IL RUOLO DELLO STATO NELL'ETÀ DELLA TECNICA E LE SFIDE DELL'INTELLIGENZA ARTIFICIALE*

di Daniela Mone**

Sommario. 1. Introduzione. – 2. Lo Stato nell'età della tecnica. Le sfide dell'Intelligenza Artificiale: coordinate dell'analisi. – 3. Le ragioni dell'interventismo europeo. – 4. Sui profili critici dell'*AI Act*. – 4.1. I conflitti di interesse. – 4.2. Le questioni del regolamento «generico» e della debolezza dei controlli ed il ruolo dei privati. – 4.3. La tutela sostanziale dei diritti apprestata dall'*AI Act*. – 5. Qualche considerazione di sintesi su un tema in continua evoluzione.

1. Lo Stato nell'età della tecnica. Le sfide dell'Intelligenza Artificiale: coordinate dell'analisi. Gli scritti raccolti nel numero speciale 1, 2026 della rivista *Diritto Pubblico Europeo - Rassegna Online*, dal titolo Lo Stato nell'età della tecnica, rappresentano approfondimenti degli interventi che diversi studiosi hanno tenuto nell'ambito della VI Conferenza annuale di ICON-S Italy «Lo Stato *vis à vis* i poteri economici e privati nell'era digitale», svoltasi presso l'Università di Cagliari, il 3-4 ottobre 2025. Tali interventi e, quindi i contributi che ne sono il precipitato, sono attraversati da un *fil rouge* comune, in quanto ciascuno dei rispettivi Autori ha partecipato alla suddetta Conferenza come componente di una cordata originariamente composta da sette panels, in ognuno dei quali si guarda al ruolo dello Stato nell'età della tecnica sotto uno specifico profilo: dalle dinamiche trasformative della forma di governo alla sicurezza, dai diritti sociali alle future generazioni, dalla partecipazione, democrazia e informazione alla transizione ecologica e all'Intelligenza Artificiale.

La dimensione tecnologica in cui oggi operano gli Stati, invero, ha inciso in modo decisivo sulle funzioni tradizionalmente loro proprie, sui rischi che gli stessi sono chiamati ad affrontare nonché sulle modalità per la risoluzione delle nuove ma anche delle perduranti esigenze che attraversano le società contemporanee.

Così è intuitivo il rilievo della tecnica nell'ambito della cd. transizione ecologica dello Stato, atteso che la riconversione delle attività umane verso modelli sostenibili a fini di riduzione dell'inquinamento e del riscaldamento globale, trova in essa la leva essenziale. L'emergenza ambientale è, di fatto, oggi una questione globale, cui vengono associati scenari di «catastrofe ecologica» ed ha portato le istituzioni pubbliche, ad ogni livello, a impegnarsi per una transizione ecologica, appunto, che possa scongiurarla. Non è casuale, in tale prospettiva, la modifica, con la l. cost. n. 1/2022, «la quale, per la prima volta nell'esperienza repubblicana, ha modificato un principio fondamentale», di un articolo ricompreso fra i principi fondamentali e dell'art. 41 Cost., per introdurre esplicitamente la «tutela dell'ambiente,

* *Sottoposto a referaggio*.

** Professoressa Associata di Diritto costituzionale e pubblico – Università della Campania Luigi Vanvitelli.

dell'ecosistema e della biodiversità» ed i «fini ambientali». La positivizzazione della stessa rappresenta, infatti, il punto di arrivo di un processo che culmina con il suo accoglimento fra i principi costituzionali, a testimonianza della rilevanza acquisita dal tema nella società contemporanea. Il rapporto fra tecnica e transizione ecologica è stato affrontato, sotto svariati profili, nel panel coordinato da Alfonso Vuolo: dall'impatto delle valutazioni tecnico-scientifiche su clima e ambiente sulle scelte politiche e sulla giurisprudenza al rapporto fra salvaguardia degli equilibri ambientali e la solidarietà ed uguaglianza anche nella loro dimensione transgenerazionale.

È proprio quest'ultimo profilo, quello della dimensione transgenerazionale, a rappresentare il tema specifico del panel coordinato da Francesco Paterniti. In tale sezione, i contributi analizzano gli effetti della tecnica sulla percezione e rappresentazione di futuro disvelandone, paradossalmente, a fronte di una sua tradizionale interpretazione in termini di progresso, l'idea di uno spazio di radicale incertezza. Tutto sembra possibile ma non sapendosi con certezza quali saranno le conseguenze delle azioni attuali, non è dato neanche sapere se ne deriveranno vantaggi o rischi per la persona. Ed emerge, quindi, prepotentemente, il tema, di grande rilevanza giuridica, della responsabilità degli effetti delle decisioni assunte oggi sulle generazioni di domani. È urgente, in tale scenario, riflettere sulle modalità attraverso cui le decisioni politiche, con contenuto tecnologico, possano essere guidate da principi che garantiscano il benessere delle generazioni future. Si tratta di un'istanza che, in primo luogo, «impone una revisione, o quanto meno un ripensamento, delle categorie fondamentali della teoria della Costituzione, prestando particolare attenzione alla relazione tra normatività e temporalità», tenendo conto che, considerata la rigidità costituzionale e la limitazione delle procedure di revisione, «l'orientamento al futuro del costituzionalismo emerge non come opzione contingente, ma come carattere strutturale dell'esperienza costituzionale, legato alla funzione di stabilizzazione delle aspettative normative e alla necessità di assicurare la continuità dell'ordine giuridico» (Paterniti). Ciò non vuol dire anche che la Costituzione introduca una sorta di «gerarchia temporale fra generazioni» (Paterniti), limitando la libertà politica delle generazioni contemporanee, ma che, «in un'ottica di reciprocità normativa tra generazioni, della stessa rigidità deve essere colta la capacità di garantire la trasmissibilità dei diritti fondamentali e la sostenibilità delle scelte collettive» (Paterniti).

La sicurezza è un ulteriore angolo visuale attraverso il quale si può indagare l'incidenza del progresso tecnologico sulle funzioni statali, in particolare sulla capacità dello Stato di preservarla. Tale tematica è affrontata nel panel coordinato da Giuseppe Laneve. Ebbene, la tecnica può contribuire a salvaguardare la sicurezza, ad esempio, quella energetica, nell'ambito della relativa transizione, garantendo autonomia del Paese nonché la «continuità, o addirittura [per] la sopravvivenza stessa, della vita sociale, economica e democratica degli ordinamenti» (Laneve).

Ma la tecnica può anche insidiare la sicurezza, sol che si consideri l'invasività delle tecnologie «fino agli strati più profondi della mente» rendendo necessario «perimetrare e difendere uno spazio di sicurezza del pensiero» «vitale per l'individuo ma altresì per la tenuta del sistema democratico» (Laneve). O ancora i rischi possono essere legati alla sfera individuale o sociale della persona, quando la tecnica potrebbe minare la sua sfera privata e la sua partecipazione alla vita comunitaria.

L'impatto della tecnologia sui diritti sociali è oggetto di approfondimento del panel introdotto da Marcello Salerno. La questione, invero, può essere approfondita partendo dall'interrogativo «sul confine tra ciò che il legislatore può o deve liberamente consentire e ciò che, invece, può o deve tradursi in ruolo attivo dell'ordinamento, in prestazioni sociali da garantire» (Salerno) nell'età della tecnica. I contributi sviluppati nell'ambito della sessione, partendo dal «principio di uguaglianza sostanziale […] come criterio di legittimità

Issn 2421-0528

costituzionale degli interventi pubblici e come parametro di giudizio sulle omissioni del legislatore», analizzano il tema della povertà energetica, rispetto alla quale «[…] diviene fondamentale l'intervento legislativo statale che riconduca nel quadro dei livelli essenziali delle prestazioni (LEP) anche i diritti energetici in modo da fissare una soglia uniforme di «povertà energetica» al di sotto della quale non è possibile scendere»; quello della transizione digitale del sistema sanitario rispetto al quale, parimenti, si ritiene che «le prestazioni sanitarie digitali rientrano a pieno titolo nel perimetro dei livelli essenziali delle prestazioni e, in particolare, dei livelli essenziali di assistenza (LEA) che, anche in questo caso, diventano la declinazione più concreta e sostanziale dell'eguaglianza» (Salerno); il tema del fine vita, dove la questione dell'uguaglianza assume rilevanza in ordine alle condizioni di accesso alle procedure medicalmente assistite e ai rischi della differenziazione territoriale in mancanza di una disciplina omogenea sul territorio nazionale.

L'impatto della tecnica non risparmia la dimensione democratica dello Stato. La diffusione delle nuove tecnologie, invero, è potenzialmente idonea a migliorarla, ampliando, in generale, le modalità partecipative in un'epoca contrassegnata da profonda «crisi dei circuiti rappresentativi classici» (Troisi) ma può anche minarne le fondamenta, configurandosi, in corrispondenza del loro utilizzo, rischi di accentuazione di disuguaglianze cognitive e di amplificazione della disinformazione. Contestualmente alla crisi partitica e di forme tradizionali della partecipazione politica si assiste, infatti, alla tendenza sempre più imponente a «spinte isolazionistiche che hanno travolto la capacità di dialogo dei partiti come arma per l'intercettazione del consenso» proprio per effetto della diffusione delle nuove tecnologie digitali (Troisi). D'altra parte, si «registra al contempo la volontà degli elettori di riappropriarsi di idonei strumenti di partecipazione che, pur senza eliminare il ruolo dei partiti, consentano di rendere effettiva la sovranità popolare» (Troisi). Le nuove tecnologie hanno un ruolo decisivo anche in tale ambito, sebbene i rischi che producono sulla democrazia partecipativa sono tali da metterne in discussione addirittura l'essenza. Su tali problematiche si sono soffermati i contributi del panel coordinato da Michele Troisi.

Gli stessi rapporti tra organi, intesi quali soggetti qualificanti la forma di governo, sono incisi dal progresso tecnologico che, da un lato, ha marginalizzato i partiti politici a vantaggio dell'emersione di leader e, parallelamente, le assemblee a vantaggio degli esecutivi (Ferraiuolo), dall'altro, gli esecutivi (ed il capo) «rispetto a valutazioni che vengono ascritte alla dimensione tecnica, e rimesse dunque ad organismi che dovrebbero assicurarne una pretesa oggettività» (Ferraiuolo). La «spinta all'immediatezza» sollecitata dalle tecnologie, incide, altresì, «nella relazione spaziale governanti-governati» e «sul piano temporale», con l'abbandono di strategie di «medio-lungo periodo sganciate dal qui ed ora» e l'acquisizione di modalità da «campagna elettorale permanente». Gli approfondimenti sviluppati nello specifico panel coordinato da Gennaro Ferraiuolo, attengono al «rapporto tra media online e politica alla luce dei cambiamenti del principio di rappresentanza indotti dalla personalizzazione dei flussi informativi», alla «governabilità da garantire attraverso una sorta di tecnica algoritmica», al ruolo della tecnica nel PNRR e nella giurisprudenza costituzionale.

2. Lo Stato nell'età della tecnica. Le sfide dell'Intelligenza Artificiale: coordinate dell'analisi. Il settimo panel previsto, da me coordinato, era dedicato alle sfide dell'Intelligenza Artificiale. Poiché, per motivazioni connesse all'allora situazione geopolitica[1], la maggior parte degli aderenti non tenne la propria relazione e, quindi, il lettore non troverà pubblicazioni relative a quella sezione, intendo qui tratteggiare i profili più rilevanti connessi ad un tema tanto delicato quanto attuale.

