L'AI Act: la risposta del legislatore europeo alle sfide dell'intelligenza artificiale

Alessandro Mantelero
Prof. ass. del Politecnico di Torino

Sommario: 1. Premessa. – **2.** Una visione prospettica. – **3.** La modulazione del c.d. *risk-based approach* in una normativa di prima generazione. – **4.** Conclusioni

1. Premessa

Nel contribuire, con una prima breve riflessione sul testo definitivamente adottato dell'AI Act[1], al crescente dibattito giuridico sull'intelligenza artificiale (di seguito AI), le

[1] Nello specifico, il 13 marzo 2024 è stato approvato dal Parlamento europeo il testo risultante dall'accordo avutosi durante i c.d. triloghi svoltisi in dicembre. È ancora attesa l'approvazione del Consiglio europeo, che già si è dichiarato favorevole, a seguito della revisione linguistico-legale finale. Poiché non si prevedono cambi di rilievo in questi ultimi passaggi, il testo adottato dal Parlamento può essere considerato sostanzialmente definitivo. La pubblicazione sull'Official Journal è attesa in maggio. Cfr. European Parliament, 2024 (P9_TA(2024)0138 Artificial Intelligence Act European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (consultato il 14.03.24). L'articolato, suddiviso in tredici capi e corredato da un apparato di tredici allegati, ruota attorno a cinque blocchi principali: (i) usi vietati dell'AI e gestione del rischio, inclusa quella successiva alla collocazione dei sistemi sul mercato (Capi II, III, VIII, IX); (ii) norme *ad hoc* per alcuni sistemi, principalmente incentrate sulla trasparenza, e per la c.d. *general-purpose AI* (Capi IV e V); (iii) misure in favore dell'innovazione, ad esempio *sandboxes* (Capo VI); (iv) modello di *govenance*, inclusivo delle competenti autorità di supervisione (Capo VII); (v) codici di condotta (Capo X). A corredo, poi, vi sono gli usuali capi di parte generale (Capo I) e di delegazione legislativa (Capo XI), nonché in materia di sanzioni (Capo XII) e le previsioni finali (Capo XIII). Come, purtrop-

pagine che seguono guarderanno al nucleo centrale di tale articolato normativo con un approccio incentrato sulle scelte di politica del diritto.

In ragione della natura e dello spazio relativo di questa riflessione, non si darà, dunque, conto delle diverse questioni che hanno animato ed animano il dibattito dottrinale con riguardo ai molteplici aspetti della relazione fra AI, diritto e società, tanto nel nostro come negli altri ordinamenti giuridici, lasciando al lettore di approfondire i singoli profili nell'ormai ampia letteratura disponibile.

Con riferimento alla disamina dell'AI Act, infine, non è questa la sede per un'analisi di dettaglio dello stesso, specie in presenza di alcune disposizioni – come ad esempio quelle concernenti gli organi di supervisione e controllo – che da sole meriterebbero un'ampia e dettagliata discussione, come dimostrato dalle attuali criticità implementative con rispetto alle controverse proposte governative avanzate in merito in Italia. Nella seguente trattazione si è, quindi, scelto di privilegiare l'intento di dare risposta ai tre seguenti principali quesiti di indagine: (i) quale è la visione del legislatore europeo nel regolare l'AI? (ii) Quale è la rilevanza nell'ottica regolatoria dell'adozione di un paradigma incentrato sul rischio? (iii) In che modo il modello c.d. *risk-based* interseca la dimensione dei diritti fondamentali?

2. Una visione prospettica

Nel 1968 Stanley Kubrick metteva in scena 2001: Odissea nello spazio, dove un'intelligenza artificiale si curava del benessere degli esseri umani, salvo poi volgersi in malevole e dar vita ad un iconico scontro tra volere dell'essere umano e della macchina. Non era certo la prima volta che l'uomo fantasticava di automi ed intelligenza delle macchine, ma non casualmente il film usciva negli stessi anni in cui, unitamente alla fondamentale opera di Alan Westin del 1967, veniva pubblicata una serie di monografie critiche sul ruolo dei calcolatori (come li si usava chiamare a quell'epoca) nella nuova società digitale[2].

Erano quelli gli anni in cui si intravvedevano già le possibilità dell'ICT (un acronimo che efficacemente combina comunicazione, informazione ed informatica) di cui si getta-

---

po, ci ha abituato negli ultimi anni il legislatore europeo, l'articolato contiene un corposo numero di considerando (180 a fronte di 113 articoli), spesso ripetitivi del testo degli articoli. Questi ultimi, poi, in vari casi risentono delle pressioni avutesi durante il processo di "negoziazione legislativa" e della necessità di addivenire a soluzioni di compromesso, a discapito della chiarezza del tenore letterale e dell'accuratezza giuridica dello stesso.

[2] Cfr., ad esempio, Miller, *The Assault on Privacy - Computers, Data Banks, Dossiers*, Ann Arbor, 1971; Brenton, *The Privacy Invaders. Coward-McCann*, New York, 1964; Packard, *The Naked Society*, New York, 1964. Con riferimento alla dottrina italiana, si vedano Losano, *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Torino, 1969; Frosini, *Cibernetica, diritto e società*, Milano, 1973; Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; nonché, più di recente, Alpa, Bessone (a cura di), *Banche dati, telematica e diritti della persona*, Padova, 1984; Zeno-Zencovich (a cura di), *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*, Napoli, 1985.

vano le basi, anche se gli strumenti risultavano ancora inadeguati nell'esplicarne il pieno potenziale. Così di AI, di sistemi esperti, di algoritmi per l'automazione, già si ragionava, ma mancavano moli enormi di dati digitalizzati ed elaboratori in grado di processarli. Come per il vapore, il telegrafo e molte altre invenzioni, c'erano le idee ma l'implementazione era agli albori.

