

Da qui si inizia a percepire concretamente la necessità di tradurre tali principi astratti in strumenti normativi maggiormente vincolanti ed operativi.

Il passo decisivo verso una disciplina più organica della materia è rappresentato dall'approvazione del Libro Bianco sull'intelligenza artificiale, pubblicato dalla Commissione europea il 19 febbraio del 2020, sulla base della strategia europea per l'intelligenza artificiale presentata nel 2018[28]. Già nell'introduzione di tale documento, la Commissione riconosce l'ambivalenza del rapporto tra salvaguardia dei diritti della società civile e diffusione dei sistemi di *AI*: il rapido sviluppo di tali tecnologie in vari e disparati settori del vivere umano (quali, *ex multis*, l'assistenza sanitaria, l'agricoltura, la mitigazione dei cambiamenti climatici) può senz'altro comportare enormi benefici ma, specularmente, tale diffusione porta con sé una serie di rischi potenziali, che necessitano di una pronta riposta normativa. In particolare, «in un contesto di forte concorrenza globale, è necessario un solido approccio europeo (…). Per sfruttare le opportunità e affrontare le sfide derivanti dall'IA, l'UE deve parlare con un'unica voce e definire il suo modo di promuovere lo sviluppo e la diffusione dell'IA basandosi sui valori europei. (…) La Commissione sostiene pertanto un approccio normativo e orientato agli investimenti con il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi associati a determinati utilizzi di questa nuova tecnologia. Lo scopo del presente libro bianco è definire le opzioni strategiche su come raggiungere tali obiettivi»[29].

Fin da subito, pertanto, appare chiaro l'obiettivo della Commissione: dettare alcune prime linee guida per orientare la futura regolamentazione europea dell'intelligenza artificiale, per

---

COM(2018)795 adottata nel dicembre dello stesso anno, con cui è stato presentato un *Piano coordinato sull'intelligenza artificiale* con l'obiettivo di rafforzare la cooperazione tra i singoli Stati membri nella regolamentazione e commercializzazione dei sistemi di *AI*.

[25] Il settore ICT (*Information and Communication Technology*) ricomprendere tutte le tecnologie e le attività legate alla gestione e trasmissione di informazioni digitali, includendo hardware, software, reti, internet e servizi connessi.

[26] L'*High-Level Group on Artificial* Intelligence (HLEG-AI) è un gruppo indipendente di esperti istituito dalla Commissione europea nel 2018 per supportare l'elaborazione della strategia europea sull'IA. Ha il compito di fornire consulenza tecnica e orientamenti etici ed è stato creato per garantire un approccio fondato su valori europei e contribuire alla definizione di un quadro normativo coerente ed affidabile.

[27] Tali linee guida sono definite *Ethics Guidelines for Trustworthy AI* e definiscono i requisiti fondamentali che un sistema di intelligenza artificiale deve rispettare per essere considerato davvero affidabile. Tali linee guida, seppur non vincolanti, hanno costituito la principale base etica e concettuale per la successiva proposta di Regolamento.

[28] Nella stessa premessa introduttiva del Libro Bianco sull'*AI*, la Commissione espressamente ribadisce la necessità di adottare un approccio europeo solido in materia, «basato sulla strategia europea per l'IA presentata nell'aprile del 2018» con la COM(2018) 237 *final*.

[29] Dall'introduzione del testo del Libro Bianco sull'AI.

arrivare ad una normativa che sia unitaria, solida e incentrata sul raggiungimento di un adeguato bilanciamento tra innovazione tecnologica e tutela dei valori europei.
Sulla scorta di tali premesse, il Libro Bianco si articola essenzialmente in due pilastri, ovvero le Sezioni 4 e 5, rispettivamente dedicate alla creazione di un «ecosistema di eccellenza, che possa sostenere lo sviluppo e l'adozione dell'IA nell'economia e nella pubblica amministrazione dell'UE»[30], nonché di un «ecosistema di fiducia» che deve guidare cittadini ed imprese nell'utilizzo dei sistemi *AI-based*[31].
Per il consolidamento di tali premesse, da un lato, fondamentale sarà incrementare gli investimenti, il sostegno alla ricerca, nonché la creazione di reti di competenze europee e sviluppo delle capacità digitali; dall'altro lato, assicurare lo sviluppo di un'intelligenza artificiale affidabile e antropocentrica, su cui i cittadini sentano di poter contare per incrementare il proprio benessere, senza temere che tale tecnologia possa avere effetti indesiderati o essere utilizzata dolosamente[32]. Garantire affidabilità e sicurezza nell'uso dei sistemi di AI è essenziale, in quanto «oltre alla mancanza di investimenti e di competenze, la mancanza di fiducia è uno dei fattori principali che frenano una più ampia adozione dell'IA»[33].
Attraverso tale primo documento (nonché sulla scorta delle successive risoluzioni sull'*AI* adottate dal Parlamento europeo[34]), la Commissione ha posto le basi per la successiva proposta legislativa dell'*AI Act*, delineando fin dal principio un modello europeo che mira a favorire l'innovazione tecnologica senza tuttavia compromettere la protezione dei diritti e la fiducia dei cittadini.

3. Artificial Intelligence Act: l'avvento del primo Regolamento in materia di regolamentazione dell'intelligenza artificiale. Ciò premesso, l'*iter* che ha condotto all'approvazione definitiva del testo attuale del Regolamento (UE) 2024/1689 è stato lungo e tortuoso[35]. Esso ha avuto formalmente inizio il 21 aprile 2021[36] quando la Commissione europea ha presentato una proposta di regolamento volto ad armonizzare le regole europee sull'intelligenza artificiale, nonché un piano coordinato che comprende una serie di azioni congiunte per la Commissione e gli Stati membri. Nella relazione esplicativa di accompagnamento alla suddetta proposta da subito si evince – in linea con quanto già statuito nel Libro Bianco sull'*AI* – quale deve essere l'obiettivo da perseguire: «preservare la *leadership* tecnologica dell'UE e garantire che i cittadini europei possano beneficiare delle nuove tecnologie sviluppate e funzionanti nel rispetto dei valori, dei diritti fondamentali e dei principi dell'Unione»[37]. Pertanto, fin da questa embrionale proposta, l'*AI Act* viene presentato come un quadro normativo che intende innanzitutto tutelare cittadini ed imprese – garantendo l'impiego di un AI affidabile e «umanocentrica» – e favorire lo sviluppo

[30] § 4 del Libro Bianco sull'AI.
[31] G. Olivato, op. cit.
[32] L. Mischitelli, *La strategia europea sull'intelligenza artificiale: stato dell'arte e scenari futuri*, in *Agenda Digitale*, pubblicato il: 6 ottobre 2020.
[33] § 5 del Libro Bianco sull'AI.
[34] Come già illustrato nel paragrafo introduttivo del presente contributo alla pagina 3.
[35] Innanzitutto, di primaria rilevanza è evidenziare la scelta normativa di ricorrere ad un Regolamento, quale fonte vincolante in tutti i suoi elementi e direttamente applicabile all'interno dei singoli Stati membri, senza necessità di ricorrere ad atti di recepimento interni. P. Mengozzi, C. Morviducci, *Istituzioni di diritto dell'Unione Europea*, Padova, 2018.
[36] In realtà, tale proposta di regolamento (COM(2021)206), ha visto la luce a seguito di un'ampia consultazione pubblica e delle risoluzioni adottate dal Parlamento europeo nel 2020 e 2021 con cui, come detto, è stato sollecitato un intervento normativo organico in materia. Il testo della proposta è consultabile online sul sito web ufficiale dell'Unione europea.
[37] Così al § 1 della proposta, in cui vengono enunciate le motivazioni e gli obiettivi della stessa.

tecnologico europeo, assicurando nel complesso che tale nuova tecnologia sia utilizzata come strumento al servizio della società, nel rispetto dei diritti e dei valori sanciti dall'Unione europea[38].

Dopo la pubblicazione della proposta di regolamento, si è aperto il procedimento legislativo vero e proprio, con l'avvio dei lavori paralleli del Parlamento europeo e del Consiglio[39].

In Parlamento il testo del regolamento è stato più volte oggetto di emendamenti e modifiche, incentrate principalmente sull'elaborazione di un approccio più restrittivo, soprattutto in materia di pratiche vietate. Il Consiglio, invece, nel dicembre del 2022 formalizza la sua posizione sul testo del regolamento, in un orientamento generale[40], in cui viene ribadita la necessità di articolare la normativa in modo da assicurare che i sistemi di *AI* immessi sul mercato siano sicuri e rispettosi dei diritti e valori riconosciuti in UE.

Da qui, si aprono i veri e propri triloghi tra le istituzioni europee al fine di raggiungere un accordo sul testo definitivo[41].

Solo dopo mesi di scambi e negoziati, il 9 dicembre 2023, viene raggiunto un accordo tra Parlamento europeo e Consiglio sul testo della normativa, che verrà poi definitivamente approvato dal Parlamento europeo il 13 marzo 2024 e dal passaggio formale in Consiglio, avvenuto il 21 maggio dello stesso anno. Viene in tal modo completato l'*iter* di approvazione del Regolamento, che è entrato in vigore a partire dall'agosto dello scorso anno[42].

Ricostruito brevemente il percorso che ha condotto all'approvazione del testo definitivo dell'*AI Act*, è importante ora segnalare quello che è l'obiettivo primario del Regolamento, ovvero garantire la sicurezza dei sistemi di AI immessi sul mercato e la loro conformità alla normativa in tema di diritti fondamentali, per facilitare la creazione di un mercato unico europeo anche in tale settore[43].