[1] In adesione allo sciopero previsto per quel giorno in solidarietà con la popolazione palestinese.

L'Intelligenza Artificiale[2], la più potente e pervasiva delle tecnologie digitali del mondo contemporaneo, incide in modo significativo sul ruolo e, soprattutto, sul funzionamento dello Stato nel raggiungimento degli scopi che gli sono propri nell'ambito del costituzionalismo. I rischi cui la tenuta democratica dell'ordinamento[3] è sottoposta sono innegabili e intuitivi e, purtroppo, mentre taluni seppur ineliminabili in radice, risultano mitigabili e, perciò, ammissibili, altri sono inaccettabili per il loro potenziale impatto sui diritti fondamentali. Eppure, le opportunità che offrono lo sviluppo e l'utilizzo dell'IA sono altrettanto indiscutibili ed irrinunciabili, sia in termini di miglioramento potenziale della stessa tenuta democratica dello Stato, sia in termini di soddisfacimento dei diritti fondamentali della persona.

Non si può fermare il progresso, né è razionale rinunciare ai sicuri benefici dello stesso[4]. È quindi ragionevole correre rischi accettabili o resi tali da ogni possibile attività finalizzata a mitigarli, a partire dalla diffusione della consapevolezza, con i potenziali benefici che ne deriveranno, che ci si trova di fronte ad una tecnologia capace di cambiare «lo stesso senso dell'uomo», incidendo sulla sua dignità, come Papa Leone XIV ha affermato con forza nell'Enciclica Magnifica Humanitas dello scorso 15 maggio[5].

Il reg. UE n. 1689/2024[6], ad applicazione progressiva ed integralmente in vigore a partire dal 2027[7], si propone di regolamentare l'utilizzo dell'IA promuovendo «la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile» [8], ossia funzionale allo sviluppo

---

[2] D'ora in poi anche IA.

[3] Sull'impatto dei poteri digitali sulla democrazia, nettissimo il pensiero di A. Simoncini, *Potere cibernetico e futuro del diritto costituzionale*, in *Quad. cost.*, 1, 2026, 39: «[…] è chiaro che oggi i soggetti socialmente, economicamente e politicamente più potenti, cioè più capaci di interferire unilateralmente con la nostra libertà, siano proprio quelli che – altrettanto genericamente – definiremo poteri digitali».

[4] M. Corradino, *Potere pubblico e intelligenza artificiale*, in A. F. Uricchio, C. Caldarola (a cura di), *L'intelligenza artificiale tra regolazione e esperienze applicative AI ACT (regolamento UE) e disegno di legge governativo*, Bari, 2025, 48-49.

[5] Lettera Enciclica *Magnifica Humanitas* del Santo Padre Leone XIV *sulla custodia della persona umana nel tempo dell'intelligenza artificiale*, 15 maggio 2026. Il Papa ricorda che la dignità umana è una dignità ontologica che spetta in quanto tale ad ogni uomo e non in relazione alle sue capacità o al suo valore: «[…] la dignità fondamentale di ogni persona non si acquisisce e non si merita, né ha bisogno di essere dimostrata». Le ideologie transumaniste e postumaniste, concependo l'uomo come «materiale da perfezionare» ed il progresso come superamento dell'umano, rischiano, invece, di legittimare la svalutazione dei soggetti più fragili e l'idea di «sacrifici necessari» all'ottimizzazione della specie. Per scongiurare tale rischio, occorre integrare le tecnologie in una visione umana e relazionale, evitando che le conquiste scientifiche, svincolate dal progresso morale e sociale, finiscano per rivolgersi contro l'uomo.

[6] Regolamento (UE) n. 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) n. 2018/858, (UE) 2018/1139 e (UE) n. 2019/2144 e le direttive n. 2014/90/UE, (UE) 2016/797 e (UE) n. 2020/1828 (*Regolamento sull'intelligenza artificiale*), d'ora in poi anche *AI Act* o Regolamento.

[7] Il 16 giugno 2026, il Parlamento europeo ha approvato in via definitiva la proposta di regolamento che modifica alcune norme dell'*AI Act*, nell'ambito del pacchetto normativo cd. «*Omnibus digitale*». Quanto alla sua applicazione, in particolare, «gli obblighi per i sistemi di IA ad alto rischio si applicheranno (in modifica dell'art. 113, lett. c) dell'*AI Act*): dal 02 dicembre 2027 per i sistemi di IA indipendenti ad alto rischio; dal 02 agosto 2028 per i sistemi di IA integrati come componenti di sicurezza e disciplinati dalla normativa settoriale UE sulla sicurezza e sulla vigilanza del mercato» (*Le modifiche all'AI Act approvate in via definitiva dal Parlamento UE*, in *dirittobancario.it*)

[8] Reg. UE n. 1689/2024, art.1, par.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».

della persona umana[9], in piena coerenza col principio personalista[10] che permea la nostra Carta costituzionale[11].

La strategia elaborata dal Legislatore europeo, al fine di conciliare sviluppo e diffusione dell'innovazione e tutela dei diritti, è, nel rispetto dei principi di proporzionalità[12] e di sussidiarietà[13], di rifuggire da un approccio interdittivo e, soprattutto, uniforme rispetto all'utilizzo dell'IA e di adottarne, invece, uno differenziato a seconda del rischio ad esso connesso, «prudenziale»[14].

Per i sistemi il cui utilizzo presenta un rischio inaccettabile è sancito, dunque, il divieto[15]; in corrispondenza di un rischio elevato, è previsto l'obbligo di conformità a requisiti specifici; ove il rischio associato sia limitato o minimo è previsto il rispetto di requisiti più leggeri e facoltativi[16].

[9] P. Benanti, S. Maffettone, *Noi e la macchina. Un'etica per l'era digitale*, LUISS University Press, 2024, 10-11, parlano di necessità di «umanizzare la tecnica» impedendo che questa possa «macchinizzare l'uomo». Per gli A. «è urgente poter riportare al centro dei processi di *decision making* non solo le tecniche ma anche tutta una serie di dimensioni antropologiche ed etiche. C'è bisogno di una nuova *agorà* ove tornare a rendere possibile la convivenza umana in una stagione in cui l'automatizzazione e la decisione algoritmica rischiano di rimpiazzare l'umano e le strutture valoriali della nostra convivenza sociale» (12).

[10] In tal senso A. Iannuzzi, *L'AI Act nell'ecosistema normativo europeo in tema di digitale tra continuità e discontinuità,* in *BioLaw Journal –Rivista di BioDiritto*, 3, 2025, 253, in riferimento al diritto all'intervento umano previsto dall'art. 22, par. 3, del GDPR, poi ripreso dall'*AI Act* con la supervisione umana (art. 14).

[11] L'impostazione antropocentrica della disciplina europea dell'IA la pone nel solco della tradizione costituzionale europea e in coerenza con la Costituzione italiana fondata sul principio personalista che «in realtà non è un «principio» al pari degli altri che pure sono a fondamento dell'ordine repubblicano; semmai, è il principio, come ciò che sta appunto all'inizio e, a un tempo, alla fine del percorso costituzionale»: così A. Ruggeri, *Il principio personalista e le sue proiezioni*, in *Federalismi.it*, 28 agosto 2013, 3. In tale prospettiva, O. Pollicino, *AI Act e sovranità normativa: la strategia europea sull'intelligenza artificiale*, in *Agendadigitale.eu*, marzo 2026, 242, vede nell'inclusione tra gli usi vietati dei sistemi di manipolazione comportamentale e di classificazione biometrica non una scelta meramente tecnica ma la conferma di un principio fondamentale della tradizione europea: la persona non può essere ridotta a oggetto di calcolo algoritmico. L'*AI Act*, cioè, traduce la tutela della dignità in divieti concreti, ponendo un limite alla logica dell'efficienza e del profitto.

[12] Per G. De Minico, E. Palomba, M. Parente*, AI Act e Legge italiana sull'Intelligenza artificiale: un'armonizzazione "fin troppo perfetta"*, in *Lecostituzionaliste.it*, 20 dicembre 2025, 1, «L'*AI Act* adotta una prospettiva antropocentrica che classifica i sistemi di IA in base al rischio per i diritti fondamentali dei destinatari (pratiche di IA inaccettabili, sistemi di IA ad alto rischio, sistemi di IA a basso e minimo rischio), modulando le regole ad essi applicabili secondo il canone della proporzionalità».

[12] Per G. De Minico, E. Palomba, M. Parente*, AI Act e Legge italiana sull'Intelligenza artificiale: un'armonizzazione "fin troppo perfetta"*, in *Lecostituzionaliste.it*, 20 dicembre 2025, 1, «L'*AI Act* adotta una prospettiva antropocentrica che classifica i sistemi di IA in base al rischio per i diritti fondamentali dei destinatari (pratiche di IA inaccettabili, sistemi di IA ad alto rischio, sistemi di IA a basso e minimo rischio), modulando le regole ad essi applicabili secondo il canone della proporzionalità».

[13] Come ben precisa M. Carta, *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, in *rivista.eurojus.it*, 3, 2024, 198: «Il principio di sussidiarietà svolge una funzione limitata nel settore, per cui la motivazione dell'atto di ravvicinamento è assorbita dalla stessa esigenza di superare le divergenze tra le legislazioni degli Stati membri, elemento questo del tutto evidente anche nel regolamento sull'AI».

[14] Così F. Gallo, *Cyberspazio, diritti e tutele*, in A. F. Uricchio, C. Caldarola (a cura di), *L'intelligenza artificiale tra regolazione e esperienze applicative AI ACT (regolamento UE) e disegno di legge governativo*, Bari, 2025, 17.

[15] Sono vietate le pratiche di IA, connesse ad un rischio inaccettabile, indicate nell'art. 5.

[16] C. Caldarola, *L'AI ACT: il nuovo regolamento europeo sull'intelligenza artificiale - Un'analisi di impatti e prospettive*, in A. F. Uricchio, C. Caldarola (a cura di), *L'intelligenza artificiale*, cit., 89. Per O. Pollicino, *Possiamo affermare che l'AI Act sia parte integrante del digital constitutionalism?*, in *BioLaw Journal –Rivista di BioDiritto*, 3, 2025, 241, con l'AI Act si registra un «cambio di paradigma che segna il passaggio da un costituzionalismo fondato sul bilanciamento assiologico a uno fondato sulla gestione del rischio». In argomento v. anche F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'Intelligenza Artificiale*, in *Il Diritto dell'Unione Europea*, 3-4, 2021, 453-465 ss.; V. D'Antino, *L'approccio basato sul rischio nell'AI Act: un nuovo paradigma di regolazione dell'intelligenza artificiale*, in *Federalismi.it*, 2 luglio 2025, 19.

L'approccio prescelto è definito *risk-based* ed è contraddistinto dalla finalità di garantire lo sviluppo dell'innovazione, ossia dell'IA, nel rispetto dei diritti fondamentali. La tutela dei diritti fondamentali, dunque, non è la finalità prioritaria né tantomeno esclusiva della regolazione[17]. L'Europa, infatti, non ha optato per un'impostazione *rights-based* ma ha approvato una «normativa industriale e di mercato che mira a garantire la sicurezza dei prodotti tecnologici»[18]. E la sicurezza è funzionale a sostenere l'innovazione e promuovere lo sviluppo del corrispondente mercato.