Tuttavia, proprio la visione delle potenzialità dell'informatica, già allora induceva a ragionare in termini di impatto sociale con una chiara tensione fra il nuovo utile portato delle tecnologie ed il rischio relativo[3]. L'acritica fiducia nel progresso che aveva caratterizzato secoli passati era stata piegata nel '900 dall'esperienza delle guerre, dall'incertezza dei paradigmi scientifici, dalla percezione della debolezza dell'io umano. Al progresso quindi si univa la hybris, nella sfida di generare qualcosa di affascinante e terribile (come era stato per l'atomo), che contrapponeva alla visione positiva della controcultura americana interrogativi sul futuro di un mondo connotato da processi automatizzati.

Si potrebbe obiettare che tutto questo riguarda il passato e che ha poco di giuridico in relazione al commento dell'AI Act oggetto di queste brevi note. Tuttavia, servirebbe ricominciare da Westin, per ricordare come il giurista non possa riflettere su quelle che sono le regole prescindendo dalle istanze forti che connotano la società e generano il contesto cui le regole giuridiche, meri strumenti, sono chiamate a tentare di dare una delle possibili risposte.

Così, venendo ai giorni nostri, non si può comprendere l'AI Act ed il tenore delle previsioni ivi contenute senza tenere a mente il dominio statunitense e cinese sui mercati AI, la mossa arrischiata di Open AI (leggasi Microsoft) nel rendere disponibile sul mercato una tecnologia immatura come ChatGPT, o l'uso sistemico da parte di stati totalitari di strumenti di controllo biometrico e sociale. Fare un elenco delle categorie di usi vietati dell'AI contenute nell'AI Act, discutere le norme sui modelli della cosiddetta General Purpose AI (GPAI), affrontare il tema della valutazione d'impatto, risulterebbero esercizi incomprensibili se pensati solo nell'ottica di astratte categorie giuridiche, perpetuando un dogmatismo miope di cui non si avverte più il bisogno.

Muovendo da questa prospettiva, occorre in primo luogo collocare l'AI Act nel contesto geo-politico di pertinenza. Questa normativa non nasce, infatti, dal nulla né nasce dalle sole esigenze legate ai possibili impatti dell'AI, bensì è parte di un più ampio disegno dell'UE in tema di società digitale. Quando nel 2019 venne presentato il piano strategico della nuova Commissione europea, la regolamentazione del digitale venne posta come elemento fondamentale della legislazione dell'UE per il periodo 2019-2023. A quell'epoca le normative vigenti in tema di società digitale erano poche, *in primis* la Direttiva 95/46/CE sui dati personali, la sua filiazione in materia di e-privacy, la Direttiva 2000/31/CE sul commercio elettronico (centrale soprattutto in tema di responsabilità dei *providers*) e la

[3] Cfr. Rodotà, *op. cit.*

direttiva sull'informazione del settore pubblico (Direttiva 2013/37/UE). Oggi le normative adottate o prossime ad esserlo a livello europeo si contano invece a decine[4].

V'è, dunque, una strategia di politica del diritto che va ben oltre l'AI Act e che va preliminarmente colta per poter adeguatamente valutare la portata di quest'ultimo. Varie sono le direttrici che hanno spinto il legislatore europeo a un, forse sin troppo, intenso sforzo regolatorio nel corso della legislatura che va a chiudersi nel 2024.

In primis, ovviamente, ci sono i cambiamenti della struttura della società digitale. Dopo l'informatica distribuita degli anni '80 e l'avvento di Internet dei '90, da cui trassero origine le prime normative sui dati e sul commercio elettronico, l'esplosione dei sensori (leggasi IoT) e della potenza di calcolo (leggasi *cloud computing*) hanno aperto la strada all'AI, ma anche a nuove minacce sul fronte della *cybersecurity* e delle varie possibili ricadute sociali. Parallelamente, la concentrazione che ha connotato gli ultimi decenni dell'economia digitale, unitamente al superamento della distinzione fra mondo *on-line* ed *off-line*, hanno lasciato solo il ricordo di un contesto fatto di piccoli operatori da tutelare, rispetto al rischio legale a fronte dei loro pionieristici investimenti nel digitale, ed hanno richiesto più efficaci risposte al dominio di piattaforme globali[5].

Già rispetto a questi primi fattori, l'AI Act risulta una risposta necessaria a far fronte al cambio di paradigma tecnologico che ha abilitato l'ultima rivoluzione dell'AI, nonché ai fenomeni di concentrazione del potere informativo e di mercato su cui questa rivoluzione si basa. Non è, infatti, un caso che le applicazioni più avanzate e critiche dell'AI, nell'ambito GPAI, siano appannaggio di un numero estremamente limitato di operatori su scala globale da cui deriva un forte potere di condizionamento del mercato e dello scenario geo-politico, stante la loro localizzazione prevalente negli USA ed in Cina.

Proprio il piano geo-politico costituisce un elemento cruciale dell'ondata regolatoria dell'UE sul digitale. Qui il punto centrale è dato dalla cronica debolezza del settore industriale europeo rispetto ai concorrenti asiatici e nordamericani. Dalle materie prime alle piattaforme, l'UE non è riuscita ad acquisire posizioni di dominio tecnologico sul piano globale. Complici anche politiche aggressive di acquisizione delle realtà imprenditoriali più innovative ad opera dei maggiori operatori, l'Europa è ad oggi in gran parte terra di colonizzazione per le multinazionali straniere del digitale. In aggiunta, il gigantismo di tali multinazionali ed il loro peso nel condizionare la società digitale hanno di recente portato queste ultime ad agire come realtà quasi-statuali, non solo definendo in maniera autonoma ed autoreferenziale politiche nelle relazioni sociali mediate dal digitale (si pensi, ad esempio, alla dimensione culturale delle politiche di moderazione dei contenuti), ma anche esercitando non di rado (dalle *smart cities* alle applicazioni in uso durante la pandemia) funzioni proprie dello Stato[6].

---

[4] Per una mappa della normativa UE in materia, si veda ad esempio https://www.bruegel.org/sites/default/files/2023-11/Bruegel_factsheet.pdf (consultato il 02.03.24).

[5] Cfr. Digital Markets Act e Digital Services Act.

[6] Cfr., ad esempio, in tema Goodman, Powles, *Urbanism Under Google: Lessons from Sidewalk Toronto*, in *Fordham Law Review*, 2019, 88 (2), 457 ss.