Innanzitutto, quindi, il *fil rouge* che tiene insieme l'intero testo normativo è dato dalla necessità di predisporre un quadro normativo orizzontale ed armonizzato per un'adeguata regolamentazione dell'intelligenza artificiale in tutta Europa, nella consapevolezza che approcci frammentari e normative nazionali eterogenee possono condurre a divisioni interne al mercato unico europeo, diventando un ostacolo alla produzione e diffusione di prodotti e

---

[38] R. Panetta, *AI Act: cos'è e come plasma l'intelligenza artificiale in Europa*, in *Agenda Digitale*, originariamente pubblicato il 12 marzo 2024.

[39] Per un approfondimento sui procedimenti di formazione degli atti aventi forza di legge nell'Unione europea, si veda, *ex multis*: G. Strozzi, R. Mastroianni, *Diritto dell'Unione Europea. Parte istituzionale*, Torino, 2020, 183 – 200.

[40] «L'intelligenza artificiale è di fondamente importanza per il nostro futuro. Oggi siamo riusciti a raggiungere un delicato equilibrio che stimolerà l'innovazione e l'adozione della tecnologia dell'intelligenza artificiale in tutta Europa. Con tutti i vantaggi che presenta, da un lato, e nel pieno rispetto dei diritti fondamentali dei nostri cittadini, dall'altro», con queste parole Ivan Bartoš – vice primo ministro ceco per la Digitalizzazione e ministro dello Sviluppo regionale – commenta il raggiungimento di tale orientamento generale in Consiglio.

[41] I triloghi sono negoziati informali tra le istituzioni coinvolte nel procedimento legislativo dell'Unione europea – Commissione, Parlamento e Consiglio. Sono funzionali a ricercare rapidamente un accordo sul testo di un atto legislativo. Pur non essendo previsti formalmente dai Trattati europei, sono divenuti una prassi consolidata nell'ordinario *iter* legislativo, visto che gli stessi consentono di conciliare le diverse posizioni istituzionali e di accelerare l'adozione finale degli atti legislativi. R. Adam, A. Tizzano, *Manuale di Diritto dell'Unione Europea*, Torino, 2024.

[42] Come si evidenzierà meglio in seguito, l'*AI Act* è formalmente entrato in vigore i 1° agosto 2024, tuttavia molte delle sue disposizioni diverranno pienamente applicabili in fasi diverse, ciò principalmente per consentire agli Stati membri e agli operatori economici di adeguarsi progressivamente al nuovo quadro normativo. L'applicazione completa è prevista per agosto 2026 (con eccezione per i sistemi ad alto rischio, per i quali il periodo di transizione si estende fino ad agosto 2027). T. Ricci, *AI Act, partiti i divieti: ecco che devono fare le aziende UE*, in *Agenda Digitale*, pubblicato il 3 febbraio 2025.

[43] C. Casonato, O. Giulia, *AI Regulation in Europe: Exploring the Artificial Intelligence Act*, in A. Fabris, S. Belardinelli, *Digital Environments and Human Relations*, Berlino, 2024, 87 – 112.

servizi di intelligenza artificiale nei vari Paesi[44].
Tale auspicata omogeneità normativa mira senz'altro a promuovere lo sviluppo e l'adozione dell'intelligenza artificiale come tecnologia abilitante per la competitività europea[45]; tuttavia, specularmente, tale finalità deve armonizzarsi con la necessità di assicurare la diffusione di un'intelligenza artificiale antropocentrica ed affidabile, in grado di garantire la maggior tutela possibile riconosciuta ai diritti e ai valori sanciti dalla Carta dei diritti fondamentali dell'Unione europea (quali la salute e la sicurezza dei cittadini, ma anche la tenuta dei principi democratici e dello Stato di diritto)[46].
In particolare, infatti, lo stesso *AI Act*, già dai Considerando 4 e 5, sottolinea le vaste potenzialità applicative dei sistemi *AI-based* nei più disparati settori del vivere umano, comportando – a seconda degli specifici utilizzi – sia grandi utilità che rischi potenziali per interessi di rilevanza pubblica o per la garanzia di diritti fondamentali della società. In tale ottica, quindi, e «in considerazione dell'impatto significativo che l'IA può avere sulla società e della necessità di creare maggiore fiducia, è essenziale che l'IA e il suo quadro normativo siano sviluppati conformemente ai valori dell'Unione sanciti dall'articolo 2 del trattato sull'Unione europea (TUE), ai diritti e alle libertà fondamentali sanciti dai trattati e, conformemente all'articolo 6 TUE, alla Carta. Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani»[47]. E tale intento viene confermato anche nel primo articolo dello stesso Regolamento[48], in cui, sommariamente, viene indicato il contenuto della normativa e le modalità attraverso il quale perseguire gli obiettivi suindicati, in particolare, dettando regole armonizzate per l'immissione sul mercato e l'uso di sistemi di AI, divieti di talune pratiche e specifici requisiti di utilizzo per sistemi ad alto rischio, nonché regole di trasparenza, di monitoraggio e di armonizzazione.
Chiariti gli obiettivi perseguiti dalla normativa eurounitaria, il testo del Regolamento prosegue, illustrando, nel suo articolo 2, l'ambito oggettivo e soggettivo di applicazione delle disposizioni ivi contenute. L'*AI Act* tende, innanzitutto, a adottare un ambito di applicazione assai vasto, al fine di assicurare che la disciplina dettata si riferisca all'intero ciclo vitale dei

[44] C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw – Rivista di Biodiritto*, 3, 2021, 415 – 437.
[45] M. Pappalardo, *L'ambito di applicazione dell'AI Act*, in AIRIA (a cura di), *Navigare l'European AI Act*, Milano, 2024, 29 – 30.
[46] Così si legge espressamente nel testo del Considerando 1 del Regolamento: «(1) Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, 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 («Carta»), 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».
[47] Cfr. Considerando 6 del Regolamento.
[48] Cfr. art. 1 del Regolamento: «1. Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e 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, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione. 2. Il presente regolamento stabilisce: a) regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione; b) divieti di talune pratiche di IA; c) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi; d) regole di trasparenza armonizzate per determinati sistemi di IA; e) regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali; f) regole in materia di monitoraggio del mercato, vigilanza del mercato, governance ed esecuzione; g) misure a sostegno dell'innovazione, con particolare attenzione alle PMI, comprese le start-up».

sistemi di intelligenza artificiale disciplinati.
Nel dettaglio, dal punto di vista soggettivo, il Regolamento si applica a tutti gli operatori coinvolti nella filiera di produzione, sviluppo, distribuzione ed uso dei sistemi *AI-based* e, quindi, a tutti gli operatori che a diverso titolo rivestono un ruolo attivo «nella catena del valore dei sistemi di IA»[49]*:* ai fornitori, ai *deployers*[50], ai rappresentanti autorizzati[51], agli importatori e ai distributori.
Dal punto di vista oggettivo, invece, il Regolamento trova applicazione nei confronti di tutti i sistemi di *AI*, così come definiti nell'articolo 3: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[52]. L'estrema ampiezza della suddetta definizione non è casuale, il legislatore unionale ha infatti consapevolmente deciso di utilizzare un riferimento così generico per una tecnologia come l'intelligenza artificiale, in costante evoluzione e cambiamento, per non rischiare di dettare una definizione eccessivamente cristallizzata ed incapace di adattarsi alle future scoperte e applicazioni[53].
Tutto ciò premesso, per realizzare gli obiettivi prefissati, il Regolamento presenta un quadro normativo solido ma flessibile che, da un lato, mira ad essere completo e *future proof*[54] e, dall'altro lato, introduce un sistema regolatorio proporzionato ed incentrato su un approccio basato sul rischio[55].
Il c.d. *risk-based approach*[56] è l'elemento maggiormente innovativo della regolamentazione europea e può essere definito come uno strumento di politica del diritto volto a contemperare l'esigenza di mitigare i rischi connessi ad un uso non regolamentato di sistemi *AI-based*, con quella di non frenare lo sviluppo economico ed industriale legato all'uso di queste tecniche[57].
La Commissione europea già nel Libro Bianco del 2020 esponeva svariate perplessità verso l'adozione di una regolamentazione indistinta per tutti i sistemi di AI, dal momento che – nella realtà fattuale – non tutte le applicazioni dell'intelligenza artificiale presentano rischi equivalenti; pertanto, una disciplina totalmente uniforme avrebbe condotto ad effetti

[49] M. Pappalardo, op. cit.
[50] Si evidenzi che, in sede di traduzione, si è deciso di mantenere il riferimento al termine inglese *deployers*, anziché adottare la traduzione letterale di «utilizzatore professionale», ciò al fine di non generare possibili errori di interpretazione ed applicazione della normativa.
[51] Il rappresentante autorizzato, ai sensi dell'art. 3 del Regolamento, è «una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento».
[52] Cfr. art. 3 n. 1 del Regolamento.
[53] E. Raffiotta, *I profili definitori e i principi dell'AI Act*, in AIRIA (a cura di), *Navigare l'European AI Act*, Milano, 2024, 43 – 57.
[54] Cfr. Considerando 26 del Regolamento: «Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di IA inaccettabili, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA».
[55] A. Ojanen, *Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, pubblicato il: 30 giugno 2025.
[56] Si tratta di un modello ampiamente utilizzato nei sistemi giuridici occidentali. In particolare, l'Unione europea, nel corso del XXI secolo, se ne è servita per regolamentare settori cruciali quali la tutela dell'ambiente, la salute e, ora, le tecnologie digitali.
[57] G. De Gregorio, P. Dunn, O. Pollicino, *Approccio basato sul rischio: come è applicato nelle normative UE sul digitale* in *Agenda Digitale*, pubblicato il: 15 settembre 2022.

distorsivi per lo sviluppo tecnologico e, soprattutto, risultati insufficienti a regolare le applicazioni più compromettenti per i diritti fondamentali.
L'*AI Act* ha accolto positivamente tali preoccupazioni, e ha posto quale architrave della normativa un approccio basato sul rischio, ovvero un approccio regolatorio fondato sulla proporzionalità del rischio: l'aspetto centrale di questo meccanismo è dato proprio dalla previsione di diverse fasce di intensità di rischio riferite ai sistemi di *AI* in uso, a cui vengono ricollegate regimi regolatori differenziati[58]. Tale impostazione, richiamata fin dai Considerando 26 e 27 e poi compiutamente articolata negli articoli da 5 a 52[59], è definibile quale vera e propria piramide del rischio articolata in vari livelli a seconda dell'intensità dell'impatto negativo che i sistemi intelligenti generano su diritti e valori fondamentali, e a cui vengono ricollegate conseguenze giuridiche differenziate[60].