La produzione di regole efficaci, infatti, si propone di trasmettere fiducia agli utenti di IA, riducendo al minimo i rischi derivanti dal suo impiego, proprio allo scopo di promuovere lo sviluppo del mercato relativo a questa tecnologia[19]. Parimenti, attraverso la loro chiarezza, l'UE si prefigge di agevolare la *compliance* dei produttori alle regole che, contestualmente, li metta al riparo da sanzioni e ne stimoli gli investimenti, garantendo lo sviluppo del settore[20]. L'efficacia di un tale approccio, opposto a quello statunitense incentrato su una pressocché totale *self-regulation* e diverso da quello cinese, volto a disciplinare l'impiego delle tecnologie digitali a fini di sorveglianza[21], condivisibile per la sua coerenza rispetto al costituzionalismo, andrà apprezzata sul piano sostanziale, anche alla luce di eventuali revisioni[22]. Esse, da un lato, sono indotte da richieste statunitensi, talora inaccoglibili e inaccettabili, suscettibili di porsi in contrasto con il cd. *Brussels effect*, dall'altro, sollecitate dallo stesso Mario Draghi in diverse occasioni, tra cui la presentazione alla Commissione, il 9 settembre 2024, del Rapporto sul futuro della competitività europea[23], in considerazione degli effetti negativi che l'*over-regulation* potrebbe determinare sulla competitività delle imprese del vecchio continente e lo sviluppo dell'innovazione nello spazio UE[24].

Ulteriori interventi di revisione risultano, peraltro, auspicabili alla luce delle valutazioni

[17] A. Simoncini, *Potere cibernetico*, cit., 50, parla di Europa orientata a «*twin objectives*: promuovere la crescita economica attraverso lo sviluppo tecnologico e, al tempo stesso, mantenere un elevato livello di protezione dei diritti fondamentali».

[18] In tal senso, ancora A. Simoncini, *AI Act e digital constitutionalism,* in *BioLaw Journal –Rivista di BioDiritto*, 3, 2025, 237: «L'*AI Act* […] non nasce come strumento orientato alla tutela dei diritti, ma come normativa industriale e di mercato che mira a garantire la sicurezza dei prodotti tecnologici. Non è uno strumento *right-based*, ma *risk-based*». Parzialmente differente la posizione di F. Donati, *La protezione dei diritti fondamentali nel Regolamento sull'intelligenza artificiale*, in *rivistaaic.it*, 1, 2025, 5 ss., per il quale l'Europa ha seguito un modello *«rights-driven»*.

[19] C. Caldarola, *L'AI Act*, cit., 90-91, sottolinea il ruolo della regolazione a garanzia della sicurezza dell'IA come stimolo all'innovazione. Ancora sul concetto di fiducia che con l'*AI Act* l'UE vuole trasmettere ai cittadini nell'utilizzo di un'IA affidabile, R. Razzante, *AI Act: misure per sostenere l'innovazione,* in A. F. Uricchio, C. Caldarola (a cura di), *L'intelligenza artificiale*, cit., 129.

[20] C. Caldarola, *L'AI Act*, cit., 88, 90. In tal senso V. D'Antino, *L'approccio basato sul rischio nell'AI Act*, cit., 16, parla di «approccio europeo all'IA, imperniato sull'eccellenza e sulla fiducia […]».

[21] C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di Intelligenza Artificiale*, in *BioLaw Journal,* 3, 2021, 417, a proposito dell'approccio statunitense orientato alla *self- regulation*, segnalano comunque, la previsione, a livello di singoli Stati e città, di discipline e parziali divieti relativi ad usi dell'IA. A. Simoncini, *Potere cibernetico*, cit., 49-50, osserva che, in effetti, con la seconda Amministrazione Trump, anche gli USA aderiscono alla dottrina della cd. «sovranità digitale», ritenendo l'IA «un asset strategico per raggiungere la superiorità americana nel mercato globale» per cui «la produzione e lo sviluppo dell'IA (principalmente per scopi militari) devono essenzialmente rimanere un interesse nazionale federale, anche a scapito delle legislazioni statali».

[22] V. nota 8.

[23] *The Draghi report: A competitiveness strategy for Europe* in *https://commission.europa.eu/topics/competitiveness/draghi-report_en#paragraph_47059,* in particolare, 30. Tali preoccupazioni sono state ribadite in ulteriori diverse occasioni. V., da ultimo, l'intervento di Mario Draghi al Politecnico di Milano, il 1 dicembre 2025, fruibile al link *https://www.polimi.it/il-politecnico/news/dettaglio-news/inaugurazione-163-anno-accademico.*

[24] V. C. Casonato, *AI Act: un dialogomultidisciplinare.Introduzione,* in *BioLaw Journal –Rivista di BioDiritto,* 3, 2025, 227.

critiche emerse con riguardo ai diversi profili specifici della disciplina.
È chiaro che la valutazione della normativa sarà positiva se non ne risulteranno oneri eccessivamente pesanti per la competitività dell'industria europea al punto da pregiudicare l'innovazione e bloccare lo sviluppo dell'IA ma parallelamente, un'eventuale revisione sarà condivisibile, se attraverso la riduzione di tali oneri e l'eventuale modifica di talune previsioni adottate, la stessa non legittimerà rischi inaccettabili di violazione dei diritti fondamentali a beneficio dei produttori. I diritti fondamentali, in altri termini, dovranno essere oggetto di tutela sostanziale attraverso misure effettivamente in grado di ricondurre l'IA al governo dell'uomo, a garanzia della sua dignità.
Solo così, delineando una cornice giuridica alla tecnica[25], assicurando l'individuazione delle responsabilità per decisioni della macchina impattanti sulle persone e, ancor prima, fissando *ex ante* l'etica tanto nella progettazione che nel funzionamento del sistema di Intelligenza Artificiale[26], non si tradirà il costituzionalismo.

3. Le ragioni dell'interventismo europeo. L'interventismo europeo in materia di Intelligenza Artificiale risponde, dunque, all'esigenza di bilanciare lo sviluppo e l'utilizzo dei sistemi di IA con la salvaguardia dei diritti fondamentali, esposti a gravi rischi in caso di impiego non adeguatamente regolato[27].
Evidentemente la diffusione di una tecnologia pervasiva quale l'IA e, ancor più la sua forma generativa[28] che si sottrae all'effettivo controllo dell'uomo, può impattare fortemente sulla dignità e sui diritti fondamentali della persona[29], quindi sulla tenuta democratica delle istituzioni, esponendoli a rischi di pregiudizio.
L'AI Act, come si è detto, si propone di regolare in modo rigoroso i sistemi di IA, cd. ad alto rischio, al fine di ridurre il più possibile le probabilità che gli eventi dannosi potenzialmente

[25] La riflessione di N. Irti, *Tecnocrazia e politica povera, che dualismo!*, in *il Sole 24 Ore*, 1 marzo, 2026, sul punto, invero non lascia affatto ben sperare. L'insigne giurista, conclude il suo intervento con parole piene di amarezza: «Se la tecnocrazia, disdegnosa della politica, è come racchiusa in esercizi di logica finanziaria o vagheggianti utopie di funzionalità economica, sta, dall'altro lato, la povertà culturale dei ceti politici, che quasi per ventura si trovino detentori del potere. Questo è il dualismo in cui si lacera la storia del nostro tempo».
[26]Come avverte il Papa, infatti, nella citata Enciclica *Magnifica Humanitas*, 19: «[…] non possiamo considerare l'IA moralmente neutra». In ogni sistema sono incorporate scelte, priorità e una determinata concezione della persona e della società, per cui la valutazione etica non può riguardare soltanto le finalità d'uso, ma deve estendersi anche alla sua progettazione ed ai criteri inscritti nei dati e nei modelli che lo guidano. In tale prospettiva, «Il punto critico, alla luce della Dottrina sociale della Chiesa, non è l'uso della tecnica in quanto tale, ma la visione che vi soggiace» (21).
[27] Sul punto sempre fondamentali le pagine di A. Barbera, *Art. 2,* in G. Branca (a cura di), *Commentario della Costituzione italiana*, Bologna, 1975, *passim*, circa la necessità di collegare, ai diritti di libertà, «istituzioni» che li rendano effettivi. Di recente in argomento, con riferimento alla tutela dei diritti nel mondo digitale, C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quad. cost.*, 3, 2023.
[28] «L'intelligenza artificiale generativa rappresenta una delle frontiere più avanzate dell'IA, distinguendosi per la sua capacità non solo di analizzare dati esistenti ma di creare contenuti completamente originali. A differenza dell'analisi tradizionale, l'IA generativa utilizza algoritmi di apprendimento automatico, in particolare reti neurali profonde come le GAN (*Generative Adversarial Networks*) e modelli di trasformazione come il Transformer utilizzato in GPT, per generare testi, immagini, video o audio che prima non esistevano. Questa tecnologia si basa su modelli di apprendimento che contengono un vasto numero di informazioni, i cosiddetti "modelli di base", fondamentali per consentire l'addestramento e il funzionamento delle tecnologie di IA generativa» (*https://www.agendadigitale.eu/tag/intelligenza-artificiale-generativa/*).
[29] In tal senso papa Leone XIV, nell'Enciclica *Magnifica Humanitas*, p. 3, ricorda con le parole di Benedetto XVI quanto la tecnica sia «fatto profondamente umano, legato all'autonomia e alla libertà dell'uomo» e nello stesso tempo, con le parole di Francesco, quanto mai come con la tecnica di oggi, «l'umanità ha avuto tanto potere su se stessa».

connessi al loro utilizzo[30] si verifichino e da rendere accettabili i rischi residui[31]: mai lesivi della dignità[32], valore che connota il reg. UE n. 1689/2024, riconducendolo così al costituzionalismo digitale[33].

Si tratta, dunque, di una regolazione, fondamentalmente e comprensibilmente, di natura preventiva.

Oggetto di interesse, in queste pagine, sarà la disciplina dei sistemi di IA «ad alto rischio» e quindi il complesso di adempimenti previsti relativi «all'utilizzo dei dati, alla trasparenza, alla supervisione umana e alla cybersicurezza»[34], ferma restando la rilevanza delle disposizioni relative all'uso di IA cui corrisponde un rischio inaccettabile o, invece, basso o nullo («sistemi di IA, diversi dai sistemi di IA ad alto rischio», art. 95, reg. UE n.1689/2024), non fosse altro che in relazione ai criteri utilizzati per ascrivere un sistema all'una o all'altra categoria[35].

Si consideri, in tale prospettiva, anche la possibilità, di cui all'art. 6, par. 3, del Regolamento, che un sistema di IA, pur rientrante tra le ipotesi elencate nell'Allegato III, non sia ritenuto ad alto rischio ove non presenti un rischio significativo per la salute, la sicurezza o i diritti fondamentali, anche in ragione della sua mancata incidenza materiale sull'esito del processo decisionale. Ora, è vero che l'art. 80 consente all'autorità di vigilanza del mercato di intervenire qualora ritenga erronea tale classificazione. Tuttavia, tale intervento resta eventuale, tendenzialmente successivo e subordinato all'attivazione del controllo pubblico. Ne deriva che la qualificazione iniziale del sistema, rimessa in larga misura al *provider*, produca effetti rilevanti sul regime applicabile prima di un'effettiva verifica esterna[36].