In tale contesto è, quindi, chiara la necessità per l'UE di dotarsi di una normativa che regoli ad ampio spettro il digitale. Non potendo, infatti, avvalersi di forme di pressione e persuasione informali, il *bully pulit* cui faceva riferimento Reidenberg[7], onde poter indirettamente condizionare i produttori di tecnologia[8], non resta che il rimedio esogeno di norme vincolanti a presidio degli interessi europei. Questo è un ulteriore elemento connotante (anche) l'AI Act, e sul piano della norma giuridica, è evidenziato non solo dal ricorso all'intervento legislativo in sé, laddove i paesi produttori di AI sono invece più orientati verso approcci di *soft law*, ma anche dalle specifiche disposizioni sull'efficacia territoriale dell'AI Act, ove se ne prevede l'applicabilità ai fornitori dei sistemi di AI disponibili nell'UE indipendentemente dallo stabilimento del fornitore, incluso il caso in cui fornitori ed utilizzatori primari (*deployers*) siano localizzati fuori dall'UE, ma il risultato generato dai sistemi di AI venga usato nell'Unione .

Mettere al centro dell'approccio regolatorio gli interessi europei comporta però la necessità, di definire quali essi siano o meglio di definire le priorità fra quelli che costituiscono la ragion d'essere dell'Unione. A riguardo, se si confronta l'iter dell'elaborazione legislativa dell'AI Act con quello del GDPR, sono evidenti significative ed indicative differenze. La leadership del direttorato DG Justice, incentrato su libertà, sicurezza e giustizia, che aveva connotato l'elaborazione del GDPR è qui sostituita da quella di DG Internal Market, Industry, Entrepreneurship and SMEs. L'ossatura dell'AI Act è chiaramente quella di una regolamentazione industriale e di sicurezza dei prodotti, come per altro è stata sovente presentata dalla Commissione.

Risulta quindi evidente un forte iato fra il modo in cui i rischi dell'AI sono stati metabolizzati nel discorso di politica del diritto, incentrato sui temi dell'etica – si pensi alle iniziative dell'EDPS, nonché al più discutibile apporto del High-Level Expert Group on Artificial Intelligence (di cui si trova traccia in uno dei considerando dell'AI Act) – e dei diritti fondamentali, sebbene non di rado con una lamentabile confusione fra i due piani, e la visione fatta propria della Commissione rivolta principalmente alla sicurezza industriale, con un'ampia attenzione alla gestione del rischio in termini di valutazione di conformità e con l'attribuzione di un peso significativo agli standard industriali.

Non a caso, la proposta della Commissione includeva riferimenti alla tutela dei diritti fondamentali rispetto ai potenziali impatti dell'AI, ma senza una specifica elaborazione a riguardo. Tutto questo in contrasto con un dibattito pubblico da cui emergeva come i rischi dell'AI avessero meno a che fare con il danno che il robot collaboratore può recare all'operaio e ben più con la potenziale discriminazione e disinformazione che gli algoritmi stanno introducendo nella società. Solo all'esito del dibattito parlamenta-

---

[7] Cfr. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 1998, 76 (3), 553 ss.

[8] Vedasi in questa linea The White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 ottobre 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (consultato il 31.10.23).

re, anche grazie all'appoggio dell'accademia internazionale[9], una maggior elaborazione sull'impatto sui diritti fondamentali è ora presente nell'AI Act.

Questa connotazione della proposta regolatoria, qui brevemente tratteggiata, mette però in luce l'obiettivo del legislatore europeo, che non è primariamente quello della tutela dei diritti fondamentali, bensì quello di favorire lo sviluppo dell'AI in un contesto di debolezza industriale del settore in Europa. È da qui che deriva l'approccio incentrato sulla sicurezza del prodotto e, soprattutto, l'equilibrio scelto nella gestione del rischio di cui si dirà più ampiamente nel seguito. Qui, in termini generali, basti rilevare come le scelte di politica industriale hanno condotto ad una visione incline all'accettazione del rischio, diversa dalla più marcata avversione per lo stesso che si ravvisa invece nel GDPR (v. art. 35, GDPR).

Da ultimo, va rilevato come l'intensa attività regolatoria sul digitale che ha connotato questi ultimi anni abbia sollevato una serie di questioni sistemiche che hanno inciso anche sull'AI Act. In primo luogo, la parcellizzazione delle varie iniziative in termini di soggetti promotori, ha indotto ad un'elaborazione dei testi più per silos che in maniera sistematica. Come già rilevato da regolatori quali l'EDPB e l'EDPS, l'ansia di addivenire ad un nuovo quadro normativo, indotta dai motivi di cui si è detto, ha prodotto in tempi piuttosto ristretti molti ed articolati testi, senza che fosse affinato il coordinamento fra gli stessi. In secondo luogo, tale ampio sforzo regolatorio ha inciso sui tempi dei vari *iter* di approvazione, con il risultato che alcune aree sono solo parzialmente normate: ne è esempio la mancata approvazione del pilastro complementare all'AI Act, ovvero la direttiva sulla responsabilità civile correlata all'uso dell'AI.

Va per altro osservato come l'approccio adottato dal legislatore europeo si connoti per un notevole pragmatismo, guardando ad una regolamentazione incentrata sui rimedi *ex ante*, in chiave di gestione del rischio ed approccio *by-design* al prodotto, piuttosto che sui rimedi risarcitori *ex post* che spesso ancora stimolano il dibattito dottrinale, ma si rivelano sempre più essere regole di chiusura di una normativa che mira a prevenire i rischi dei sistemi complessi. Questo perché il rimedio tradizionale della responsabilità civile mal si concilia con un contesto connotato da complessità tecnologica, operatori globali con grandi capacità finanziarie, polverizzazione dei danni e, nell'ottica di stimolare la fiducia nelle nuove tecnologie (la c.d. *trustworthy AI*), necessità di garantire ambienti tecnologici sicuri piuttosto che rimedi in caso di disastrose conseguenze.