Sviluppato secondo una prospettiva c.d. *top-down*, il Regolamento nel dettaglio prevede quattro diverse fasce di rischio in cui vengono collocate le principali applicazioni di *AI*.
Al vertice di questa piramide, si collocano i sistemi a rischio inaccettabile, ovvero le pratiche ritenute incompatibili con l'impianto valoriale europeo, e a cui è interamente dedicato il Capo II, articolo 5 del Regolamento, rubricato proprio *prohibited artificial intelligence practices*. Come verrà esposto meglio *infra*, in tale articolo il Regolamento qualifica alcune pratiche di AI come intrinsecamente incompatibili con i valori dell'UE, traducendosi in violazioni palesi e non mitigabili dei diritti fondamentali. Seppur con alcune eccezioni, tali pratiche sono soggette ad un divieto assoluto di implementazione, commercializzazione ed utilizzo nel mercato unico europeo.
Tutto ciò che non rientra in questo primo livello – e che quindi non è espressamente vietato – è soggetto, d'altra parte, a obblighi di conformità più o meno elevati, a seconda del rischio che tali sistemi possono comportare per la tutela dei diritti e dei valori eurounitari. La logica portante è che «più è alto il rischio e maggiori sono gli oneri e le responsabilità degli autori e utilizzatori delle applicazioni intelligenti»[61].
Pertanto, al livello immediatamente inferiore – ovvero al Capo III della normativa – si trovano i sistemi ad alto rischio, classificati a partire dall'articolo 6 e qualificati come sistemi che possono incidere negativamente su diritti fondamentali e che, pertanto, sono soggetti ad obblighi e requisiti assai stringenti[62]. In questo gradino piramidale vengono ricompresi (i) i sistemi intelligenti che costituiscono componenti di sicurezza di un prodotto, o sistemi che costituiscono essi stessi prodotti, disciplinati dalla normativa Europea riportata nell'Allegato I; (ii) i sistemi intelligenti c.d. «indipendenti» tassativamente[63] elencati nell'Allegato III del

---

[58] V. D'Antino, *L'approccio basato sul rischio dell'AI Act: un nuovo paradigma di regolazione dell'intelligenza artificiale*, in *Federalismi.it*, 18, 2025, 19.
[59] Cfr. Considerando 26 del Regolamento, ai sensi del quale: «Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di IA inaccettabili, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA»
[60] M. Almada, N. Petit, *The EU Ai Act: A Medley of Product Safety and Fundamental Rights*?, Firenze, 2023.
[61] E. Raffiotta, op. cit.
[62] Cfr. Considerando 46 del Regolamento: «È opportuno che i sistemi di IA ad alto rischio siano immessi sul mercato dell'Unione, messi in servizio o utilizzati solo se soddisfano determinati requisiti obbligatori. Tali requisiti dovrebbero garantire che i sistemi di IA ad alto rischio disponibili nell'Unione o i cui output sono altrimenti utilizzati nell'Unione non presentino rischi inaccettabili per interessi pubblici importanti dell'Unione, come riconosciuti e tutelati dal diritto dell'Unione».
[63] Parte della dottrina critica la scelta del legislatore unionale di indicare tassativamente i sistemi ad alto rischio nell'Allegato III, sottolineando il rischio che questa strategia così prudenziale possa non stare al passo con l'attuale evoluzione tecnologica così rapida e dirompente. Tra questi: A.A. Gikay, P. L. Lau, C. Sengul, A. Miron,

Regolamento ed impiegati in settori sociali particolarmente sensibili, con effetti potenzialmente incisivi sulla vita dei cittadini in termini di salute, sicurezza, e tutela dei diritti fondamentali[64].

Per tali applicazioni, l'*AI Act* prevede l'imposizione di requisiti rigorosi, in ogni fase del ciclo di vita del sistema, come: l'adozione di misure di sicurezza informatica ed accuratezza del sistema, la previsione di obblighi di trasparenza verso gli utenti, l'inclusione di meccanismi di supervisione umana. Il rispetto di questi ed altri requisiti viene assicurato attraverso la predisposizione di valutazioni e test di conformità.

Al terzo livello della piramide del rischio, vengono collocate quelle applicazioni che, pur non comportando rischi elevati in termini di sicurezza e tutela dei diritti fondamentali, potrebbero comunque influire negativamente sull'utente finale e per i quali il Regolamento prevede – all'articolo 50 – minimi obblighi di trasparenza. Si tratta dei sistemi a rischio – per così dire – limitato, riferendosi ad esempio a sistemi che interagiscono con gli esseri umani (come *chatbot*) o sistemi di *AI* generativa, che generano o manipolano immagini e contenuti. Per tali applicazioni sono previsti minimi obblighi di trasparenza, a tutela dell'utilizzatore finale, che deve essere sempre a conoscenza di star interagendo con strumenti automatizzati[65].

Da ultimo, al livello più basso della piramide, si trovano i sistemi a rischio nullo o minimo per i quali non sono previsti obblighi specifici, anche se il Regolamento – nel suo articolo 95 – prevede la possibilità per i fornitori e *deployer* si aderire a codici di condotta volontari[66]. Tali sistemi (quali, ad esempio, videogiochi o filtri antispam) possono quindi essere introdotti e distribuiti nel mercato unico europeo senza essere soggetti a obblighi particolari, ferma restando l'applicazione delle norme europee generali su protezione dei dati, responsabilità e concorrenza.

Tale breve ricostruzione della struttura e degli obiettivi perseguiti dall'*Artificial Intelligence Act* permette di mettere in luce fin da ora come il legislatore unionale abbia scelto di adottare un modello regolatorio complesso, strutturato secondo un approccio basato sul rischio che – con la sua architettura multilivello – consente di intervenire in modo oculato in base alla pericolosità dei sistemi intelligenti utilizzati, predisponendo obblighi proporzionalmente crescenti all'impatto di tali tecnologie sulla vita delle persone.

La *ratio* è chiara: ricercare un punto di equilibrio che consenta, da un lato, di agevolare lo sviluppo tecnologico senza imporre ostacoli che possano frenare la competitività tecnologica dell'UE, senza tuttavia, dall'altro lato, mettere in ombra il necessario consolidamento di un impianto normativo a servizio e a tutela dei diritti e dei valori europei.

Al fine di verificare se l'assetto predisposto dal legislatore europeo sia davvero efficace, sia sul fronte dell'innovazione tecnologica sia su quello della tutela dei diritti, è imprescindibile sviluppare un *focus* d'analisi sul livello più severo di risposta normativa adottato dal Regolamento: ovvero l'articolo 5, dedicato ai sistemi intelligenti vietati, in quanto intrinsecamente incompatibili con i valori e i diritti dell'Unione europea.

L'esame di tale disposizione, della sua struttura, della sua finalità ed efficacia, è un passaggio

---

B. Malin, *High-Risk Artificial Intelligence Systems under the European Union's Artificial Intelligence Act: Systemic Flaws and Practical Challenges*, dicembre 2023.

[64] M. Colonna, *I sistemi ad alto rischio e i General Purpose AI Models*, in AIRIA (a cura di), *Navigare l'European AI Act*, Milano, 2024, 71 - 80.

[65] T. Mahler, *Between Risk Management and Proportionality: The Risk-based Approach in the EU's Artificial Intelligence Act Proposal*, in *Nordic Yearbook of Law and Informatics*, 2021, 258 ss.

[66] Cfr. art. 95.1 del Regolamento: «L'ufficio per l'IA e gli Stati membri incoraggiano e agevolano l'elaborazione di codici di condotta, compresi i relativi meccanismi di governance, intesi a promuovere l'applicazione volontaria ai sistemi di IA, diversi dai sistemi di IA ad alto rischio, di alcuni o di tutti i requisiti di cui al capo III, sezione 2, tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore che consentono l'applicazione di tali requisiti».

essenziale al fine di valutare l'effettiva capacità dell'*AI Act* nel suo complesso di proteggere il nucleo essenziale dei diritti fondamentali unionali.