Quanto ai sistemi di IA ad alto rischio, l'art. 6 dell'*AI Act*, in combinato disposto con gli Allegati I e III, delinea il perimetro della categoria. Occorre, tuttavia, considerare anche le previsioni relative ai modelli di IA per finalità generali, inclusi quelli con rischio sistemico: essi non sono, in quanto tali, sistemi ad alto rischio, ma possono rientrare nella categoria quando siano integrati in sistemi destinati ad operare negli ambiti di cui all'art. 6, e segnatamente nei settori indicati dall'Allegato III.

L'*AI Act* considera «ad alto rischio» i sistemi individuati in base a tale articolo ed impiegati

---

[30] La definizione di rischio, ai sensi dell'art. 3, par. 1, punto 1, del reg. UE n. 1689/2024, è: «la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso».

[31] In base all'art. 9, par. 3 del Regolamento, attraverso gli adempimenti previsti per i sistemi cd. ad alto rischio si deve tendere a rendere accettabili i rischi residui nonostante le misure di riduzione ed attenuazione attivate.

[32] Al Considerando 28 del Regolamento viene espressamente considerato il rapporto fra IA e dignità umana. Della centralità della dignità nell'Enciclica *Magnifica Humanitas* di Leone XIV si è detto. Giova qui riportare il passaggio in cui, p. 23, richiamando Giovanni Paolo II, il papa pone la domanda a cui occorre rispondere, in definitiva, quando ci si interroga sull'IA: «l'IA rende la vita umana sulla terra, in ogni suo aspetto "più umana"? La rende più "degna dell'uomo"?» Solo in caso affermativo è perseguibile.

[33] «L'AI Act non può essere letto in isolamento. Esso dialoga con altre normative che insieme compongono l'architettura del *digital constitutionalism* […] Insieme, queste normative non sono frammenti isolati, ma tasselli di un mosaico: un ordinamento digitale europeo che si costruisce passo dopo passo e che riflette la volontà di dare un'anima costituzionale al governo delle tecnologie» (O. Pollicino*, Possiamo affermare che l'AI Act sia parte integrante del digital constitutionalism?*, cit., 243). In tal senso, ancora, l'A., *Ai Act e sovranità normativa*, cit., vede nell'*AI Act*, un cambio di paradigma in Europa, nel campo delle tecnologie digitali, con il quale si mira a orientare lo sviluppo della tecnologia attraverso il diritto, così ridefinendo «i confini della sovranità».

[34] V. D'Antino, *L'approccio basato sul rischio nell'AI Act,* cit., 23-24.

[35] Ad esempio, A. Simoncini, *AI Act e digital constitutionalism,* cit., 238, critica la mancata inclusione, fra le IA vietate, dell'Intelligenza Artificiale Generale (AGI).

[36] Reg. UE n. 1689/2024, art. 80. Procedura per i sistemi di IA classificati dal fornitore come non ad alto rischio in applicazione dell'allegato III «1. Se ha motivi sufficienti per ritenere che un sistema di IA classificato dal fornitore come non ad alto rischio a norma dell'articolo 6, paragrafo 3, sia in realtà ad alto rischio, l'autorità di vigilanza del mercato effettua una valutazione del sistema di IA interessato in relazione alla sua classificazione come sistema di IA ad alto rischio sulla base delle condizioni di cui all'articolo 6, paragrafo 3, e degli orientamenti della Commissione».

nei settori elencati nell'Allegato III: biometrico, delle infrastrutture critiche, istruzione e formazione del personale, lavoro, accesso a servizi essenziali, attività di contrasto, migrazione, asilo e gestione del controllo delle frontiere, amministrazione della giustizia e processi democratici. Per realizzare un'Intelligenza Artificiale realmente antropocentrica, sarà necessario sviluppare e commercializzare sistemi di IA il cui rischio elevato viene sufficientemente attenuato e ridotto grazie agli adempimenti previsti in base al Regolamento.
La riflessione che si propone è volta a mettere in luce alcuni significativi e oggettivi limiti della normativa in esame, inclusa, invero, quella di livello statale, rappresentata, nell'ordinamento italiano, dalla l. n. 132/2025, recante *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, nella prospettiva di individuarne possibili correttivi.
Essa, infatti, poggia sul presupposto che occorra migliorare la disciplina dell'IA e non, invece, superarla in favore di modelli di autoregolazione privata. L'approccio europeo, fondato sulla centralità della persona, sulla tutela dei diritti fondamentali e sulla responsabilità pubblica della regolazione, infatti, sembra rappresentare, allo stato, la via più coerente con i presupposti del costituzionalismo. Al contrario, un arretramento verso forme di *self-regulation* rischierebbe di consegnare a soggetti privati scelte incidenti su libertà, eguaglianza e dignità, in contrasto con l'impianto assiologico delle democrazie costituzionali.

***4. Sui profili critici dell'*Ai Act.** Diverse sono le previsioni del Regolamento, concernenti i sistemi di IA ad alto rischio, che presentano profili critici. Si proverà a tener conto dei più rilevanti, naturalmente senza alcuna pretesa di completezza, per valutarne l'impatto sull'efficacia complessiva della disciplina apprestata rispetto allo scopo dichiarato di garantire la diffusione di un'IA antropocentrica in Europa.

4.1. I conflitti di interesse. In primo luogo, emerge in più punti della regolazione, un ruolo assai incisivo dei regolati (privati) riguardo ad attività da cui dipende, in ultima analisi, l'efficacia sostanziale della disciplina *de qua*, a partire da quello loro riconosciuto nella valutazione della conformità di un sistema di IA ad essa. Tale valutazione, infatti, eccetto che in determinati casi, è fondata su procedure la cui scelta è nella disponibilità del fornitore del sistema stesso, ossia il regolato. Questi, ai fini di detta valutazione, può ricorrere al controllo interno, di cui all'allegato VI, riconducibile esclusivamente a sé o ad un organismo notificato, di cui all'allegato VII[37].
Le preoccupazioni, al riguardo, sono giustificate altresì - e per la stessa ragione, ossia un eventuale possibile conflitto di interessi- laddove si consideri che gli stessi adempimenti il cui rispetto assicura presunzione di conformità di un sistema di IA, sono, di fatto, individuati dai regolati[38].
Tornando alla valutazione della conformità, entrambe le modalità percorribili sopra indicate si prestano, invero, a delle critiche.
Nel primo caso, il controllo appare del tutto autoreferenziale, risultando poco verosimile che il fornitore rilevi difformità rispetto ai requisiti di cui alla sezione 2 del Capo III del Regolamento, precludendosi la possibilità di immissione sul mercato, messa in servizio e uso del sistema[39]; nel secondo, la critica attiene alla natura dell'organismo notificato, un soggetto

[37] Reg. UE n. 1689/2024, art. 43.
[38] Reg. UE n. 1689/2024, art. 40, che rinvia al Reg. UE n. 1025/2012.
[39] F. Donati, *La protezione dei diritti fondamentali nel Regolamento sull'intelligenza artificiale*, cit., 18-19, trova ragionevole affidare la verifica della conformità ai requisiti dell'IA Act ai fornitori dei sistemi ad alto rischio per evitare disfunzioni scaturenti dalla necessità di controllare numerosissimi «sistemi sottoposti a continue modifiche e aggiornamenti», a patto che siano istituite, a livello nazionale, autorità di controllo efficienti, ben preparate ed

sempre privato ed espressione del settore, che viene investito delle sue funzioni dall'autorità di notifica dei diversi Stati, delle quali, peraltro, non viene sancita l'indipendenza dal Governo, ma esclusivamente l'indipendenza funzionale[40].

A monte di tali rilievi emerge – e veniamo al secondo livello di conflittualità- la natura coregolatoria della normativa che i fornitori di sistemi di IA sono tenuti a rispettare: si tratta di norme che, adottate sulla base del reg. UE n. 1025/2012, dovrebbero risultare da una cornice posta dalla Commissione che ne individui il contenuto politico, che connota qualunque norma di armonizzazione, per quanto tecnica, e da regole stabilite da organismi privati di regolazione che, in base all'art. 10 del regolamento citato, la Commissione, nel 2023[41], ha individuato nel CEN e nel CENELEC. Ebbene, la prevalenza rispetto al soggetto pubblico dei privati e, segnatamente dei privati più forti all'interno di tali organismi, sarebbe innegabile e consentita dalle maglie larghe con cui il primo, con le proprie fonti (ossia l'UE, con il regolamento) è intervenuto a ridurre la discrezionalità dei secondi (cioè, i regolati)[42].

Stessa criticità è stata rilevata a proposito dei codici di buone pratiche, di cui all'art. 56[43] che, tuttavia, non riguardano i sistemi di IA ad alto rischio ma i modelli di IA per finalità generali. Questi, ove applicati negli ambiti di cui all'art. 6 (allegati 1 e 3) sono ascrivibili a tale categoria, divenendo destinatari anche della relativa normativa.

L'art. 53, par. 4, attribuisce all'adesione agli stessi da parte di fornitori di sistemi di IA a finalità generale, la presunzione di conformità agli obblighi di cui al suo paragrafo 1, «finché non è pubblicata una norma armonizzata». La conformità alle norme armonizzate europee, una volta approvate, garantirà ai fornitori «la presunzione di conformità nella misura in cui tali norme contemplano tali obblighi»[44]. L'adesione ai codici, peraltro, è volontaria, sebbene chiaramente incentivata, dal momento che i fornitori possono anche dimostrare «mezzi alternativi adeguati di conformità ai fini di approvazione da parte della Commissione»[45]. Lo stesso vale, ai sensi dell'art. 55, per i fornitori di modelli di IA a finalità generale con rischio

indipendenti. Posizione diversa è sostenuta da G. De Minico, E. Palomba, M. Parente*, AI Act e Legge italiana,* cit., su cui vedi nota successiva.

[40] Si tratta di un ulteriore profilo critico della regolazione ai sensi dell'art. 70 del Regolamento, che, come evidenziato da G. De Minico, E. Palomba, M. Parente*, AI Act e Legge italiana,* cit., 3, a differenza dell'originario art. 59, par. 4-*bis* non sancisce una rigorosa indipendenza «genetica e funzionale dai rispettivi Esecutivi nazionali». Sulla base di tale previsione europea, la l. n. 132/2025, ha potuto individuare quali autorità nazionali per l'Intelligenza artificiale, quindi anche quali autorità di notifica, due Agenzie governative già esistenti, l'Agid (Agenzia per l'Italia digitale) e l'ACN (Agenzia per la cybersicurezza nazionale) che, da un lato, dipendendo dal Governo, contribuiscono al processo di accentramento in seno alla Presidenza del Consiglio delle scelte strategiche in materia, esponendole alla mutevolezza dell'organo; dall'altro, essendo anche la PA utilizzatrice dei sistemi IA, non garantiscono obiettività del suo controllo (4).

[41] Commissione europea, Decisione di esecuzione C (2023) 3215, 22 maggio 2023, in *ec.europa.eu*.