Tuttavia, la mancanza di un sistema di regole di chiusura sulla responsabilità civile nell'AI[10] – stanti le questioni inerenti all'allocazione della stessa sia rispetto alle varie componenti dei sistemi AI, sia rispetto all'interazione uomo-macchina – segna una catti-

---

[9] Brussels Privacy Hub, *More than 150 university professors from all over Europe and beyond are calling on the European institutions to include a fundamental rights impact assessment in the future regulation on artificial intelligence*, 12 settembre 2023, https://brusselsprivacyhub.com/2023/09/12/brussels-privacy-hub-and-other-academic-institutions-ask-to-approve-a-fundamental-rights-impact-assessment-in-the-eu-artificial-intelligence-act/ (consultato il 07.03.24).

[10] Cfr. da ultimo Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024, 64 ss.

va coordinazione dell'approccio europeo ove altri legislatori (si pensi alle proposte brasiliane in tema di AI) hanno più appropriatamente combinato la gestione del rischio, con le relative sanzioni in caso di difformità, e la responsabilità civile per i danni causati dall'AI.

Non è stata, dunque, felice la scelta di tenere distinti i due profili, così come quella di affrontarli con due strumenti legislativi di natura differente e, per giunta, promuovere un parallelo aggiornamento del quadro normativo della responsabilità da prodotto in generale. Va da sé che sviluppare un modello di tutela *ex ante*, incentrato sull'analisi del rischio, senza poi elaborare un quadro adeguato e coerente per le ipotesi residuali in cui la cattiva o carente gestione dei rischi sia causa di danni finisce per menomare l'impatto complessivo dell'intervento normativo come derivante dall'AI Act, che risulta così un'opera incompiuta in una visione ampia della regolamentazione dell'AI. Né, a differenza della tutela dei dati personali, si può qui argomentare una limitata rilevanza dei profili risarcitori, posto che la delega ai sistemi di AI di ruoli di gestione di infrastrutture critiche, sia sul piano funzionale sia su quello sociale, non fa presagire scenari di danno potenziale circoscritto.

3. La modulazione del c.d. *risk-based approach* in una normativa di prima generazione

L'AI Act è stato elaborato dal legislatore europeo come un modello di regolamentazione incentrato sul rischio (*risk-based approach*) per le ragioni di cui si è detto inerenti alla necessità di "mettere in sicurezza" lo sviluppo dell'AI e di prevenirne eventuali conseguenze avverse, specie in un contesto dove limitato è il controllo diretto dello sviluppo dell'AI attraverso l'industria europea.

L'approccio incentrato sul rischio, in sé non una novità – né con riguardo alla sicurezza industriale, né a quella da prodotto e, nemmeno, nell'ambito della protezione dei diritti fondamentali, come dimostrato dalla pluridecennale esperienza della protezione dei dati personali –, può tuttavia essere modulato in maniere molteplici con ricadute diverse sugli interessi tutelati e sulle forme di tutela.

A riguardo, va rilevato come l'AI Act sia una legislazione di prima generazione, rispetto alla quale più marcato è dunque il *trade-off* fra le esigenze di tutela e quelle di non inibire l'investimento in una nuova tecnologia. Come è stato il caso della responsabilità da prodotto difettoso rispetto all'evoluzione manufatturiera o, più recentemente, della responsabilità dei fornitori di servizi online (*Internet service providers*) rispetto all'espansione della rete Internet, limitazioni in termini di responsabilità o di oneri di controllo in capo ai principali attori dell'espansione di una nuova tecnologia sono state introdotte per favorire tale espansione, seppur al prezzo di minori tutele.

La stessa logica pro-innovazione è fatta propria ora dall'AI Act, come risulta evidente dalla scelta di fondo relativa al modo in cui l'approccio incentrato sul rischio è stato calibrato. In tal senso, salvo minori previsioni in termini di trasparenza ed i casi di divieto, l'AI Act regola solamente gli usi dell'AI connotati da alto rischio. In secondo luogo, defini-

sce tale ambito operativo mediante una tipizzazione, basata sull'elenco di cui all'Allegato III. Da ultimo, elabora il concetto di rischio in termini di accettabilità.

Se si confronta l'AI Act con il GDPR, non a caso una legislazione di terza o quarta generazione (a seconda di come vengano scandite le partizioni normative in materia[11]), la differenza nell'approccio incentrato sul rischio è evidente. Il GDPR riguarda tutti i livelli di rischio, riservando all'alto rischio una procedura *ad hoc* (DPIA) e configurandolo come soglia non superabile, con la conseguente necessità di ridurre il rischio al di sotto della stessa, secondo una quantificazione contestuale e non tipizzata.

Le ragioni del diverso approccio seguito nell'AI Act sono, appunto, quelle legate alla necessità di trovare un difficile equilibrio fra gestione del rischio ed investimenti in un settore già debole quale l'industria AI europea. In tale ottica, si è scelto di circoscrivere questo primo intervento ai soli casi più gravi, ricorrendo alla nozione di alto rischio.

In secondo luogo, si è preferito un approccio tipizzante per facilitare gli operatori nel conoscere fin da subito se soggetti o meno alla nuova normativa. Questa scelta, volta ad un'apparente semplificazione, si è poi rivelata intrinsecamente complessa in ragione della difficoltà di dare una definizione puntuale delle applicazioni ad alto rischio ed all'evoluzione degli usi dell'AI. Da qui interventi correttivi, quali possibilità di deroghe[12] e di modifiche future all'Allegato III[13], con un quadro complessivo che più che semplificare rischia di rendere tortuoso e foriero di contenziosi il panorama operativo industriale dell'AI.

Meritevole d'attenzione è poi il criterio secondo cui i casi di alto rischio vengono gestiti in termini di strategie di mitigazione. Secondo il modello del rischio industriale, si ritiene che lo sviluppo dell'AI possa trovare giustificazione[14] sebbene foriero di rischi elevati. Da qui il criterio dell'accettabilità del rischio residuale, che in quanto tale non

---

[11] Cfr. Mayer-Schönberger, *Generational Development of Data Protection in Europe*, in Agre, Rotenberg (a cura di), *Technology and Privacy: The New Landscape*, Cambridge, Ma-London, 1997, 219 ss.

[12] Cfr. art. 6.4, AI Act ("A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation set out in Article 49 (2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.").