4. Le c.d. «pratiche vietate» e la tutela dei diritti fondamentali ai sensi dell'articolo 5 del Regolamento. Al Capo II del Regolamento, denominato *prohibited artificial intelligence practices*, si colloca l'articolo 5, dedicato proprio all'individuazione e regolamentazione di quei sistemi di intelligenza artificiale che comportano un livello di rischio definito «inaccettabile», traducendosi, a determinate condizioni, in evidenti e non aggirabili violazioni di diritti e valori fondamentali.

Innanzitutto, il percorso che ha condotto all'approvazione di questo articolo è stato travagliato ed articolato: già nella proposta presentata dalla Commissione europea nel 2021 era previsto un insieme, seppur limitato, di sistemi e pratiche vietate; tuttavia, il Parlamento europeo ha più volte avanzato la richiesta di un ampliamento di tale elenco e di un inasprimento dei divieti e delle sanzioni ad esso collegati. Seguirono quindi svariati dibattiti e scontri tra le istituzioni europee – in particolare, nel dialogo fra Consiglio e Parlamento[67] – su quale dovesse essere il contenuto di tale disposizione. L'accordo finale è pertanto il frutto di un compromesso, che riflette la tensione costante tra le esigenze di progresso tecnologico e quelle di tutela dei diritti fondamentali.

Oggi, in definitiva, l'articolo 5 elenca una serie di sistemi e tecniche di *AI* di per sé considerate contrarie al rispetto della dignità umana, della libertà e dell'eguaglianza: e, per tali ragioni, la *ratio* della disposizione deve essere individuata proprio nel tentativo di fissare una soglia invalicabile oltre la quale il legislatore unionale ha deciso di non andare, per impedire che l'innovazione tecnologica possa tradursi in un regresso valoriale e costituzionale[68].

Ciò premesso, l'articolo 5 individua svariate categorie di sistemi *AI-based* e, se per alcuni di questi sistemi è previsto un assoluto divieto di implementazione (art. 5 lett. *a), b)* ed *e),* per altri sono previsti divieti solo in linea di principio e accompagnati da alcune eccezioni, e/o sottoposti al rilascio di un'autorizzazione da parte di un'autorità amministrativa o giudiziaria (lett. *d), f), g)* e *h*).

In generale, comunque, tutte le tecniche ed i sistemi menzionati da tale disposizione, sollevano forti perplessità in tema di compatibilità con la tutela dei diritti e delle libertà fondamentali e, per questa ragione, viene previsto un regime di divieti e condizioni assai rigoroso.

Nel dettaglio, ai sensi della lett. *a)*, sono innanzitutto vietati l'immissione sul mercato e l'utilizzo di sistemi intelligenti che utilizzano tecniche manipolative o ingannevoli, volte a compromettere il comportamento del singolo individuo, influenzando la sua capacità decisionale in modo da indurlo a prendere una decisione che, altrimenti, non avrebbe preso. Parimenti vietato, è l'uso di tecniche che sfruttano la vulnerabilità di un soggetto (dovuta ad età, disabilità o situazione sociale ed economica), al fine di distorcerne il comportamento, arrecandogli un significativo danno o pregiudizio (lett. *b*).

La natura di tali tecniche viene illustrata più esaustivamente nel Considerando 29 del Regolamento, ai sensi del quale «tali sistemi di AI impiegano componenti subliminali quali stimoli audio, grafici e video che le persone non sono in grado di percepire poiché tali stimoli

[67] In particolare, durante i triloghi (2023 – 2024), il confronto tra il Parlamento europeo ed in Consiglio si è concentrato principalmente sull'ambito operativo del divieto di identificazione biometrica nello spazio pubblico: il Parlamento chiedeva infatti la previsione di un divieto quasi totale, mentre diversi Stati membri ed il Consiglio insistevano per ammettere maggiori eccezioni, principalmente per finalità di contrasto e sicurezza pubblica. Il punto d'incontro definitivo, raggiunto nel dicembre 2023, ha mantenuto il divieto come regola generale, seppur con l'introduzione di deroghe circoscritte e sottoposte a condizioni rigorose.

[68] G. Scafati, *Le pratiche vietate*, in *AIRIA* (a cura di), *Navigare l'European AI Act*, Milano, 2024, 59 – 70.

vanno aldilà della percezione umana o altre tecniche manipolatrici o ingannevoli che sovvertono l'autonomia, il processo decisionale o la libera scelta di una persona senza che sia consapevole di tali tecniche o, se ne è consapevole, senza che sia in grado di controllarle o resistervi o possa evitare l'inganno»[69].

Vietato è anche l'utilizzo di sistemi di *social scoring*[70], ovvero sistemi volti a classificare i singoli individui sulla base di un'analisi del proprio comportamento sociale o di caratteristiche personali, determinando un trattamento pregiudizievole e/o sproporzionato rispetto al comportamento tenuto dal soggetto (lett. *c*). Anche in questo caso, il riferimento al Considerando 31 del Regolamento può essere chiarificatore. Viene infatti precisato che l'impiego di tali tecniche di attribuzione di un punteggio sociale, possono finire per «ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia» In particolare, la disposizione normativa stabilisce che il punteggio sociale ottenuto da tali sistemi *AI-based* può arrivare a determinare un trattamento pregiudizievole per persone fisiche o interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, nonché un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del comportamento sociale degli stessi soggetti coinvolti[71]. Si tratta, in definitiva, di sistemi che possono facilmente tradursi in una lesione di valori fondamentali, quali il principio di non discriminazione, incidendo in modo penalizzante su gruppi già minoritari o marginalizzati: spesso, infatti, software di previsione di reati o di calcolo del recidivismo si basano su informazioni che arrivano a criminalizzare le stesse condizioni di povertà di soggetti già in difficoltà o finiscono per tradursi in pratiche razziste nei confronti di comunità minoritarie[72]. Inoltre, tali programmi di *social scoring* determinano spesso un'impropria commistione fra comportamenti privati e posizioni pubbliche dei cittadini, determinando l'attivazione di sistemi di sorveglianza di massa propri di ordinamenti illiberali o autoritari che finiscono per ledere la stessa dignità umana.

Assolutamente vietato anche l'utilizzo di sistemi intelligenti che, attraverso tecniche di *scrapting*[73], ampliano o creano *ex novo* banche dati di riconoscimento facciale (lett. e); tale divieto, rafforzato dal riferimento al Considerando 43 del Regolamento, è giustificato dal fatto che l'utilizzo di tali tecniche può finire per accrescere un senso di sorveglianza di massa, comportando palesi violazioni a diritti fondamentali quali il diritto alla *privacy* e alla vita

[69] Cfr. Considerando 29 del Regolamento.

[70] Per *social scoring* si intende l'uso di sistemi di intelligenza artificiale per attribuire punteggi o classificazioni alle persone fisiche sulla base del loro comportamento sociale, delle loro interazioni o del riferimento a dati personali raccolti in diversi contesti, allo scopo di valutarne l'affidabilità o la conformità a standard definiti. Tali pratiche possono naturalmente tradursi in forme di discriminazione violazione di dignità umana ed eguaglianza, e sono tipiche di modelli di sorveglianza algoritmica.

[71] Cfr. Considerando 31 del Regolamento: «Il punteggio sociale ottenuto da tali sistemi di IA può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale. I sistemi di IA che comportano tali pratiche inaccettabili di punteggio aventi risultati pregiudizievoli o sfavorevoli dovrebbero pertanto essere vietati».

[72] Y. Citino, *Cittadinanza «a punti» e social scoring: le pratiche scorrette dell'era dell'intelligenza artificiale*, in *Diritti Comparati. Comparare i diritti fondamentali in Europa*, pubblicato il: 22 giugno 2022 e A. Diamante, *Punteggio sociale: distopia o realtà? L'Ue traccia i confini*, in *Agenda Digitale*, pubblicato il: 11 settembre 2025.

[73] Lo *scrapting* è una tecnica informatica che consente di estrarre automaticamente grandi quantità di dati da siti web o altre fonti online, spesso mediante l'uso di software automatizzati. Se applicato senza limitazioni o regole, lo *scrapting* può raccogliere dati personali e sensibili su larga scala senza il consenso espresso degli interessati, creando significativi rischi per la privacy e la protezione dei dati personali così raccolti. Anche al Considerando 43 del Regolamento si trova un riferimento alla necessità di predisporre un divieto mirato all'uso di tali sistemi.

privata[74].
Oltre a queste pratiche totalmente vietate, vi sono anche tecniche e sistemi di *AI* per cui sono previsti divieti accompagnati da deroghe o eccezioni. Tra questi, ad esempio, ai sensi della lett. d), è vietato l'uso di sistemi intelligenti che effettuano valutazioni del rischio di recidivismo o di commissione di reati da parte dei singoli, in base all'analisi di caratteristiche personali; tale divieto, tuttavia, non si applica «ai sistemi di AI utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»[75]. Il Considerando 42 del Regolamento sul punto rimarca un principio fondamentale: le persone dovrebbero infatti essere giudicate in base al loro effettivo comportamento e non, invece, sulla base di un comportamento previsto da sistemi di intelligenza artificiale e basato unicamente sul riferimento a tecniche di profilazione di dati personali e sensibili, senza che vi sia peraltro un concreto riscontro fondato su un «ragionevole sospetto che la persona sia coinvolta in un'attività criminosa sulla base di fatti oggettivi verificabili e senza una valutazione umana a riguardo»[76].