[42] G. De Minico, *Le fonti del diritto: un argine all'intelligenza artificiale?*, in *Rivista AIC*, 3, 2025, 87. M. Tuozzo, *Le fonti della società digitale: potenzialità e limiti dei nuovi paradigmi di normatività*, in *DPE Rassegna online*, 2, 2025, 416-417, rileva che «Pur inscrivendosi [l'*AI Act*] in una cornice di *hard law*» e introducendo «una significativa via di fuga attraverso la normazione tecnica prevista dall'art. 4» tuttavia, attraverso il ricorso alla procedura delineata nel Reg. (UE)n. 1025/2012, «mette in luce una forma di coregolazione, in cui la partecipazione pubblica e quella privata risultano più articolate e visibili rispetto a quanto analizzato per i Codici di condotta» (416-417).

[43] Per i sistemi di IA che non sono ad alto rischio, l'art. 95, par. 1, prevede 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, tramite l'elaborazione di codici di condotta incentivata dall'Ufficio per l'IA e gli Stati membri. Ancora condivisibili, al riguardo, le considerazioni critiche espresse da G. De Minico, *Le fonti del diritto: un argine all'intelligenza artificiale?*, cit., 90-91, circa l'eccessivo spazio riservato ai privati nella loro elaborazione, dal momento che le indicazioni provenienti dal soggetto pubblico sono minime, come risulta dall'art. 95, par. 2.

[44] Reg. UE n. 1689/2024, art. 53, par. 4.

[45] *Ibidem*

sistemico, rispetto ad obblighi, tuttavia, diversi e più stringenti[46].
I codici di buone pratiche sono espressione di coregolazione dal momento che l'Ufficio per l'IA, che rappresenta la parte pubblicistica[47], oltre ad incoraggiarne l'elaborazione da parte di una serie variegata di soggetti[48] ne valuta, unitamente al comitato[49], il rispetto degli obblighi di cui agli articoli 53 e 55, prima dell'adozione, oltre che il rispetto degli stessi, post adozione[50].
La natura coregolatoria ed il rilevante ruolo attribuito ai soggetti regolati nell'elaborazione della disciplina cui i loro sistemi di IA devono conformarsi, comportano il rischio di demandare ai privati, in una situazione di evidente conflitto di interessi, decisioni suscettibili di incidere sui diritti fondamentali[51] a vantaggio dei propri interessi economici ossia della propria libertà d'impresa, laddove il bilanciamento tra diritti dovrebbe essere riservato ad organi politicamente responsabili[52]. Non può, d'altra parte, negarsi come il coinvolgimento dei privati possa rivelarsi decisivo sia ai fini di una maggiore effettività delle regole, favorita dalla partecipazione dei destinatari alla loro elaborazione, sia per garantire la tempestività del loro adeguamento all'evoluzione del contesto tecnologico e valorizzare il patrimonio di conoscenze specialistiche, proprio di un settore ad elevata complessità tecnica[53].

4.2. Le questioni del regolamento «generico» e della debolezza dei controlli ed il ruolo dei privati. Il conflitto di interessi non esaurisce i profili critici delle previsioni in esame. Ad esso, invero, si collegano le riserve circa il ricorso alla fonte regolamentare, in un ambito nel quale l'esigenza di armonizzazione del mercato interno, ai sensi dell'art. 114 TFUE[54], si intreccia strettamente con la tutela dei diritti fondamentali, esposti ai rischi derivanti dall'utilizzo dell'IA[55].

---

[46] Rispetto al compito di indentificare la sussistenza di rischi sistemici con la conseguente applicazione della disciplina prevista dal Regolamento, F. Donati, *La protezione*, cit., 16, ritiene i relativi criteri di individuazione «formulati in maniera talmente ampia da attribuire alla Commissione europea, nella sostanza, un potere di politica industriale, idoneo a indirizzare lo sviluppo di questi sistemi».
[47] Reg. UE n. 1689/2024, art. 64.
[48] Reg. UE n. 1689/2024, art. 56, par. 3: «Fornitori di modelli di IA per finalità generali, pertinenti autorità nazionali competenti, organizzazioni della società civile, industria, mondo accademico altri pertinenti portatori di interessi, quali i fornitori a valle e gli esperti indipendenti, [che] possono sostenere il processo».
[49] Reg. UE n. 1689/2024, art. 65.
[50] G. De Minico, *Le fonti del diritto*, cit., 89-90.
[51] Se, ad esempio, la cornice pubblicistica si limita a stabilire che il sistema relativo al riconoscimento facciale, non deve discriminare, evidentemente tale obiettivo può essere perseguito attraverso tante scelte tecniche che sottendono altrettante scelte politiche, riguardo il livello di margine di errore, la modalità di misurazione del *bias*, ecc. Se queste regole tecniche vengono definite da organismi privati, si demanda agli stessi, privi di investitura democratica e di responsabilità, anche la scelta politica sottesa.
[52] G. De Minico, *Le fonti del diritto*, cit., 80. M. R. Ferrarese, *Scrittura digitale e normatività tecnologica*, in *Quad. cost.*, 1, 2026, 79, invero, valuta come «la sovranità digitale diventa piuttosto una sorta di condominio tra Stati e soggetti privati e ha una fisionomia cangiante, che dipende sia dai continui cambiamenti e dalle innovazioni in campo tecnologico, sia dalla volontà politica degli Stati di ricorrere a forme di regolazione».
[53] F. Gallo, *Cyberspazio, diritti e tutele*, cit. 22, per il quale un rischio dell'*AI Act* è la sua obsolescenza: da qui la decisiva rilevanza dei codici di condotta nazionali, del ruolo della giurisprudenza, del Legislatore, degli strumenti di *soft law*.
[54] A. Simoncini, *AI Act e digital constitutionalism*, cit., 237.
[55] D. U. Galetta, B. Cappiello, *Il Regolamento UE sull'intelligenza artificiale e le amministrazioni pubbliche: basi giuridiche, obiettivi e limiti di un esperimento normativo dagli esiti incerti*, in A. F. Uricchio, C. Caldarola, (a cura di), *L'intelligenza artificiale*, cit., 11, spiegano come l'AI Act, pur volto anche alla tutela dei diritti fondamentali, si fondi sull'art. 114 TFUE, poiché i Trattati non prevedono una specifica base giuridica per adottare atti derivati in tale materia. Il collegamento tra funzionamento del mercato unico digitale e protezione dei diritti legittimerebbe un'armonizzazione europea di carattere espansivo.

La scelta del regolamento si giustifica in ragione della necessità di assicurare un'applicazione uniforme della disciplina nell'intero territorio dell'Unione. Tuttavia, tale finalità, nella fattispecie, è contraddetta dall'ampio spazio lasciato all'autoregolazione dei soggetti privati, destinato a produrre discipline applicative potenzialmente differenziate nei diversi Stati membri. Ne deriva una evidente tensione: l'Unione interviene, con uno strumento normativo idoneo a comprimere gli spazi di intervento statale, in nome dell'uniformità ma, al tempo stesso, affida una parte significativa della definizione delle regole impattanti sui diritti fondamentali agli stessi operatori economici destinatari della disciplina[56].

Il rischio è, pertanto, che il reg. UE n. 1689/2024, per le cui caratteristiche di indeterminatezza si è parlato di «regolamento generico»[57], non realizzi pienamente la propria funzione tipica di uniformazione normativa e produca un ulteriore effetto problematico: ridurre lo spazio decisionale degli Stati membri senza sostituirlo con una disciplina europea sufficientemente determinata, trasferendo così una quota rilevante della regolazione effettiva ai soggetti privati[58].

Ulteriori profili critici emergono con riferimento alla disciplina del monitoraggio dei sistemi di IA ad alto rischio, prevista dagli artt. 72 e 73 del Regolamento. Il limite principale risiede nella collocazione prevalentemente *ex post* degli stessi, destinati a operare appunto dopo l'immissione sul mercato o la messa in servizio del sistema, quando eventuali effetti pregiudizievoli sui diritti fondamentali non soltanto degli utilizzatori possono essersi già prodotti[59].

Come si è visto, i controlli preventivi, ossia la valutazione di conformità *ex ante* è affidata a

---

[56] La critica della scelta della fonte regolamentare è fondata sui principi di sussidiarietà e proporzionalità (su cui v. D. U. Galetta, B. Cappiello, *Il Regolamento UE sull'intelligenza artificiale e le amministrazioni pubbliche,* cit., 11). Se la dimensione transnazionale dell'IA e il rischio di frammentazione giustificavano l'intervento dell'Unione ai sensi dell'art. 114 TFUE, ciò non rendeva necessario il ricorso a una fonte direttamente applicabile e fortemente limitativa degli spazi statali. La criticità risiede, dunque, nell'ampiezza di una disciplina che, pur comprimendo la discrezionalità degli Stati membri, richiede una significativa integrazione mediante standard, codici e strumenti di coregolazione privata, finendo così per trasferire margini decisionali ai soggetti privati più che all'Unione (3, 18).

[57] In parallelo con la nota categoria delle direttive dettagliate, si è teorizzata quella dei «regolamenti generici»: C. Burelli, *La scelta dell'atto da parte del legislatore dell'UE: il mercato unico digitale alla prova della qualità della legislazione,* in *Federalismi.it*, 22 ottobre 2025, 4. La tendenza al ricorso al «regolamento generico», da intendersi quale fonte speculare alla cd. direttiva dettagliata, ha rappresentato un regresso sotto il profilo della qualità legislativa dal momento che gli scopi sottesi alla scelta di tale fonte, quale atto uniformante, non sarebbero raggiunti, com'è evidente nell'ipotesi in esame (C. Burelli, *La scelta*, cit., 42-43).

[58] Per questo esito, non si condivide la conclusione di C. Burelli, *La scelta dell'atto*, cit., 42-43, per la quale, nonostante si sia adottato un regolamento, ossia una fonte ad «astratta intensità precettiva», si ha comunque una normativa generica al punto da trovarsi di fronte ad «una (mera) «illusione di un'armonizzazione» per cui «la questione della scelta dello strumento, così come quella della c.d. *légistique*, dimostrano come «tutto cambia perché nulla cambi» e, forse, modificando gli addendi il risultato resta il medesimo». Critiche sul punto anche in D. U. Galetta, B. Cappiello, *Il Regolamento UE sull'intelligenza artificiale e le amministrazioni pubbliche*, cit., 18. A. Simoncini, *Ai Act*, cit., 239, invero, vede nel ricorso alla pratica dei rinvii del Regolamento oltre che a privati e alla Commissione, anche agli allegati, quello che «Schmitt definiva compromesso dilatorio; ovverosia, norme approvate con un contenuto intenzionalmente non autoapplicativo, proprio perché non si riesce a raggiungere un reale accordo a livello politico e si preferisce spostare ad una successiva sede "tecnica" la definizione concreta della regola» che, tuttavia, ha un contenuto politico.