[13] Cfr. art. 7, AI Act, in cui si riconosce alla Commissione il potere di "adopt delegated acts in accordance with Article 97 to amend Annex III by adding or modifying use-cases of high-risk AI systems where both of the following conditions are fulfilled: (a) the AI systems are intended to be used in any of the areas listed in Annex III; (b) the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.".

[14] Si veda anche il riferimento espresso ai benefici nell'art. 7, AI Act ("When assessing the condition under paragraph 1, point (b),, the Commission shall take into account the following criteria: [...] "the magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety").

deve necessariamente essere non alto, ma solo giustificato da prevalenti interessi di diversa natura.

Tale criterio di accettabilità viene ad essere elaborato attraverso la valutazione del rischio prevista dall'AI Act, ossia la valutazione di conformità di cui agli artt. 43, 17 e 9. Va, tuttavia, rilevato come una componente di tale valutazione sia anche la stima dell'impatto sui diritti e sulle libertà fondamentali, rispetto a cui pare doversi escludere un'accettabilità fondata su un'indistinta comparazione fra gli interessi in gioco. Il livello di tutela fornito dall'ordinamento europeo, nonché dai singoli Stati Membri, ai diritti fondamentali ne escludono la possibilità di compressione per la semplice presenza di interessi contrapposti o in virtù di un'accettabilità sociale. Solo in caso di un bilanciamento con interessi ritenuti pari o superiori dall'ordinamento potrà essere, infatti, giustificata una necessaria e proporzionata compressione dei diritti fondamentali.

Da ultimo, vi sono casi in cui il legislatore europeo ha ritenuto alcune applicazioni AI inaccettabili proprio in ragione del forte contrasto con i diritti fondamentali ed i principi del diritto comunitario. Si tratta di quelle indicate nell'art. 5 dell'AI Act, tra cui figurano tecniche manipolative, il c.d. *social credit scoring*, ed alcuni usi invasivi delle tecnologie biometriche. A riguardo ampio è stato il dibattito, con anche il coinvolgimento della società civile, circa l'individuazione degli usi vietati e circa le deroghe (non poco articolate, specie circa l'uso dell'identificazione biometrica) che si sono aggiunte nel corso del processo legislativo.

Il modello complessivo che emerge dall'intero quadro normativo nell'approccio al rischio correlato all'AI più che basarsi sulla spesso evocata piramide del rischio (molte applicazioni non regolate, alcune con limitati requisiti richiesti *ex lege*, poche ad alto rischio soggette alla valutazione di conformità, pochissime vietate) – che in realtà poco dice in merito alle scelte di politica legislativa ed è, soprattutto, funzionale ad una narrazione che vuole evidenziare l'intervento minimalista e circoscritto ai casi più gravi da parte del legislatore europeo, sottolineandone l'orientamento pro-innovazione –, dovrebbe essere invece ricostruito secondo la tripartizione degli approcci adottati nella valutazione del rischio.

A tal riguardo occorre distinguere fra *technology impact assessment*, *conformity impact assessment* e *fundamental rights impact assessment* (i termini inglesi sono quelli di maggior uso come riferimento concettuale nel dibattito europeo). Il primo è sostanzialmente simile all'esercizio elaborato nell'art. 5 dell'AI Act per definire le categorie vietate, si tratta di una valutazione *ex ante* formulata in astratto circa una data tipologia di applicazioni tecnologiche, tenendo conto degli usi noti e potenziali, di cui si valuta l'accettabilità normativa in ragione dell'impatto delle stesse sui principi fondanti del diritto dell'Unione. Ne sono esempio l'uso di tecnologie subliminali volte a manipolare la volontà individuale proprie di "AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons

significant harm". Rientra anche nella stessa tipologia di valutazione (*technology assessment*) l'elenco delle ipotesi di applicazioni reputate ad alto rischio di cui all'Allegato III, ove anche qui i sistemi di AI sono considerati in termini di categorie d'uso a prescindere dalla specifica configurazione ed impiego contestuale.[15]

In proposito, mentre per la possibile variazione delle categorie vietate, in ragione dell'evoluzione tecnologica e del contesto socio-tecnico, si prevede il ricorso a successivi interventi di modifica dell'art. 5 dell'AI Act, la valutazione circa le applicazioni ad alto rischio è demandata per il futuro all'operato della Commissione. Quest'ultima scelta, seppure tale da circoscrivere l'azione della Commissione nei limiti definiti dall'art. 7 dell'AI Act, comporta tuttavia l'attribuzione alla stessa della possibilità di modificare l'oggetto della normativa, cosa che pare peculiare, considerata la natura istituzionale della Commissione e la legittimità del processo legislativo dell'Unione.

Di diversa natura è, invece, la valutazione di conformità (*conformity assessment*). Che essa si basi sulle procedure di cui all'Allegato VII (Conformity assessment based on assessment of quality management system and an assessment of the technical documentation) o all'Allegato VI (Conformity assessment procedure based on internal control), a seconda che riguardi o meno l'uso di tecnologie biometriche ad alto rischio come definite nell'Allegato III[16], sempre richiede l'implementazione di un sistema di gestione della qualità *ex* art. 17 dell'AI Act, di cui è componente centrale il sistema di gestione del rischio previsto all'art. 9, comprensivo anche della valutazione dell'impatto sui diritti fondamentali.

La valutazione di conformità, a differenza del *technology assessment*, è una valutazione incentrata su una data applicazione AI, connotata da specifiche e caratterizzanti funzionalità, sebbene suscettibile di essere impiegata in diversi scenari d'uso[17]. Tale valutazione si incentra sul rischio industriale in termini tradizionali di pregiudizio all'integrità fisica e sicurezza del prodotto/servizio, ma include anche i rischi in termini di

---

[15] Si fa riferimento, ad esempio, nell'ambito educativo a "AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels", laddove varie sono le possibilità di configurare tali sistemi in ragione dei parametri impiegati e delle soglie adottate, nonché differenti possono essere i risvolti applicativi in base allo specifico contesto socio-culturale d'uso.

[16] Cfr. art. 43, paragrafi 1 e 2, AI Act.