Allo stesso modo, è vietato l'uso di sistemi di *AI* volti ad inferire le emozioni di un soggetto sul luogo di lavoro o di istruzione, a meno che l'uso di tale sistema non sia collegato a finalità mediche o di sicurezza pubblica (lett. *f)*. Aldilà della dubbia base scientifica di tali sistemi di inferenza delle emozioni, il Considerando 44 del Regolamento, sottolinea inoltre come l'uso di tali tecniche sui luoghi di lavoro e di istruzione debba essere vietato in virtù dello squilibrio di potere che interessa tali contesti, a discapito – chiaramente – del soggetto profilato; tale aspetto, combinato con la natura estremamente invasiva di tali sistemi, determina inevitabilmente «un trattamento pregiudizievole o sfavorevole per i singoli o per interi gruppi»[77].
Alla lett. *g)* è previsto poi un divieto di utilizzo di tecniche di categorizzazione biometrica[78] che classificano i soggetti in base al riferimento a dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale[79]. Anche qui, sono previste eccezioni: tale divieto non si applica infatti nel caso di filtraggio di informazioni biometriche acquisite legalmente o per finalità pubbliche di *law enforcement*.
Infine, ampio spazio è dedicato alla regolamentazione dell'utilizzo delle tecniche di identificazione biometrica[80] in tempo reale in luoghi accessibili al pubblico (lett. *h*). Viene

[74] Cfr. Considerando 43 del Regolamento: «L'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso dovrebbero essere vietati, in quanto tale pratica accresce il senso di sorveglianza di massa e può portare a gravi violazioni dei diritti fondamentali, compreso il diritto alla vita privata».
[75] Cfr. art. 6.1, *lett. d)* del Regolamento.
[76] Cfr. Considerando 42 del Regolamento.
[77] Cfr. Considerando 44 del Regolamento.
[78] Per categorizzazione biometrica si intende quel processo volto a stabilire se i dati biometrici di un individuo appartengono ad un gruppo sociale con alcune caratteristiche predefinite. Già il Considerando 30 del Regolamento insiste sulla necessità di predisporre severi divieti di utilizzo di tali sistemi «per trarre inferenze in merito alle opinioni politiche, all'appartenenza sindacale, alle convinzioni religiose o filosofiche, alla razza, alla vita sessuale o all'orientamento sessuale di una persona».
[79] Cfr. articolo 6.1, lett. *g)* del Regolamento.
[80] Il Considerando 17 del Regolamento definisce un sistema di identificazione biometrica remota come un sistema di AI destinato all'identificazione di persone fisiche senza un loro coinvolgimento attivo e mediante il confronto dei dati biometrici di una persona con quelli contenuti in una banca dati di riferimento. Si tratta, più nel dettaglio, di tecniche che permettono di distinguere un soggetto in forza di caratteristiche fisiche uniche, come le impronte digitali, il DNA, la forma dell'iride, la struttura vascolare della retina, la struttura venosa della

previsto un divieto generale di utilizzo di tali tecniche di *AI*, in quanto l'uso di tali sistemi è particolarmente invasivo dei diritti e delle libertà delle persone interessate, in quanto lo stesso potrebbe avere ripercussioni concrete sulla vita privata di un'ampia fetta della popolazione, facendola sentire costantemente sotto sorveglianza e scoraggiando indirettamente l'esercizio della libertà di riunione o di altri diritti fondamentali[81]. Tali tecniche, infatti, hanno spesso una struttura discriminatoria e razziale intrinseca. E la formazione degli agenti su rischi e limiti di questi istituti, seppur obbligatoria e necessaria, non è sufficiente a contrastare i pregiudizi algoritmici presenti in tali sistemi, spesso causa di errori discriminatori che determinano un devastante impatto psicologico nella vita dei soggetti colpiti[82].

La previsione di tali divieti, tuttavia, è accompagnata da una serie di eccezioni. Queste ultime consentono infatti l'impiego di sistemi di identificazione biometrica di questo tipo, esclusivamente in presenza di circostanze eccezionali, ovvero (i) per la ricerca mirata di vittime di reati o di persone scomparse; (ii) per la prevenzione di specifiche minacce per l'incolumità pubblica, come minacce terroristiche; (iii) per l'identificazione di persone sospettate di aver commesso reati specificamente elencati e circoscritti[83].

In tali casi eccezionali, comunque, l'uso di tecniche di questo tipo è subordinato al rilascio di un'autorizzazione preventiva da parte d un'autorità giudiziaria o amministrativa indipendente, la cui decisione è vincolante[84].

Tutti i divieti e le disposizioni previste dall'articolo 5 e analizzati, sono entrati in vigore a partire dal 2 febbraio 2025[85]; mentre i Capi del Regolamento relativi alla *governance* e al sistema sanzionatorio, sono entrati in vigore a partire dal 2 agosto 2025[86].

Tutto ciò premesso, il legislatore unionale ritiene quindi che l'impatto negativo che tutte queste tecniche e tecnologie hanno sui diritti fondamentali sia talmente elevato da giustificare un divieto (quasi) assoluto di implementazione ed utilizzo, che si traduce in una limitazione o in una totale compressione dello sviluppo di tali tecnologie nel mercato unico dell'Unione

---

mano, oppure attraverso i tratti differenziali del suo comportamento, come il modo di camminare o il timbro della vita. Così in G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, 11.

[81] Cfr. Considerando 32 del Regolamento: «L'uso di sistemi di IA di identificazione biometrica remota «in tempo reale» delle persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto è particolarmente invasivo dei diritti e delle libertà delle persone interessate, nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali. Le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori».

[82] A. Spaziani, *Il modello europeo di gestione della crisi alla luce del Digital Services Act e dell'AI Act*, in *DPCE Online*, 2, 2025, 624 – 627.

[83] Il Considerando 33 del Regolamento approfondisce le ragioni della previsione di tali eccezioni, sottolineando come, in situazioni di interesse pubblico e tutela della pubblica sicurezza, l'uso di tali tecnologie potrebbe avere un ruolo determinante.

[84] Tuttavia, in situazioni di particolare urgenza è possibile iniziare ad utilizzare i sistemi in questione anche senza autorizzazione, a condizione che la stessa venga richiesta entro le successive 24 ore. E, se tale autorizzazione venisse respinta, l'uso del sistema sarebbe immediatamente interrotto e i dati raccolti fino a quel momento verranno cancellati.

[85] Cfr. art. 113 del Regolamento: «Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Si applica a decorrere dal 2 agosto 2026. Tuttavia: a) I capi I e II si applicano a decorrere dal 2 febbraio 2025; b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025 (…)».

[86] In particolare, l'art. 99 del Regolamento, espone le sanzioni applicabili in caso di mancato rispetto delle previsioni contenute nell'articolo 5: «3. La non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 35 000 000 EUR o, se l'autore del reato è un'impresa, fino al 7 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore».

europea.
Pertanto, in definitiva, ciò che guida l'articolo 5 (e, più in generale, l'intero Regolamento) è un principio finalizzato a realizzare una tutela anticipata dei diritti fondamentali, che comporta talvolta un'esclusione preventiva di determinate tecnologie o pratiche, ritenute ontologicamente incompatibili con l'ordinamento comunitario e i valori *ivi* riconosciuti[87].
Tuttavia, nondimeno, tale scelta ed impostazione normativa solleva questioni complesse: non sempre, infatti, il confine tra ciò che è lecito e ciò che è proibito risulta immediatamente chiaro e, la presenza di eccezioni condizionate, l'uso di concetti talvolta eccessivamente generici, nonché la discrezionalità rimessa ai singoli Stati membri nell'adattarsi a tali previsioni, sollevano seri dubbi circa l'effettività e l'uniformità della disciplina contenuta nell'articolo 5 del Regolamento[88].

5. Le criticità normative e applicative dell'articolo 5 del Regolamento e il contributo offerto dalle recenti Linee guida della Commissione europea. La ricostruzione operata nel precedente paragrafo permette di apprezzare fin da subito la centralità dell'articolo 5 nell'impianto valoriale delineato dall'*AI Act*, che ha l'ambizione di tracciare un percorso di tutela effettiva dei diritti fondamentali europei, potenzialmente compromessi dall'uso di determinate pratiche di *AI*.
Tuttavia, la concreta efficacia di tale previsione normativa risulta condizionata da una serie di criticità (normative e applicative) che rischiano di inficiarne l'effettiva utilità. Delle varie spinosità evidenziate da dottrina e giurisprudenza nell'analisi dell'articolo 5 del Regolamento, di seguito ne verranno analizzate due delle principali[89].
Una di suddette criticità – peraltro di immediata percezione – riguarda la struttura lessicale rintracciabile in alcuni punti dell'articolo 5: infatti, già da una rapida lettura del testo della disposizione normativa, è facile accorgersi della formulazione talvolta eccessivamente generica di alcuni dei suoi riferimenti.
In particolare, le condizioni fissate per delimitare l'ambito operativo dei divieti previsti, risultano caratterizzate da una certa indeterminatezza, che finisce per attribuire forte discrezionalità applicativa ai singoli Stati e alle autorità pubbliche. Tale indeterminatezza determina talvolta forti incertezze e difformità nell'applicazione della disciplina nel territorio unionale, arrivando fino a causare l'apertura di numerosi contenziosi[90].
Qualche esempio concreto può essere chiarificatore: basti considerare la lett. a) della disposizione, che parla espressamente di «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, inducendole a prendere una decisione che altrimenti non avrebbero preso». Si tratta chiaramente di espressioni prive di un ancoraggio definitorio preciso e, pertanto, suscettibili di svariate interpretazioni e riferimenti imprecisi.
E allo stesso modo, la lett. *b*) della disposizione fa riferimento a condizioni di «vulnerabilità