[59] Quanto ai controlli dell'Autorità europea sull'intelligenza che è l'ufficio sull'intelligenza artificiale deputato a un'attività di monitoraggio sulla condotta imprenditoriale, nonché di coordinamento sull'azione delle rispettive autorità nazionali a ciò preposte, si tratta di controlli *ex post*, «a macchine intelligenti già operanti sul mercato», la cui ridotta efficacia è di tutta evidenza (F. Gallo, *Cyberspazio, diritti e tutele*, cit., 18).

procedure di controllo interno del fornitore[60].
Anche nella fase successiva, invero, l'effettività del monitoraggio dipende in parte significativa dall'iniziativa del soggetto regolato: sia quanto alla raccolta, documentazione e analisi dei dati sulle prestazioni del sistema, ai sensi dell'art. 72, sia quanto alla segnalazione degli incidenti gravi prevista dall'art. 73. Quindi non può trascurarsi il rischio di un modello di vigilanza nel quale il controllo pubblico successivo resta comunque condizionato dalla completezza, tempestività e affidabilità delle informazioni provenienti dagli operatori economici.
È vero, infatti, che le autorità di vigilanza del mercato possono intervenire anche d'ufficio, nell'esercizio dei poteri loro attribuiti dalla disciplina sulla sorveglianza del mercato. Permangono, tuttavia, i profili problematici segnalati: a prescindere dagli obblighi di segnalazione, i sistemi di monitoraggio post-commercializzazione costituiscono il principale canale informativo su cui si innesta l'intervento delle autorità pubbliche di vigilanza. Sulla base di tali informazioni tali autorità eserciteranno i poteri pubblici previsti dagli artt. 74 e 79[61]: possono valutare il sistema, richiedere documentazione e informazioni, imporre misure correttive e, nei casi più gravi, disporre il ritiro o il richiamo del sistema. A questo circuito si affiancano le autorità preposte alla tutela dei diritti fondamentali, cui l'art. 77 riconosce poteri di accesso alla documentazione e di impulso rispetto allo svolgimento di test tecnici[62].
La natura successiva dei controlli esterni, unitamente al ruolo, anche in tale ambito molto rilevante, riconosciuto ai regolati e alla numerosità delle autorità coinvolte nelle diverse attività con rischi di sovrapposizione di competenze[63] e, non ultimo, la natura non necessariamente indipendente dal Governo di quelle statali[64] inducono a riflettere sulla eventualità di interventi correttivi al fine di migliorare l'attività di controllo e, quindi, l'efficacia della normativa a garanzia di un'IA antropocentrica[65].

4.3. Ti La tutela sostanziale dei diritti apprestata dall'AI Act tolo. Passando al piano della tutela sostanziale, una previsione di assoluta rilevanza è contenuta nell'art. 14 *AI Act*, relativo alla sorveglianza umana, ossia all'obbligo, rispetto ai sistemi IA ad alto rischio, di garantire, nella fase di progettazione e sviluppo, che possano «essere efficacemente

60. Infatti, come rileva ancora F. Gallo, *Cyberspazio, diritti e tutele*, cit., 18: «[…] un controllo di tal genere, rimesso allo stesso controllato, offre poche garanzie di obiettività quanto al rispetto delle regole fissate dalle stesse norme comunitarie».
61 Le autorità nazionali di vigilanza del mercato non intervengono, infatti, soltanto a seguito delle segnalazioni degli incidenti gravi di cui all'art. 73 o delle informazioni emerse dal monitoraggio post-commercializzazione previsto dall'art. 72.
62 Diverso, ma complementare, è il piano degli artt. 88 ss., relativo ai modelli di IA a finalità generale. In tale ambito la vigilanza è accentrata in capo alla Commissione, tramite l'Ufficio IA, con poteri di monitoraggio, richiesta di informazioni, valutazione e imposizione di misure correttive. Il raccordo con le autorità nazionali emerge soprattutto quando il modello a finalità generale è integrato in sistemi di IA vigilati a livello nazionale: in tali casi, le autorità di vigilanza del mercato possono sollecitare l'intervento della Commissione ove ciò sia necessario per l'esercizio dei propri compiti (art. 88, paragrafo 2).
63 V. sul punto le interessanti considerazioni di E. C. Raffiotta, *Dalla* self-regulation *alla* over-regulation *in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in *Osservatorio sulle fonti*, 2, 2023, 256-258.
64 V. nota 41.
65 Per A. Simoncini, *Potere cibernetico*, 56, la strada per superare una dannosa *over-regulation* è «di affiancare agli strumenti normativi oggi esistenti un livello ulteriore di protezione, che passi attraverso il fattore umano, ovverosia chi progetta la tecnica», passando da una tutela *by design* e *by default* ad una tutela *by education*. Sui rischi dell'*over-regulation*, v. G. Pitruzzella, *Diritti e innovazione tra Europa e Stati Uniti*, in Quad. cost., 1, 2026, 29 ss.

supervisionati da persone fisiche durante il periodo in cui sono in uso»[66]. Considerando che, ove siano toccati dati personali, la tutela offerta dall'art. 22, reg. UE n. 679/2016[67], considerata più forte in quanto riconoscimento di un diritto soggettivo dell'utente a non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, continuerà ad applicarsi[68], la scelta più blanda del Regolamento può ritenersi ispirata alla volontà di conciliare detta tutela all'obiettivo di sviluppare la tecnologia, riducendo eventuali duplicazioni ed applicazioni in settori non incidenti su dati personali. Un divieto generalizzato delle decisioni completamente automatizzate avrebbe potuto, infatti, limitare eccessivamente l'impiego di sistemi di IA in molti settori.

All'attuazione di tale sorveglianza è sostanzialmente funzionale l'obbligo di «Trasparenza e fornitura di informazioni ai *deployer*» di cui all'art. 13 che, tuttavia, se punta a garantire una migliore conoscenza del sistema non riguarda la possibilità di ricostruire lo schema argomentativo seguito dalla macchina e, quindi, non consente un effettivo sindacato né, di conseguenza, la contestabilità dell'*output*. Per questo, tale obbligo ha ad oggetto una trasparenza finalizzata a garantire la sorveglianza umana che, tuttavia, non va oltre il funzionamento operativo del sistema, non consentendo una comprensione dell'algoritmo e una spiegazione completa[69]. Rispetto a tale situazione, considerato il rischio di *automation bias*, la tendenza dell'essere umano ad affidarsi alle valutazioni della macchina e a non contestarne gli esiti può ridurre la sorveglianza umana a una mera «illusione di controllo»[70].

---

[66] In relazione al diritto all'intervento umano del GDPR, A. Iannuzzi, *L'AI Act nell'ecosistema normativo europeo*, cit., p. 253, afferma che esso connota il provvedimento quale «prima concretizzazione dell'umanesimo digitale che propugna l'Ue».

[67] Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva n. 95/46/CE (regolamento generale sulla protezione dei dati), d'ora in poi anche GDPR (General Data Protection Regulation)

[68] Così V. D'Antino, *L'approccio*, cit., 23, nota 63: «Occorre comunque precisare che il complesso di doveri e obblighi dell'AI Act non pregiudica l'applicabilità dell'art. 22 GDPR, che per l'appunto si riferisce solo alle decisioni completamente automatizzate e basate sul trattamento dei dati personali, non interessando quelle che siano state adottate dal funzionario con l'ausilio di sistemi di IA sulla base di *big data*». Esprime, tuttavia, riserve sul punto, A. Simoncini, *AI Act e digital constitutionalism*, cit., 238, che considera tale obbligo «versione indubbiamente più debole del diritto a non essere soggetti a decisioni totalmente automatizzate posto dall'art. 22 del GDPR».

[69] In tale prospettiva le parole di A. Simoncini, *AI Act e digital constitutionalism*, cit., 238, che parla «a proposito dell'obbligo di trasparenza funzionale» di «versione ridotta rispetto al diritto generale a spiegazioni comprensibili», altrove dallo stesso sostenuto.

[70] Circa il principio della non esclusività (della decisione algoritmica) che si sostanzia nella previsione di «un possibile intervento umano che possa correggere eventuali errori della macchina» (M. Corradino, *Potere pubblico e intelligenza artificiale*, in A. F. Uricchio, C. Caldarola (a cura di), *L'intelligenza artificiale tra regolazione,* cit.), invero già previsto dal d.lgs n. 36/2023 (*Nuovo Codice dei Contratti Pubblici*), unitamente a quello della riserva del controllo umano, A. Di Ruzza, *L'Intelligenza Artificiale e la disciplina nel Codice dei Contratti Pubblici*, in A. F. Uricchio, C. Caldarola (a cura di), *L'intelligenza artificiale tra regolazione,* cit., 286. M. Corradino, *Potere pubblico e intelligenza artificiale*, cit., 46, si chiede se, sebbene «nessuno ritiene [ritenga] ammissibile o perfino pensabile un sistema che veda l'uomo "*out of the loop*", del tutto fuori dal sistema […] davvero l'uomo può[possa] essere in grado di dominare un sistema basato sull'intelligenza artificiale» (46). Si può apprezzare la rilevanza della questione se si considera, ad esempio, il caso della giustizia. Dal combinato disposto del reg. UE n. 2024/1689 e della l. n. 132/2025, emerge che l'applicazione dell'intelligenza artificiale all'attività giudiziaria è formalmente ricondotta a un modello antropocentrico e di supporto, nel quale la decisione resta riservata al magistrato. Tuttavia, le criticità della disciplina finora rilevate, si manifestano anche con riferimento al settore in considerazione. La sorveglianza umana, pur normativamente prevista, rischia, infatti, di risultare inefficace se l'operatore non è posto nelle condizioni effettive di comprendere, verificare e contestare l'*output* algoritmico. Quanto alle disposizioni specificamente relative alla giustizia, la distinzione tra attività meramente ausiliaria e attività incidente sul processo decisionale, prevista sia dal Regolamento (Considerando 61; Allegato III, punto 8, lett.

Non dissimile, in quanto comunque finalizzata a ritenerlo inadeguato a fondare un controllo sostanziale della decisione della macchina, la critica all'art. 86 sul «Diritto alla spiegazione dei singoli processi decisionali».

Si tratta, comprensibilmente, di un punto delicato della critica della regolazione apprestata dall'UE, ritenuta inadeguata, sempre sotto il profilo dell'effettività della «sorveglianza umana», anche con riferimento all'utilizzo di sistemi di IA non generativa il cui logaritmo è, in linea di massima, conoscibile[71] dal momento che ci si trova di fronte ad ipotesi comunque riconducibili ad istituti tradizionali dell'ordinamento giuridico[72]. L'uomo, tuttavia, anche in tal caso, sarebbe soggetto all'*automation bias*, con la conseguente attivazione di un controllo della macchina, di fatto, solo formale.

In tali casi, tuttavia, il principale limite non sembra imputabile alla disciplina normativa, bensì alla concreta capacità della persona, da sviluppare attraverso un'adeguata formazione generale e digitale, di mantenere il controllo sul sistema e di esercitare su di esso una autonoma capacità critica, evitando di essere progressivamente assorbita dalle sue logiche,

a: 8. Amministrazione della giustizia e processi democratici: a) i sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie) che dalla l. n. 132/2025 , art. 15, non è sempre netta, come, ad esempio, quando il sistema assiste il giudice nella ricerca, interpretazione e applicazione del diritto o nella valutazione dei fatti. Infine, il ruolo attribuito al Ministero della giustizia nella disciplina, autorizzazione e sperimentazione degli impieghi dell'IA negli uffici giudiziari può sollevare un problema di compatibilità con le esigenze di piena indipendenza della funzione giurisdizionale, per il condizionamento che può derivarne, indirettamente, sulle decisioni dei giudici. Da tali criticità può derivare la compressione di diritti fondamentali a partire dal diritto di difesa, come condivisibilmente sottolineano G. De Minico, E. Palomba, M. Parente*, AI Act e Legge italiana*, cit., 2-3, per le quali neppure la legge italiana ha superato le criticità del Regolamento. Critiche e condivisibili anche le considerazioni di F. Iannone, *Prime riflessioni sull'IA: la legge 145/2025 letta in cornice eurounitaria e sovranazionale* in *Giustiziainsieme.it*, 7 novembre 2025; F. Dal Canto e S. Rovelli, *Il modello costituzionale di ordinamento giudiziario e la sfida della digitalizzazione della giurisdizione: il ruolo del Ministero della Giustizia e del Consiglio superiore della magistratura prima e dopo la legge italiana sull'intelligenza artificiale*, soprattutto 6, 13; M. D'Amico, *Giustizia, giudici e IA*, in *https://www.ordinamentogiudiziario.info/commenti/giustizia-giudici-e-ia-di-marilisa-damico*, 28 ottobre 2025. Per un giudizio positivo sulla l. n. 132/2025, con riferimento al settore della giustizia, v. R. D'Angiolella, *Giustizia e intelligenza artificiale tra l'AI ACT e il disegno di legge italiano. L'insostituibilità del giudice, il metodo e l'argomentazione giuridica*, in *Giustiziainsieme.it*, 30 luglio 2025.