[17] Seguendo con l'ipotesi fatta in precedenza, vedasi nota 15, la valutazione di conformità riguarderà un dato applicativo AI che, sulla base di parametri inerenti alla votazione dello studente in un dato arco di tempo, alla performance nelle singole materie, all'età, alle serie storiche usate nella fase di *training* ed a molti altri parametri ancora, sarà in grado di valutare l'ammissione ad una dato corso di laurea. Non si tratterà quindi di un tipo di applicativo AI, ma di uno specifico prodotto con proprie scelte di *design* e di *training*, pur tuttavia lo stesso sarà suscettibile di essere applicato in contesti differenti in termini di variabili demografiche, di tipologia di indirizzo di studio etc.

pregiudizio per i diritti fondamentali[18]. A riguardo, l'impostazione del legislatore europeo è quella di demandare all'adozione di standard specifici tale giudizio di conformità[19].

Va in proposito rilevato come il ricorso al processo di standardizzazione per la valutazione di conformità sia coerente con la prassi della gestione del rischio industriale e da prodotto, in termini di sicurezza (incluso quella fisica dei soggetti umani che interagiscono con le macchine, qui l'AI), ma appaia inadeguato in relazione alla componente inerente alla valutazione dell'impatto sui diritti fondamentali. Riguardo a questi ultimi, non solo l'opacità dei sistemi di standardizzazione[20], ma anche il mancato coinvolgimento di esperti in tema di diritti fondamentali costituiscono una prima criticità, persino stimmatizzata nella bozza di richiesta di standardizzazione avanzata dalla Commissione a CEN-CENELEC, di cui esplicitamente si ammette la scarsa competenza in materia di diritti fondamentali[21].

Al di là dei problemi strutturali del sistema di standardizzazione, vi è poi la più sostanziale obiezione metodologica circa la difficoltà del ricorso a standard per la valutazione dell'impatto sui diritti fondamentali. Gli standards, infatti, per loro natura sono utilizzabili in presenza di processi connotati da una dinamica costante e ripetitiva, così è possibile definire uno standard nella costruzione delle strade ferrate, poiché le variabili di velocità, peso, pendenza, etc. si muovono entro *ranges* costanti rispetto ad un'attività di circolazione dei treni che risulta avere connotati uniformi a prescindere dai diversi itinerari di percorrenza.

Una simile uniformità non è ravvisabile nel contesto dell'impatto dell'AI sui diritti fondamentali, laddove la stessa applicazione AI può avere impatti diversi in ragione delle caratteristiche delle tecnologie impiegate, del contesto d'uso e dei soggetti coinvolti. Se si considerano, ad esempio, i sistemi di videosorveglianza basati su AI, in termini di impatto sui diritti fondamentali, diversi sono gli scenari a seconda che vengano usati in spazi pubblici o privati, che in questi ultimi si trovino minori o altri soggetti vulnerabili[22], che vengano implementate funzionalità di tracciamento in tempo reale o meno, che siano utilizzati in contesti connotati da alti livelli di criminalità con la finalità di contrasto del crimine, ed a seconda di molti altri fattori ancora che si potrebbero aggiungere in ragione della varietà degli scenari possibili.

---

[18] Cfr. art. 9.2.a, AI Act ("identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to the health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose").

[19] Cfr. art. 40, AI Act (Harmonised standards and standardisation deliverables).

[20] Cfr. Veale, Borgesius, *Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, in *Computer Law Review International*, 2021, 22 (4), 97 ss. https://doi.org/10.9785/cri-2021-220402.

[21] Cfr. European Commision, *Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence*, 5 dicembre 2022, https://ec.europa.eu/docsroom/documents/52376?locale=en (consultato il 25.02.24).

[22] Cfr. anche Malgieri, *Vulnerability and Data Protection Law*, Oxford-New York, 2023.

Risulta, dunque, evidente come la variabilità della dimensione contestuale della valutazione dell'impatto sui diritti fondamentali mal si concili con un'idea di standardizzazione, se si intende con questa la possibilità di definire un iter procedurale preciso ed uniforme, fatto di specifiche fasi di conformazione della tecnologia secondo *patterns* predefiniti. Diversa può, invece, essere la conclusione laddove per standards ci si riferisca a standard metodologici, ossia non standard definitori di un dato processo bensì volti a stabilire l'approccio metodologico generale alla gestione del rischio nel caso dei diritti fondamentali, quindi con specifico riguardo al tema centrale dei criteri di valutazione dell'impatto necessari per una comparazione fra le varie opzioni di design nello sviluppo dell'AI[23].

Da ultimo, a seguito del dibattito al Parlamento europeo, è stato poi introdotto nell'AI Act uno specifico obbligo di valutazione dell'impatto sui diritti fondamentali (FRIA, Fundamental Rights Impact Assesment) ad opera degli utilizzatori primari (*deployers*) dei sistemi di AI. Tale valutazione assume ruolo centrale in linea con la natura contestuale della valutazione d'impatto sui diritti fondamentali. Quest'ultima può, infatti, solo in parte essere elaborata dal fornitore dell'AI sulla base dei possibili scenari d'uso, come accade nella valutazione di conformità, e necessita di tener conto della concreta applicazione dell'AI nel caso specifico. Questo è in linea con i processi di valutazione di impatto con riguardo ai diritti umani (HRIA) ed alla tutela dei dati personali (DPIA), entrambi basati su valutazioni contestuali dell'effettivo pregiudizio potenziale per i diritti e le libertà in gioco.

In linea con la teoria generale, con riferimento all'allocazione del rischio e delle relative responsabilità in termini giuridici, la FRIA si combina dunque alla valutazione di conformità, spostando sugli utilizzatori primari (*deployer*) parte dell'onere di gestire le potenziali conseguenze negative dell'AI rispetto al contesto operativo specifico e reale dei sistemi di AI, con riguardo al quale tali soggetti hanno maggiori margini di controllo o, quantomeno, di valutazione del rischio concreto.

Infine, a differenza della valutazione di conformità, per la FRIA non si prevede il ricorso a processi di standardizzazione, in linea con le precedenti esperienze in tema di DPIA e HRIA, laddove sono state le prassi operative a delineare i migliori modelli di valutazione del rischio.