[87] A. Lamberti, *Costituzionalismo digitale, poteri delle piattaforme, intelligenza artificiale e democrazia*, in *Consulta Online*, 2, 2025, 1102 – 1110.
[88] R. Razzante, *AI e tutela dei diritti fondamentali*, in *Dirittifondamentali.it*, 1, 2024, 133 – 140.
[89] U. Cemalovic, *Prohibited artificial intelligence practices according to Article 5 of the European Union's regulation on AI – between the 'too late' and the 'not enough'*, in *International Journal of Law and Information Technology*, 32, 2024. Tale contributo osserva che, nonostante l'importanza normativa, l'*AI Act* e il suo articolo 5 «arriva tardi e non va abbastanza lontano». L'autore sostiene, in particolare, che le proibizioni previste rischiano di essere insufficienti a garantire un'intelligenza artificiale antropocentrica ed affidabile.
[90] H. Zhong, E. O'Neill, J. A. Hoffman, *Regulating AI: Applying insights from behavioural economics and psychology to the application of article 5 of the EU AI ACT*, in *Cornell University*, pubblicato a dicembre 2023.

di una persona fisica o di un gruppo di persone, dovuta all'età, alla disabilità o ad una specifica situazione sociale o economica» senza individuare criteri oggettivi precisi e funzionali ad accertare tali condizioni di vulnerabilità.
Una vaghezza definitoria di questo tipo rischia senz'altro di rendere incerta una precisa individuazione delle condotte vietate, finendo per delegare un eccessivo potere discrezionale alle autorità nazionali di vigilanza, con effetti potenzialmente divergenti tra i singoli Stati membri.
In secondo luogo, altro aspetto di particolare rilevanza critica che emerge dallo studio dell'articolo 5 del Regolamento, riguarda il sistema di eccezioni previsto dalla normativa, che consente – a determinate condizioni – l'impiego di alcune delle tecniche e dei sistemi di AI di regola vietati; ampio spazio viene in particolare dedicato all'elencazione delle condizioni che consentono l'impiego dei sistemi di identificazione biometrica in tempo reale in spazi pubblici e da parte di autorità competenti (lett. *h*) dell'articolo 5)[91].

Tale sistema di eccezioni, indubbiamente, rappresenta uno dei punti più discussi del Regolamento, prevedendo deroghe significative rispetto ai divieti originariamente previsti[92].
Anche in questo caso, l'esame del testo della normativa può essere d'aiuto nell'evidenziare le principali perplessità di dottrina e giurisprudenza in relazione al sistema delle eccezioni delineato. Volgendo l'attenzione, in particolare, ai sistemi di identificazione biometrica remota in tempo reale, l'articolo 5 – pur prevedendo un divieto generalizzato di utilizzo di tali sistemi – ne consente tuttavia l'impiego in determinati contesti, qualora l'uso di tali sistemi sia da considerarsi come strettamente funzionale al raggiungimento di determinate finalità[93].
La *ratio* di tali deroghe è immediata e lodevole: consentire l'impiego di strumenti che (seppur invasivi) possono, in determinati contesti eccezionali, rivelarsi necessari ad affrontare situazioni di pericolo per la sicurezza pubblica.
Sebbene, come detto, la *ratio* di tali previsioni sia condivisibile, nella pratica, l'applicazione effettiva di queste deroghe risulta problematica[94].
E questo per diverse ragioni.
Innanzitutto – e questo ci consente di ricollegarci alla prima problematica già esposta all'inizio del presente paragrafo – un aspetto problematico di tali previsioni è legato alla formulazione lessicale di alcune di queste eccezioni, talvolta non sufficientemente definita. Nel dettaglio, l'utilizzo di espressioni come «minacce imminenti», «reati gravi», «finalità di pubblica sicurezza» per giustificare l'impiego di sistemi altrimenti vietati, risulta spesso eccessivamente generalizzato, comportando, quindi, evidenti difficoltà e difformità applicative all'interno dei singoli Stati.
Senza considerare, in secondo luogo, che condizioni derogatorie così aspecifiche rischiano di

---

[91] La previsione di eccezioni al divieto di utilizzo di sistemi di identificazione biometrica remota in tempo reale trova fondamento nell'esigenza di bilanciamento tra la tutela dei diritti fondamentali della persona – in particolare privacy, protezione dei dati personali e tutela delle libertà individuali – e interessi pubblici ritenuti di primaria rilevanza, quali la salvaguardia dell'ordine e della sicurezza pubblica, la prevenzione di minacce imminenti, la ricerca di soggetti scomparsi o vittime di reato, nonché il contrasto a forme gravi di criminalità. In tale prospettiva, allora, l'eccezione prevista dall'art. 5, lett. h) si giustifica quale strumento di tutela di interessi collettivi di carattere superiore, pur dovendo essere interpretata restrittivamente o nel rispetto dei principi di necessità e di proporzionalità. Cfr. L. Floridi, *et. al.*, *AI4People – An Ethical Framework for a Good AI Society*, in *Minds and Machines*, vol. 28, 2018, 689-707.
[92] F. Mollo, *Il trattamento dei dati biometrici nell'AI Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in *Federalismi.it*, 28, 2024, 96 – 109.
[93] A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea IActa est?*, in *DPCE Online*, 2, 2024, 1113ss.
[94] F. Paolucci, *From Global Standards to Local Safeguards: The Ai Act, Bioemtrics, and Fundamental Rights*, in N. Menéndez Ganzàlez, G. Mobilio (a cura di), *Facial Recognition Technology*, Berlino, 2024.

essere interpretate in modo eccessivamente elastico, con una progressiva normalizzazione dell'impiego di strumenti estremamente intrusivi e il cui utilizzo è stato originariamente pensato per situazioni emergenziali ed eccezionali.
Il rischio concreto è infatti che il carattere straordinario del sistema di eccezioni finisca per tradursi in un uso ordinario delle tecnologie interessate, determinando una progressiva e continua erosione silenziosa delle garanzie costituzionali. Senza contare che, l'assenza di un sistema unionale centralizzato di controllo sull'effettiva applicabilità di tali deroghe, finisce per accrescere ulteriormente tali vulnerabilità.
In sostanza, l'impiego eccezionale di alcune delle tecnologie vietate, seppur soggetto a controlli, autorizzazioni e obblighi di necessità e proporzionalità, a causa dell'assenza di una definizione chiara dei criteri di utilizzo e dei maccanismi di supervisione, solleva dubbi sulla reale capacità di tale impianto derogatorio di prevenire abusi e violazioni dei diritti e valori unionali[95].

Tutto ciò premesso, come si è mossa e come si sta muovendo l'Unione europea di fronte a tali evidenti criticità?
Per rispondere alle incertezze interpretative e ai rischi applicativi elencati *supra*, di recente la Commissione europea ha adottato delle importanti «Linee guida relative alle pratiche di intelligenza artificiale vietate ai sensi dell'*AI Act*» (*Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689*) proprio con l'intento di fare un po' di chiarezza circa alcuni aspetti di non immediata comprensione dalla lettura del testo del Regolamento[96].
Sebbene non si tratti di disposizioni con efficacia vincolante per i singoli Stati, tali orientamenti offrono preziose informazioni sull'interpretazione dei divieti stabiliti dal Regolamento (e in particolare dall'articolo 5), accompagnate anche dal riferimento ad esempi pratici, proprio al fine di aiutare gli *stakeholders* – come autorità pubbliche e politiche, aziende e sviluppatori di sistemi di *AI* – a comprendere e rispettare le previsioni contenute nella normativa. Si tratta, in definitiva, di un supporto interpretativo di estrema rilevanza, che testimonia anche il costante impegno comunitario volto a promuovere una regolamentazione dell'intelligenza artificiale unitaria ed efficace[97].
Entrando nel dettaglio delle menzionate Linee guida, esse intervengono direttamente su

[95] In particolare, nell'opinione pubblica, l'inserimento di queste eccezioni ha suscitato forti critiche – soprattutto da associazioni per i diritti digitali. Questo perché secondo molti concedere possibilità seppur limitate alle forze dell'ordine di impiegare tecniche intelligenti di riconoscimento biometrico in tempo reale potrebbe tradursi nell'instaurazione di un sistema di sorveglianza di massa indiscriminato, con evidenti abusi e utilizzi eccessivi alle deroghe previste.
[96] Nella Comunicazione C(2025)884 final, la Commissione europea, annunciando l'approvazione delle menzionate linee guida, afferma che «Ai sensi dell'articolo 96, paragrafo 1, lettera b), della legge sull'intelligenza artificiale, la Commissione deve adottare linee guida sull'attuazione pratica delle pratiche vietate dall'articolo 5 della legge sull'intelligenza artificiale. Il progetto di linee guida allegato alla presente comunicazione mira ad aumentare la chiarezza giuridica e a fornire approfondimenti sull' interpretazione data dalla Commissione ai divieti di cui all'articolo 5 della legge sull'intelligenza artificiale, al fine di garantirne un'applicazione coerente, efficace e uniforme», rendendo da subito chiaro l'intento dei presenti orientamenti, ovvero cercare di assicurare un'applicazione quanto più coerente possibile del Regolamento tra i vari Stati membri. A tal proposito, è essenziale precisare che la crescente centralità di strumenti quali linee guida, comunicazioni e atti di *soft law* si spiega alla luce della peculiare dinamicità del settore dell'intelligenza artificiale, nel quale la rapidità dell'innovazione tecnologica rende frequentemente inadeguati i tempi e la rigidità della regolazione tradizionale. In tale prospettiva, tali strumenti svolgono una funzione essenziale di orientamento interpretativo e di armonizzazione delle prassi applicative.
[97] N. Martinello, *UE – Commissione Europrea – Giudelines on AI sysstem definition to facilitate the first AIAct's rules application: linee guida sulla definizione di sistemi di IA per implementare le norme dell'AI Act,* in *BioLaw Journal – Rivista di Biodiritto*, 2025.