[71] Del resto, sistemi di IA non generativa sono già presenti sul mercato e trovano applicazione anche in Italia nell'ambito di attività amministrative, finanziarie e lavorative, come nel campo creditizio, occupazionale, delle prestazioni pubbliche, dei servizi essenziali. La riconducibilità degli *output* ai criteri e agli obiettivi fissati dai soggetti che ne progettano o utilizzano il funzionamento consente, almeno in linea di principio, di applicare le tradizionali categorie della responsabilità giuridica. Da ricordare, al riguardo, le sentenze del Consiglio di Stato nn. 2270/2019 e 8472/2019, che hanno affermato la legittimità dell'uso degli algoritmi per la mobilità e l'assegnazione delle sedi dei docenti, per la formazione di graduatorie e per procedure concorsuali, purché siano garantite trasparenza, conoscibilità dei criteri e imputabilità della decisione all'amministrazione. In argomento, v. F. Laviola, *Algoritmico, troppo algoritmico: decisioni amministrative automatizzate, protezione dei dati personali e tutela delle libertà dei cittadini alla luce della più recente giurisprudenza amministrativa*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2020, 389 ss.

[72] Con riferimento all'IA non generativa, infatti, gli algoritmi sono in genere controllabili e ricostruibili, per cui eventuali errori o discriminazioni possono essere ricondotti al programmatore o al soggetto che utilizza il sistema. Tuttavia, in tal caso, i rischi per la democrazia e per i diritti fondamentali possono derivare, da un lato, dalla natura oligopolistica delle piattaforme digitali e dello spazio comunicativo online, ove la visibilità e la diffusione delle informazioni dipende dalle *big tech*, i cosiddetti «signori del web» e, dall'altro lato, da errori o distorsioni prodotte dagli algoritmi impiegati nei diversi settori della vita umana eventualmente, a loro volta, controllati da pochi operatori privati (si consideri l'esempio di banche-dati e strumenti di ricerca giuridica che sono condizionate dal potere dei pochi operatori che stabiliscono quali decisioni debbano essere più facilmente reperibili o quali massime debbano essere associate ad una pronuncia). Per una disamina di casi in cui l'IA viene già utilizzata, si v. A. Simoncini, *Potere cibernetico*, cit., 43-44.

contravvenendo al noto paradigma dell'*human in the loop*.
Diversamente, con riferimento all'IA generativa, l'inadeguatezza della sorveglianza umana può derivare principalmente dall'opacità del funzionamento algoritmico e dalla conseguente difficoltà di ricostruire, in termini comprensibili per l'operatore, il processo interno che ha condotto alla produzione dell'output. Ne risulta indebolita la possibilità di esercitare un controllo realmente consapevole e critico, con gravi conseguenze soprattutto quando tali sistemi siano impiegati in ambiti suscettibili di incidere significativamente sui diritti fondamentali. L'*AI Act* non vieta, infatti, in via generale, tali impieghi ma li riconduce, ove ricorrano le condizioni previste dall'art. 6 e dall'allegato III, alla disciplina dei sistemi di IA ad alto rischio, affidandosi agli obblighi ivi previsti per la relativa gestione dello stesso[73]. È tuttavia lecito dubitare, proprio per i rilevati limiti della disciplina, che tale soluzione sia sempre sufficiente a scongiurarli. Nei contesti in cui l'opacità del sistema impedisca una supervisione umana effettiva e l'errore possa produrre conseguenze particolarmente gravi sui diritti fondamentali, sembrerebbe, piuttosto, preferibile prevedere divieti settoriali o limiti d'impiego più rigorosi.

Ancora sul piano sostanziale, rileva la previsione riguardante i dati che alimentano il sistema dalla cui qualità dipende la qualità della decisione della macchina[74]. È l'art. 10, par. 3, del Regolamento a stabilire che per l'addestramento dei sistemi IA nei settori ad alto rischio, si utilizzino set di dati che siano «pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista». È intuitivo che la qualità della decisione algoritmica dipenda, in primo luogo, dalla qualità dei dati immessi nel sistema, secondo il principio del *garbage in, garbage out*: un sistema alimentato da dati incompleti, inesatti, non rappresentativi o viziati da *bias* tenderà, infatti, a produrre output altrettanto inattendibili o discriminatori.
E tuttavia, la traduzione sul piano applicativo del principio del *garbage in, garbage out* non è agevole in quanto la qualità del dato non coincide con la sua mera correttezza formale, ma richiede, altresì, la sua completezza, accuratezza, rappresentatività, attualità e neutralità. Il dato, infatti, è il risultato di processi di selezione, raccolta e classificazione che possono incorporare distorsioni di varia natura. Ne deriva che input informativi parziali, obsoleti o non rappresentativi possono compromettere l'affidabilità dell'output algoritmico, anche in presenza di un sistema tecnicamente efficiente[75].
Da non trascurare, infine, ancora sotto il profilo della tutela sostanziale, che, per quanto il Regolamento preveda forme di tutela degli individui, come il richiamato diritto alla

[73] I rischi connessi all'IA generativa non derivano soltanto dalla natura oligopolistica dei proprietari delle piattaforme digitali ma dalla impossibilità di controllare output prodotti attraverso autoapprendimento delle macchine, quindi secondo logiche non ricostruibili. Per G. De Minico, E. Palomba, M. Parente, *AI Act e Legge italiana sull'Intelligenza artificiale,* cit., 6, la l. n. 132/2025 presenta le stesse criticità dell'*AI Act* e cioè «un eccesso di fiducia nell'autodisciplina e nel valore della trasparenza. In assenza di un controllo pubblico sostanziale, tali meccanismi rischiano, infatti, di trasformarsi in una «finzione di legalità», inducendo i cittadini a confidare in una sicurezza che, senza l'intervento pubblico e una cornice eteronoma forte, resta soltanto apparente». Critico anche A. Iannuzzi, *L'AI Act nell'ecosistema* normative, cit., 253, per il quale il diritto alla trasparenza «ha un'applicazione molto difficile in rapporto ai sistemi di *machine learning*, che sono delle complesse *black box* che non consentono di tenere traccia e di dare conto dei processi decisionali».
[74] Quanto al criterio di non discriminazione, chiaramente la natura non discriminatoria della decisione dipende dalla natura non discriminatoria della raccolta dati. Così M. Corradino, *Potere pubblico*, cit., 48, ricordando il caso *Compas* rimasto emblematico, in cui l'impiego di dati statistici distorti su base etnica determinò una sovrastima del rischio di recidiva delle persone afroamericane.
[75] A. Simoncini, *Ai Act*, 238, pur riconoscendo la rilevanza di simile disposizione, pone l'accento «sulla concreta applicabilità di criteri come "completezza" o "assenza di errori" nei dataset».

spiegazione dei singoli processi decisionali di cui all'art. 86 o il diritto di segnalazione[76], si tratta, tuttavia, di strumenti di natura informativa e non di rimedi giurisdizionali autonomi contro la decisione algoritmica. Il diritto al reclamo e il diritto alla spiegazione non sono diritto al riesame, all'annullamento, alla sospensione o al risarcimento della decisione fondata sull'output del sistema. La tutela individuale resta, quindi, affidata a rimedi esterni e frammentari, desumibili dal diritto nazionale, dal GDPR o dalle discipline settoriali applicabili, per cui è condivisibile, quanto rilevato a proposito del «*due process digitale*»[77] quale «vero banco di prova per verificare se l'*AI Act* superi davvero il test del costituzionalismo europeo»[78], dal momento che «senza strumenti di giustiziabilità, le garanzie rischiano di restare sulla carta»[79].

5. Qualche considerazione di sintesi su un tema in continua evoluzione. Le riflessioni sin qui sviluppate riguardano un tema che, per sua natura, non consente approdi conclusivi, tanto meno definitivi. È possibile, piuttosto, avanzare alcune considerazioni provvisorie sugli esiti attuali dell'approccio europeo all'Intelligenza Artificiale, destinati a essere verificati e, se necessario, ripensati man mano che l'innovazione tecnologica raggiungerà ulteriori stadi di evoluzione.

La finalità del reg. UE n. 1689/2024 di promuovere uno sviluppo e un impiego dell'Intelligenza Artificiale in una prospettiva antropocentrica, appare pienamente coerente con l'impianto assiologico della Costituzione italiana, fondata sulla centralità della persona e sul riconoscimento dei suoi diritti inviolabili. Anche Papa Leone XIV, nell'Enciclica *Magnifica Humanitas*, dedicata alla protezione della persona umana nel tempo dell'Intelligenza Artificiale, richiama il tema della dignità e la necessità che l'innovazione resti orientata al bene dell'uomo.

Lo scopo della regolazione non può ridursi alla mera sicurezza tecnica dei sistemi o alla loro conformità procedurale, ma deve consistere nella garanzia di un'Intelligenza Artificiale rispondente a «un'esigenza di etica laica – non soltanto morale e religiosa – ispirata al valore della persona e alla sua tradizione consolidata nella storia europea e nel nostro passato»[80]. In questa prospettiva, la regolazione europea e nazionale dell'IA si inserisce nel solco del costituzionalismo personalista, che, appunto, non rifiuta l'innovazione tecnologica, ma richiede che essa sia orientata alla tutela della persona, della sua libertà, della sua eguaglianza e della sua dignità.

Certo, la regolazione è migliorabile. Come si è visto, ne va garantita effettività laddove gli strumenti predisposti - trasparenza, sorveglianza umana, gestione del rischio, qualità dei dati, valutazione di conformità e vigilanza pubblica - non sempre sono effettivamente capaci di impedire che l'automazione produca opacità decisionale, discriminazioni, deresponsabilizzazione o forme di disumanizzazione dei processi in cui è applicata.

Nella prospettiva di tradurre principi etici in obblighi giuridici[81], considerato che l'IA non è

[76] Art. 85, Reg. UE n. 1689/2024.

[77] Così O. Pollicino, *Possiamo affermare che l'AI Act sia parte integrante del digital constitutionalism?*, cit., 242.