Guardando a questa tripartizione del processo valutativo attraverso al quale il modello *risk-based* viene a concretizzarsi nell'AI Act e nella sua applicazione, va tuttavia rilevata una carenza di uniformità di approccio resa evidente nella mancanza di parametri comuni di valutazione del rischio e di comuni metodologie per la valutazione dell'impatto sui diritti fondamentali nel contesto AI. Se, dunque, da un lato il rischio è definito in termini generali nell'art. 3 come una combinazione di probabilità e gravità dell'evento

[23] Per un esempio di questo approccio, cfr. Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*, The Hague, 2022, capitolo 2, https://doi.org/10.1007/978-94-6265-531-7 (open acess).

pregiudizievole, una serie di parametri aggiuntivi vengono elencati nell'art. 7 con riguardo al *technology assessment*, indicazioni specifiche mancano invece per la valutazione di conformità e, in un maldestro intento semplificatorio durante i triloghi, sono state espunte dal testo definitivo della FRIA rispetto alla più accurata proposta parlamentare. Da qui la necessità di una riflessione metodologica su come realizzare la valutazione d'impatto, specie in relazione ai diritti fondamentali, punto cruciale dell'implementazione dell'AI Act.

Rispetto a questo impianto di base dell'AI Act, vanno poi considerati due blocchi di disposizioni inerenti rispettivamente agli obblighi di trasparenza previsti per i sistemi di non alto rischio e le previsioni aggiunte nella fase finale dell'elaborazione normativa per fare fronte alle preoccupazioni sollevate dai sistemi di General-purpose AI (GPAI), divenuti noti al grande pubblico soprattutto in seguito al rilascio di ChatGPT.

Circa il primo limitato gruppo di norme, l'AI Act fa proprio quanto già indicato dal Consiglio d'Europa nelle linee guida su AI e tutela dei dati personali[24] circa l'obbligo di rendere quantomeno edotto l'utilizzatore finale in merito al fatto di interagire con un sistema di AI; obbligo giustificato dalle capacità dell'AI di emulare diversi comportamenti umani nell'interazione uomo-macchina. Obblighi specifici aggiuntivi di trasparenza sono poi dettati con riguardo sia ai produttori sia agli utilizzatori primari (*deployer*) dei sistemi di AI in relazione alla capacità dell'AI di generare contenuti sintetici, specie in ragione delle criticità che questo può comportare nell'alterazione della realtà con ricadute anche sociali di rilievo (e.g., *fake news*)[25].

Più complesso è il discorso in relazione alla General-purpose AI (GPAI), ove la fretta dovuta all'emergere del problema nella fase finale del processo legislativo e le posizioni contrarie (tra cui quella del governo italiano) ad una incisiva regolamentazione di tale rilevante aspetto hanno portato a delineare una regolazione che si potrebbe definire minimalista.

Sul punto la riflessione dovrebbe andare ben oltre le limitate considerazioni consegnate a queste pagine, sollevando questioni che sono alla radice del problema della regolamentazione della tecnologia e che hanno a che fare con il ben noto dilemma di Collingridge, laddove la GPAI è una tecnologia ancora in uno stadio iniziale, non a caso afflitta da diversi irrisolti problemi operativi ed anche carente di un vero e proprio modello di business che ne giustifichi gli alti costi operativi e di impatto ambientale.

L'indifferenza per l'approccio incentrato sull'innovazione responsabile da parte degli operatori statunitensi, la decisione di rendere disponibili sul mercato soluzioni ancora instabili e fonte di molteplici rischi, oltre che generate in violazione delle norme a

---

[24] Council of Europe, *Guidelines on artificial intelligence and data protection adopted by the Committee of the Convention for the Protection of Individuals with regards to Processing of Personal Data (Convention 108) on 25 January 2019*, paragrafo 2.11, https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7 (consultato il 10.01.24).

[25] Cfr. art. 50, AI Act.

tutela dei dati personali[26] ed a protezione delle privative intellettuali[27], hanno indotto il legislatore europeo ad una reazione sul piano normativo volta a trovare un equilibrio fra la protezione e la fascinazione per le possibilità economiche (specie supportate in fase di triloghi dalla Francia in relazione al caso Mistral AI), laddove forse avrebbe invece avuto maggior ragion d'essere un approccio basato sul principio di precauzione.

Il risultato di queste tensioni di politica industriale è stata l'elaborazione di alcune norme in cui si distingue fra modelli di GPAI e sistemi che tali modelli integrano. Dei modelli preoccupa il c.d. rischio sistemico, sostanzialmente presunto in ragione di criteri dimensionali di tali modelli e con presunzione relativa, prevedendosi inoltre un pubblico registro per i modelli GPAI connotati da rischio sistemico. Aspetto centrale è appunto tale rischio, di cui i fornitori dei modelli dovranno provare di aver effettuato un'opportuna analisi e gestione, tenendo traccia del loro operato secondo l'ormai dominante paradigma di *accountability* delle normative europee in tema di società digitale.

Poiché tali modelli sono destinati ad essere inseriti in sistemi di AI anche di soggetti terzi, sono poi previsti obblighi di trasparenza per i loro creatori in favore di tali terze parti, nonché la comunicazione di informazioni circa le fonti usate per il *training* dei modelli stessi (la conoscenza delle fonti che può essere utile, ad esempio, al fine di individuare potenziali *biases*).

Da ultimo, sempre in un'ottica di contemperamento fra gestione dei rischi potenziali dell'AI e degli auspicati benefici, vanno lette le diverse disposizioni specifiche pro-innovazione contenute nell'AI Act, a partire dall'ampia eccezione prevista per le attività di ricerca[28], fino alle norme *ad hoc* in materia di *sandboxes*[29], ossia ambiti di sperimentazione controllata (già adottati nel contesto dell'attuazione del GDPR in vari Paesi), ed

---

[26] Cfr. Garante per la protezione dei dati personali, Registro dei provvedimenti n. 112 del 30 marzo 2023, doc. web n. 9870832, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832 (consultato il 05.02.24); Id., Provvedimento dell'11 aprile 2023, Registro dei provvedimenti n. 114 dell'11 aprile 2023, doc. web n. 9874702, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702 (consultato il 05.02.24); Id., ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione per le violazioni alla normativa privacy, comunicato stampa del 29.01.24, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9978020 (consultato il 05.02.24).