alcune delle criticità evidenziate all'inizio del paragrafo corrente. In particolare, il paragrafo 3 della comunicazione della Commissione, volto ad illustrare il testo di questi orientamenti (C(2025) 5052 *final*), è dedicato proprio all'«Articolo 5, paragrafo 1, lettere *a)* e *b)* del regolamento sull'IA: manipolazione, inganno e sfruttamento dannosi». Si tratta di una sezione dedicata ad illustrare e chiarire gli obiettivi delle previsioni contenute alle lettere a) e b) dell'*AI Act* e anche a definire in modo maggiormente dettagliato le tecniche considerate vietate ai sensi di tali previsioni normative. Nel dettaglio, innanzitutto, viene ribadito che tali primi divieti mirano «a prevenire la manipolazione e lo sfruttamento attraverso sistemi di IA che riducono le persone a semplici strumenti per conseguire determinati fini, nonché a salvaguardare coloro che sono più vulnerabili ed esposti alla manipolazione e allo sfruttamento dannosi»[98].

Viene poi illustrato – in modo nettamente più approfondito rispetto all'articolo 5 del Regolamento – cosa concretamente si intende per tecniche subliminali, manipolative ed ingannevoli.

Nel dettaglio: innanzitutto, le «tecniche subliminali» vengono definite come tecnologie che agiscono senza che una persona ne sia consapevole, collocandosi «al di sotto o al di sopra della soglia della percezione conscia»[99]. Si tratta di sistemi che in definitiva aggirano le difese razionali dell'individuo e vanno ad incidere sui processi cognitivi in modo occulto, alterando le scelte ed i comportamenti dello stesso e compromettendone l'autonomia e la libertà di autodeterminazione.

Le «tecniche volutamente manipolative», invece, raggruppano tutti quei sistemi di *AI* progettati o idonei ad influenzare o controllare il comportamento di un soggetto, sfruttandone vulnerabilità o distorsioni cognitive, anche senza che vi sia una intenzione manifestamente manipolativa da parte del fornitore o dell'utilizzatore di detto sistema.

Infine, le «tecniche ingannevoli» sono tecnologie basate sulla presentazione di informazioni false o fuorvianti, con l'obiettivo di ingannare i singoli soggetti influenzandone il comportamento e compromettendone l'autonomia ed il processo di libera scelta consapevole[100].

Oltre a fornire definizioni maggiormente chiare ed approfondite di questi sistemi vietati, le Linee guida propongono anche una serie di esempi concreti di suddette tecniche, proprio con l'intento di chiarire e specificare ulteriormente quanto in astratto definito nell'*AI Act*.

Si tratta, quindi, dell'enunciazione di un apparato definitorio nettamente più corposo ed articolato rispetto a quello originariamente definito nel testo della regolamentazione, che prosegue poi chiarendo quali sono le altre condizioni che giustificano l'applicazione del divieto di utilizzo di tali tecniche ingannatorie o manipolative[101].

Anche relativamente al divieto di cui alla lettera b) paragrafo 1, dell'articolo 5, la Commissione europea espressamente riconosce che «il regolamento sull'IA non definisce il concetto di vulnerabilità»; tuttavia, tale nozione può essere interpretata come categoria «comprendente un ampio spetro di riferimenti, compresi le forme di suscettibilità cognitive, emotive, fisiche e di altra natura che possono incidere sulla capacità di un individuo o di un gruppo di persone di prendere decisioni informate o influenzare in altro modo il loro

[98] Cfr. paragrafo (59) delle Linee guida.
[99] Cfr. paragrafo (64) delle Linee guida.
[100] Cfr., nel complesso, i paragrafi da (63) a (75) delle Linee guida.
[101] In particolare, dai paragrafi (76ss) viene illustratala terza condizione per l'applicazione del divieto di cui alla lettera a) dell'articolo 5: ovvero il fatto che le tecniche sopra definite devono avere come obiettivo quello di distorcere materialmente il comportamento degli individui, al fine di provocarne un danno significativo. E il testo prosegue definendo in modo articolato cosa debba intendersi per 'distorsione materiale del comportamento' e per 'danno significativo'.

comportamento. Sebbene l'articolo 5, paragrafo 1, lettera b), del regolamento sull'IA si riferisca genericamente alle vulnerabilità, esso limita le persone interessate contemplate dal divieto a quelle definite in base all'età, alla disabilità o alla situazione sociale o economica, che in linea di principio hanno una capacità più limitata di riconoscere le pratiche manipolative o di sfruttamento dell'IA o di resistervi e che necessitano di maggiore protezione»[102]. Il testo prosegue poi con una disanima articolata delle singole categorie di vulnerabilità contemplate dal divieto elencato[103].

Proseguendo nell'analisi di questi orientamenti, una parte significativa delle Linee guida (paragrafi 9 e 10) è dedicata all'approfondimento del sistema delle eccezioni elencate nell'articolo 5 del Regolamento.

Tali orientamenti, innanzitutto, chiariscono che le deroghe previste rappresentano pur sempre un'eccezione di stretta interpretazione e che, pertanto, devono trovare applicazione unicamente nei casi in cui vengano soddisfatte tutte le condizioni prefissate dal legislatore unionale, tra cui: necessità, proporzionalità, adeguate garanzie procedurali e rispetto quanto più rigoroso possibile dei diritti e valori fondamentali[104].

Con particolare riguardo ai sistemi di identificazione biometrica remota in tempo reale, fermo restando il generale divieto di impiego di tali tecniche, l'articolo 5, lettera *h*) prevede un vasto sistema di eccezioni, consentendo l'impiego di questi sistemi per varie finalità, tra cui: la ricerca mirata di vittime di reati, per la prevenzione di minacce gravi ed imminenti per la pubblica sicurezza, per l'individuazione di autori di particolari reati.

Ciò premesso, le Linee guida si preoccupano di delineare in modo più dettagliato le fattispecie concrete che rientrano nei casi eccezionali enunciati dall'*AI Act*, precisando inoltre che non solo l'attivazione della tecnologia, ma anche la sua pianificazione, deve essere sottoposta al previo controllo giudiziario o amministrativo. Infine, si insiste sulla necessità di un impiego limitato (nel tempo e nello spazio) di tali sistemi particolarmente invasivi, nonché di un impego strettamente finalizzato al perseguimento del lecito obiettivo autorizzato, escludendo qualsiasi forma di sorveglianza generalizzata.

L'intento delle Linee guida, anche in questo caso, è quindi quello di meglio chiarire le intenzioni del legislatore unionale e, contestualmente, circoscrivere in modo stringente la portata delle eccezioni contemplate, per evitare che la logica derogatoria possa svuotare di efficacia il complessivo divieto delineato.

In definitiva, quindi, da questa breve disanima, appare chiaro che tali Linee guida forniscono senza dubbio un contributo significativo alla chiarezza normativa dell'*AI Act* e del suo articolo 5 in particolare, fornendo strumenti interpretativi utili (anche e soprattutto per i destinatari della normativa) per la sua applicazione concreta[105].

Tuttavia, chiaramente, questo è solo un primo passo: tali orientamenti forniscono spiegazioni giuridiche ed esempi pratici per aiutare le varie parti in gioco a comprendere e rispettare i requisiti imposti dall'*AI Act*, tuttavia, si tratta pur sempre di indicazioni prive di natura vincolante, che necessitano di essere sorrette da interventi unionali e statali di recepimento e di integrazione, al fine di concepire davvero un sistema normativo solido e completo, che garantisca una piena tutela dei diritti, senza affossare lo sviluppo tecnologico.

---

[102] Cfr. paragrafo (102) delle Linee guida.

[103] Cfr. paragrafo (104ss) delle Linee guida, dedicati alla definizione delle singole categorie di vulnerabilità che giustificano l'applicazione del divieto in questione, ovvero: età, disabilità, specifica situazione sociale ed economica.

[104] P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano, 2020.

[105] P. Dunn, *AI Act, rischio e costituzionalismo digitale*, in *Media Law. Rivista di diritto dei media*, pubblicato il: 22 aprile 2022.