[78] *Ibidem.*

[79] *Ibidem.*

[80] Così G. M. Flick, *L'AI Act fra complessità e responsabilità: il caso della giustizia*, in *BioLaw Journal –Rivista di BioDiritto*, 3, 2025, 271-272. Nello stesso senso, A. Simoncini, *Potere cibernetico*, cit., 55, che avverte che il rispetto dei valori fondamentali dell'ordinamento non può essere ridotto a una valutazione etica soggettiva e non giustiziabile.

[81] Molte sono le questioni etiche giuridicizzate: il rischio di discriminazione viene ridotto attraverso requisiti sulla qualità dei dati e sulla gestione del rischio; l'opacità viene affrontata prevedendo obblighi di trasparenza; la deresponsabilizzazione viene affrontata attraverso la sorveglianza umana; a tutela del soggetto inciso è

neutra e che è la sua impostazione a certi valori e, non solo e non principalmente il suo utilizzo, a determinarne eventuali effetti negativi, si dovrà contestualmente tener conto che scopo principale dell'intervento europeo, fondato sull'art. 114 TFUE, è anche lo sviluppo del mercato dell'innovazione. Pertanto la traduzione di questi principi non può risolversi in un'*over-regulation*[82] che soffochi l'uno e l'altra, come ribadito da Draghi, nelle diverse occasioni evocate. Ne deriva, come sempre in campo giuridico, la necessità di bilanciamento, senza però mai rinunciare alla tutela della dignità umana. Ove l'utilizzo dell'IA possa comprometterla, va classificato come inaccettabile e, dunque, vietato.

La strada da percorrere dovrebbe essere quella di ricondurre ogni decisione, anche quando elaborata mediante sistemi di IA, alla responsabilità di una persona fisica, così da evitare la disumanizzazione del processo decisionale e la conseguente deresponsabilizzazione dei soggetti coinvolti. Quando ciò non sia possibile, finché non sarà possibile, occorrerebbe precludere l'applicazione di detti sistemi, secondo l'approccio *risk-based* del Regolamento, in ambiti il cui impatto sui diritti fondamentali la rende pericolosa.

L'attuazione di simile intento è operazione complicata tanto da potersi dubitare di riuscire a perseguirlo nella sua interezza. Oltre l'uso dell'IA, infatti, occorre regolare la stessa struttura dei processi decisionali automatizzati, riconducendo l'output ai soggetti umani e istituzionali che progettano, governano, e impiegano l'algoritmo. Su tale piano, tanto il Regolamento europeo quanto la disciplina nazionale appaiono ancora parzialmente carenti benché i numerosi obblighi fissati contribuiscano, indubbiamente, a garantire sistemi di IA che non ledano diritti fondamentali e, di conseguenza, non snaturino la democrazia.

Anche quest'ultima è oggetto di tutela del reg. UE n. 1689/2024 considerato che l'Intelligenza Artificiale può alterare le condizioni stesse del processo democratico: dalla la formazione libera del consenso alla genuinità del voto, dal pluralismo informativo alla trasparenza della comunicazione pubblica e la fiducia nelle istituzioni. La salvaguardia della democrazia emerge, in primo luogo, dal divieto di pratiche manipolative, subliminali o ingannevoli idonee a compromettere la capacità della persona di assumere decisioni libere e informate[83], impedendo che il proprio pensiero sia condizionato in modo inconsapevole[84]; in secondo luogo, dalla qualificazione come sistemi ad alto rischio di quelli destinati a influenzare l'esito di elezioni o referendum o il comportamento di voto[85]; quindi , dagli obblighi di trasparenza relativi a *deepfake*, contenuti sintetici e testi generati dall'IA su questioni di interesse pubblico[86].

Dal momento che l'IA può diventare uno strumento di condizionamento del consenso politico, viene collocata nell'area dell'alto rischio, da cui consegue la previsione di requisiti rafforzati per il suo utilizzo. In tal senso, già dal Considerando 62[87] emerge tale

previsto il diritto a ottenere spiegazioni in caso di decisioni fondate sull'*output* di un sistema ad alto rischio. Non tutte le questioni etiche, tuttavia, possono essere risolte in via regolatoria.

[82] Si rinvia sul punto a E. C. Raffiotta, *Dalla* self-regulation *alla* over-regulation *in ambito digitale,* cit.

[83] Art. 5, par. 2, Reg. UE n. 1689/2024.

[84] A. Simoncini, Potere cibernetico, cit., parla di rischio di sostituzione della «ragion pratica» con la «ragione algoritmica» (43) e, rispetto alle cd. tecnologie persuasive, di cattura della decisione umana «non perché le viene chiesto esplicitamente e consapevolmente – come nei casi delle *tecnologie decidenti* del paragrafo precedente – ma perché fornisce le informazioni o i contenuti, sulla cui base decidiamo» (47).

[85] All. III, punto 8, Reg. UE n. 1689/2024.

[86] Art. 50, Reg. UE n.1689/2024. A. Simoncini, *AI Act e digital constitutionalism*, cit., 237, parla in proposito di principio di «dealtà digitale» «ovverosia l'obbligo di trasparenza nelle interazioni uomo-macchina, cruciale per contrastare fenomeni come i *deepfake* e preservare la consapevolezza degli utenti» includendolo fra i «principi giuridici certamente di natura sostanzialmente "costituzionale"» posti dall'AI Act.

[87] «Fatte salve le norme previste dal Regolamento (UE) n. 2024/900 del Parlamento europeo e del Consiglio (34), e al fine di affrontare i rischi di indebite interferenze esterne sul diritto di voto sancito dall'articolo 39 della

preoccupazione.
Si richiama, infatti, espressamente il rischio che l'impiego di sistemi di IA determini indebite interferenze esterne nell'esercizio del diritto di voto e produca effetti pregiudizievoli sulla democrazia e sullo Stato di diritto, raccordando la disciplina dell'*AI Act* con quella dettata dal reg. UE n. 900/2024 in materia di trasparenza e targeting della pubblicità politica[88].
L'*AI Act*, in effetti, concorre, insieme ad altri Regolamenti dell'Unione europea, alla salvaguardia della democrazia nello spazio digitale[89]. In questa prospettiva rilevano, anzitutto, il *Digital Services Act*[90], che disciplina la trasparenza della pubblicità online, dei sistemi di raccomandazione e la prevenzione dei rischi sistemici connessi alla manipolazione del dibattito pubblico e il richiamato Reg. UE n. 900/2024, che interviene su uno dei profili più delicati del processo democratico, ossia la formazione del consenso elettorale.
È evidente, inoltre, che le tutele predisposte dall'*AI Act* incidono anche sul mercato interno dei servizi di media e, indirettamente, sulla loro libertà, sull'indipendenza editoriale, sul pluralismo dell'informazione e sulla tutela delle fonti giornalistiche, oggetto dello *European Media Freedom Act*[91]. Quest'ultimo, non si occupa di Intelligenza Artificiale ma ne è evidentemente interessato quando strumenti automatizzati, algoritmi di raccomandazione, sistemi di moderazione dei contenuti, tecniche di profilazione, strumenti di sorveglianza digitale o contenuti generativi impattano sul pluralismo informativo.
Anche con riferimento al versante della tutela democratica, la regolazione europea non può considerarsi risolutiva. Essa, tuttavia, contribuisce ad arginare i rischi derivanti da un utilizzo dell'Intelligenza Artificiale lasciato alla sola autoregolazione privata. Occorre, peraltro, considerare che talune criticità – come l'*automation bias* o l'effettiva capacità dei *deployer* di esercitare una reale funzione di sorveglianza sui sistemi di IA – difficilmente potranno essere superati soltanto in via normativa. Essi richiedono, piuttosto, la diffusione di una più solida cultura digitale, nonché percorsi di formazione di base e specialistica idonei a sviluppare lo spirito critico indispensabile a rendere effettivo il controllo umano sull'automazione.
Alla luce di tali considerazioni, pertanto, la scelta interventista europea, pur con tutti i limiti che la connotano, appare preferibile sia rispetto al modello statunitense, maggiormente affidato alla dinamica del mercato e all'autoregolazione degli operatori privati, sia rispetto al modello cinese, nel quale l'intervento pubblico tende a piegare la tecnologia a finalità di controllo e sorveglianza sociale. La filosofia sottesa all'*AI Act*, infatti, rappresenta un'opzione intermedia: promuovere lo sviluppo del mercato dell'innovazione, i cui benefici potenziali per l'umanità sono ormai evidenti, senza sacrificare la tutela dei diritti fondamentali, anzi

Carta e di effetti negativi sulla democrazia e sullo Stato di diritto, i sistemi di IA destinati a essere utilizzati per influenzare l'esito di elezioni o referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum dovrebbero essere classificati come sistemi di IA ad alto rischio, ad eccezione dei sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico».

[88] Regolamento (UE) n. 2024/900 del Parlamento europeo e del Consiglio del 13 marzo 2024 relativo alla trasparenza e al targeting della pubblicità politica. Sia consentito rinviare sul punto a D. Mone, *Formazione della volontà elettorale e tecnologie digitali: la pubblicità politica online nel Regolamento (UE) 2024/900*, in *Unità e pluralità del sapere giuridico*, 2, 2026, 143-164.

[89] Oltre a tali Regolamenti, «L'altra fondamentale componente di tale modello [regolatorio europeo) è costituita dall'*enforcement* antitrust» (G. Pitruzzella, *Diritti e innovazione tra Europa e Stati Uniti*, cit., 19).

[90] Regolamento (UE) n. 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva n. 2000/31/CE (*Regolamento sui servizi digitali*).

[91] Regolamento (UE) n. 2024/1083 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (*Regolamento europeo sulla libertà dei media*).

garantendo la sicurezza e l'affidabilità dei sistemi.
Essa, in definitiva, sembra inscriversi nella logica del bilanciamento propria del costituzionalismo contemporaneo, di cui la Costituzione italiana rappresenta una delle più compiute espressioni.

Abstract. Il contributo introduce lo studio sul ruolo dello Stato nell'età della tecnica, analizzato sotto diversi profili che vanno dalle dinamiche trasformative della forma di governo alla sicurezza, dai diritti sociali alle future generazioni, dalla partecipazione, democrazia e informazione alla transizione ecologica e all'Intelligenza Artificiale. Rispetto all'IA, in ragione della rilevanza di tale tecnologia, si analizza la disciplina introdotta dal reg. UE n. 1689/2024 e, in sua attuazione dalla l. n. 132/2025, evidenziandone le criticità nella prospettiva di modifiche correttive, convinti che l'approccio interventista europeo si ponga in piena coerenza con il principio personalista che ispira il costituzionalismo contemporaneo di cui la Costituzione italiana rappresenta una delle più compiute espressioni.

Abstract. This paper introduces a study on the role of the state in the age of technology, analysed from various perspectives ranging from the transformative dynamics of the form of government to security, from social rights to future generations and from participation, democracy and information to the ecological transition and Artificial Intelligence. With regard to AI, given the significance of this technology, the paper analyses the legislation introduced by Regulation (EU) n.1689/2024 and, in its implementation, by Law n. 132/2025, highlighting its critical issues with a view to corrective amendments, in the conviction that the European interventionist approach is fully consistent with the personalist principle that inspires contemporary constitutionalism, of which the Italian Constitution is one of the most accomplished expressions.

Parole chiave. Intelligenza artificiale – Dignità umana – Sorveglianza umana – Etica – Innovazione.

Key words. Artificial intelligence – Human dignity – Human surveillance – Ethics – Innovation.