[27] Cfr. United States District Court, Southern District of New York, *The New York Time Company v. Microsoft Corporation, OpenAI, Inc., OpenAI LP, OpenAI GP, LLC, OpenAI, LLC; OpenAI OPCO LLC, OpenAI Global LLC, OAI Corporation, LLC, and OpenAI Holdings, LLC*, 27 dicembre 2023, https://nytco-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf (consultato il 15.01.2024).

[28] Cfr. art. 2.6 ("This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development").

[29] Cfr. artt. 57 ss., AI Act. Per *sanbox* regolatoria, l'AI Act intende, ai sensi dell'art. 3.55, "a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision".

alle disposizioni volte a consentire di testare i prodotti AI nel mondo reale con impliciti risvolti di sperimentazione sociale che, per tale ragione, chiamano in causa anche il processo di valutazione etica[30].

4. Conclusioni

Da un primo sguardo sugli aspetti salienti dell'AI Act emergono, infine, alcuni spunti di riflessione con riguardo allo studio della materia e del diritto dell'informatica, che si connota sempre più come il laboratorio più avanzato della cultura civilistica in una società in cui le istanze collegate alla diffusione di tecnologie innovative sono tema dominante rispetto alle quali il diritto è chiamato a dare risposte in termini di regolazione del contesto socio-tecnico.

Una prima considerazione riguarda l'approccio metodologico del civilista al tema della regolamentazione della tecnologia. Decenni or sono la storiografia europea comprese, con la scuola degli *Annales*, la limitatezza di un'indagine storica meramente evenemenziale e la necessità di uno sguardo più ampio con rispetto al fenomeno storico, incluso un correlato nuovo metodo di tipo interdisciplinare ove lo storico si interessava all'economia, alla sociologia, alla psicologia e ad altri rilevanti saperi per accertare il vero. La stessa svolta pare ancora da completarsi nell'apporto civilistico allo studio del diritto.

Guardare alla concretezza dei problemi regolatori, individuare il punto di congiunzione fra la visione sistemica del diritto e la sua concretizzazione operativa, studiarne le interazioni necessarie con altri ambiti (come quello dell'analisi del rischio nel caso dell'AI), paiono esercizi meno degni della civilistica. Questo con il risultato che sono poi i c.d. pratici a colmare questa lacuna, spesso meno attrezzati in termini di comprensione del quadro sistemico e teorico. A ciò si aggiunga che una visione prevalentemente orientata al dibattito dogmatico in quanto tale ha portato ad esempio nel caso dell'AI a fantasiose discussioni circa la natura di persona giuridica dell'AI, denotando se non altro una limitata comprensione tecno-sociale del problema.

Una seconda considerazione concerne poi la maturità del settore di indagine e la maturità necessaria per avvicinarvisi. Il diritto delle società digitali vanta ormai una pluridecennale tradizione, connotata da una forte componente sovranazionale e comparatistica, che va rispettata: pensare di affrontare il tema dell'AI, o altri di tale ambito, in maniera estemporanea sulla base di qualche generica lettura e conoscenza porta a risultati deboli, che creano talora paradossi, quali quello di presentare come nuove quelle che sono idee già ben note e discusse in passato o, più banalmente, di sposare una visione municipale rispetto ad un dibattito globale di cui si disconoscono protagonisti e temi. Così nel caso dell'AI Act, non può ragionarsi guardando a quanto accade a Bruxelles, sen-

[30] Cfr. art. 60.3, AI Act ("The testing of high-risk AI systems in real world conditions under this Article shall be without prejudice to any ethical review that is required by Union or national law").

za avere in mente quanto contemporaneamente accade a Strasburgo, a Washington o a Brasilia, perché il dibattito e le strategie regolatorie, sia normative sia giurisprudenziali, sono ormai globali in questo ambito.

Un'ultima considerazione concerne poi la scientificità dell'approccio metodologico ai temi dell'AI e del digitale. Troppo spesso si argomenta una malintesa idea di maturità scientifica, secondo cui il civilista dovrebbe distinguersi per una varietà di interessi, dimenticando non solo che importanti studiosi della materia elaborarono chiari indirizzi di ricerca, ma soprattutto che non è più accettata nel panorama scientifico internazionale l'incapacità di indagare con metodo e continuità un dato tema, essendo giustamente considerato segno di debolezza l'andare da un tema all'altro senza sviluppare un'approfondita linea di ricerca che, per sua natura, richiede anni di studio ed elaborazione.

È quindi da auspicarsi che l'AI Act sia l'occasione per rafforzare le fila dei giovani civilisti dediti ai temi del diritto dell'informazione e dell'informatica, evitando di costringere molti di essi a migrare in altri Paesi con maggiori aperture metodologiche, e dando un contributo di profilo alto ma allo stesso tempo concreto al dibattito giuridico ed alla regolamentazione dell'AI, secondo quella che è storicamente la funzione dell'università, luogo di riflessione per lo sviluppo della società.

Abstract

Qual è la visione del legislatore europeo nel regolare l'intelligenza artificiale? Qual è la rilevanza dell'adozione di un paradigma incentrato sul rischio? In che modo tale paradigma interseca la dimensione dei diritti fondamentali? Questi sono i principali quesiti a cui intende rispondere una prima disamina dell'AI Act, mettendo in luce come occorra un approccio interdisciplinare e rivolto anche agli scenari internazionale e di altri Paesi per cogliere in maniera completa le dinamiche che hanno ispirato il legislatore europeo e guideranno l'implementazione dell'AI Act.

What is the European legislator's vision for the regulation of AI? What is the relevance of adopting a risk-based approach? How does this approach intersect with the fundamental rights dimension? These are the main questions that this initial analysis of the AI Act aims to answer, highlighting the need for a multidisciplinary approach that also looks at the international scenario and other countries in order to fully understand the dynamics that have inspired the European legislator and will guide the implementation of the AI Act.