6. La reale efficacia dell'AI Act (e del suo articolo 5) nella tutela dei diritti fondamentali: una riflessione conclusiva. A conclusione delle considerazioni sviluppate nel presente lavoro, non resta ora che proporre alcune riflessioni conclusive sull'efficacia complessiva dell'*Artificial Intelligence Act* nel perseguimento del suo obiettivo primario: assicurare piena tutela ai diritti e valori fondamentali riconosciuti nel contesto eurounitario.
Come già osservato, l'*AI Act* rappresenta il primo quadro giuridico organico sull'IA adottato a livello mondiale, destinato ad esercitare un'influenza regolatoria che va ben oltre i confini del mercato unico europeo[106]. Tale Regolamento ha garantito infatti all'Unione europea una posizione di avanguardia nella regolazione di queste nuove tecnologie, tentando di coniugare innovazione tecnologica e protezione dei diritti fondamentali nell'ecosistema digitale europeo.
Per perseguire tale obiettivo, viene adottato un approccio basato sul rischio, incentrato sul consolidamento di un modello di intelligenza artificiale affidabile ed umanocentrica. E la prima espressione concreta di questo approccio è la previsione di un elenco di pratiche inaccettabili, vietate in quanto irrimediabilmente lesive di dignità, libertà ed eguaglianza; elenco introdotto proprio per fissare una linea rossa invalicabile per lo sviluppo e l'uso dell'IA, nella consapevolezza che non tutto ciò che è tecnologicamente possibile è anche giuridicamente accettabile[107].
Vero tutto quanto premesso (e già ampiamente approfondito *supra*), la reale efficacia della disciplina europea – e dell'articolo 5 in particolare – dipenderà dalla sua concreta capacità di essere applicata e fatta rispettare. Come visto, la presenza di formulazioni lessicali talvolta eccessivamente ampie o prive di un ancoraggio definitorio, da un lato, e la previsione di un apparato derogatorio e di eccezioni potenzialmente suscettibili di interpretazioni estensive, dall'altro lato, finisce con il pregiudicare e compromettere la portata sostanziale dei divieti previsti nel Regolamento. Senza dimenticare che a ciò si deve aggiunge la sfida – non secondaria – della verificabilità tecnica, poiché molte delle condotte vietate richiedono complessi procedimenti di accertamento, spesso non immediato, delle modalità con cui tali sistemi intelligenti operano dietro le quinte[108].
In definitiva, il Regolamento e il suo articolo 5, rappresentano un importante passo verso una regolamentazione eticamente orientata dell'intelligenza artificiale; tuttavia, tali strumenti, da soli non sono sufficienti per garantire una tutela piena ed uniforme dei diritti fondamentali[109].
In questo quadro, per assicurare l'effettività dell'*AI Act*, un ruolo strategico dovrà essere assunto non soltanto dagli Stati membri – e dalla loro attività di implementazione della normativa – ma anche e innanzitutto dalle istituzioni europee, e dalla loro capacità di rafforzare i sistemi di monitoraggio, uniformare l'interpretazione del Regolamento e garantire meccanismi di controllo efficaci ed accessibili.

---

[106] Cina e Stati Uniti, infatti, non dispongono, ad oggi, di un quadro normativo unitario paragonabile. Gli Stati Uniti adottano un approccio settoriale e frammentato, basato su linee guida non vincolanti e su interventi federali limitati. La Cina, pur avendo introdotto normative significative, mantiene un approccio verticale e fortemente orientato alla tutela della sicurezza nazionale e comunque privo di una struttura generale equivalente all'AI Act europeo. In questo contesto, quindi, l'UE è il primo attore globale ad aver definito un quadro normativo sistematico, basato sui diritti fondamentali e su un approccio umanocentrico.
[107] M. Fasan, *L'intelligenza artificiale alla prova dell'eguaglianza. L'evoluzione del diritto costituzionale tra scenari attuali e futuri*, in M. Leone (a cura di), *Annali di Studi Religiosi*, Roma, 2025, 539 – 558.
[108] E. Prosperetti, *AI Act, divieti deboli e sanzioni aggirabili: perché così non funziona*, in *Agenda Digitale*, pubblicato il: 7 febbraio 2025.
[109] F.M. Mancioppi, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in *Federalismi.it*, 7, 2024, 112 – 134.

In tal senso, le recenti Linee Guida della Commissione europea sulle pratiche proibite rappresentano senza dubbio un importante tassello interpretativo, seppur nella loro efficacia non vincolante. Le stesse infatti forniscono esempi concreti, chiarificazioni interpretative e approfondimenti rispetto alla disciplina contenuta nell'*AI Act*, proprio al fine di tradurre la norma in prassi, con l'intento di consolidare un quadro di tutela più chiaro ed uniforme[110].
Ma restano pur sempre un primo (importante) avanzamento, sicuramente non sufficiente.
L'*AI Act* richiederà quindi un'azione istituzionale costante, finalizzata al consolidamento di un sistema di *governance* robusto e di un dialogo continuo fra società civile ed esperti del settore, nell'implementazione delle disposizioni normative.
In conclusione, il Regolamento segna senz'altro una tappa fondamentale nel percorso europeo di tutela dei diritti fondamentali nell'era della quarta rivoluzione industriale[111], tuttavia la sua reale efficacia dipenderà anche dalla sua capacità di raggiungere un adeguato punto di equilibrio tra norme, linee guida, *enforcement* e capacità adattiva. E il suo articolo 5, seppur ambizioso e innovativo, è solo un primo passo di un percorso tortuoso – destinato ad evolversi insieme alla tecnologia stessa – per garantire una gestione sostenibile e democratica dei sistemi di intelligenza artificiale, riconoscendo che la protezione dei diritti fondamentali richiede una risposta giuridica integrata e multilivello, capace di adattarsi all'evoluzione tecnologica, senza arretrare sul piano delle garanzie costituzionali.
Nell'era dell'intelligenza artificiale, la sfida non sarà dunque domare la tecnologia, ma tuttalpiù custodire l'umano. E in tale percorso, l'*Artificial Intelligence Act* è solo il primo tassello di questa responsabilità collettiva.

Abstract. L'affermazione, e la conseguente diffusione a macchia d'olio, di sistemi *AI-based* nei più disparati settori del vivere quotidiano, sollevano oggi interrogativi cruciali circa le modalità attraverso cui raggiungere un punto di equilibrio tra innovazione tecnologica e tutela dei diritti fondamentali, specialmente nell'ordinamento costituzionale europeo.
A tal proposito, l'Unione europea ha recentemente adottato l'*Artificial Intelligence Act* (*AI Act*), strumento normativo pionieristico, volto a dettare un quadro normativo finalizzato a governare l'implementazione e il conseguente utilizzo dei sistemi di AI, cercando di garantire la sicurezza ed il rispetto dei diritti fondamentali, senza tuttavia offuscare la necessaria incentivazione dell'innovazione tecnologica.
Sulla base di queste premesse, il presente contribuito vorrà concentrarsi, in particolare, sull'analisi dell'articolo 5 dell'*AI Act*, denominato *«prohibited artificial intelligence practices»* e dedicato all'individuazione e regolamentazione di sistemi *AI-based* che comportano un rischio definito 'inaccettabile', traducendosi in strumenti che comportano minacce concrete per diritti fondamentali, quali la dignità umana, la libertà e l'uguaglianza.
Nonostante, quindi, l'ambizione e le potenzialità dell'*AI Act*, considerato come il primo tentativo organico a livello globale di regolamentare in modo unitario lo sviluppo, la commercializzazione e l'utilizzo di sistemi di intelligenza artificiale, l'indeterminatezza e la flessibilità applicativa di alcune sue disposizioni e il sistema delle eccezioni previsto dall'articolo 5 – considerato talvolta facilmente aggirabile – suscitano rilevanti preoccupazioni circa la reale efficacia del Regolamento nel garantire una protezione piena e coerente dei diritti fondamentali.
Il *paper* si propone quindi di esaminare i punti di forza e i limiti dell'*AI Act*, soffermandosi in

[110] M. Fasan, *Intelligenza Artificiale e costituzionalismo contemporaneo. Principi, diritti e modelli in prospettiva comparata*, Trento, 2024.
[111] La quarta rivoluzione industriale, o Industria 4.0, indica la progressiva e costante trasformazione che investe tutti i domini dell'economia, grazie all'integrazione delle tecnologie digitali intelligenti nei processi produttivi ed industriali. Così K. Schwab, *The Fourth Industrial Revolution*, London, 2017.

particolare sull'analisi dell'articolo 5, al fine di verificare se le misure proposte siano sufficienti a tutelare i diritti fondamentali nell'era dell'intelligenza artificiale.

Abstract. The emergence and subsequent rapid spread of AI-based systems in a wide range of areas of everyday life are now raising crucial questions about how to strike a balance between technological innovation and the protection of fundamental rights, especially within the European constitutional order.
In this regard, the European Union has recently adopted the Artificial Intelligence Act (AI Act), a pioneering regulatory instrument aimed at establishing a regulatory framework to govern the implementation and subsequent use of AI systems, seeking to ensure safety and respect for fundamental rights, without however obscuring the necessary incentive for technological innovation.
On this basis, this contribution will focus, in particular, on the analysis of Article 5 of the AI Act, entitled «prohibited artificial intelligence practices» and dedicated to the identification and regulation of AI-based systems that pose a risk defined as «unacceptable», translating into tools that pose concrete threats to fundamental rights, such as human dignity, freedom and equality.
Despite the ambition and potential of the AI Act, considered the first comprehensive global attempt to uniformly regulate the development, commercialisation and use of artificial intelligence systems, the vagueness and flexibility of application of some of its provisions and the system of exceptions provided for in Article 5 – sometimes considered easily circumventable – raise significant concerns about the real effectiveness of the Regulation in ensuring full and consistent protection of fundamental rights.
This paper therefore aims to examine the strengths and limitations of the AI Act, focusing in particular on the analysis of Article 5, in order to assess whether the proposed measures are sufficient to protect fundamental rights in the era of artificial intelligence.

Parole chiave. *AI Act* – Diritti fondamentali – Pratiche vietate – Tutela dei diritti fondamentali – Articolo 5.

Key words. Artificial Intelligence Act – Fundamental rights – Article 5 – Prohibited artificial intelligence practices – UE.