ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

31 DICEMBRE 2025

Umanesimo digitale e sovranità regolatoria: il governo dell'intelligenza artificiale tra diritto europeo e nazionale

di Fernanda Faini
Professoressa associata di Filosofia del diritto
Università Telematica Pegaso

Umanesimo digitale e sovranità regolatoria: il governo dell'intelligenza artificiale tra diritto europeo e nazionale *

di Fernanda Faini
Professoressa associata di Filosofia del diritto
Università Telematica Pegaso

Abstract [It]: Il saggio intende analizzare il rapporto tra regolazione giuridica, intelligenza artificiale e sovranità tecnologica. A tal fine, il saggio esamina il modello di sovranità regolatoria che emerge alla luce della legislazione europea in materia di intelligenza artificiale, in particolare analizzando il regolamento UE 2024/1689, che mostra un approccio innovativo in merito al rapporto tra essere umano, diritto e intelligenza artificiale. Il contributo osserva poi il modello nazionale disegnato dalla legge 132/2025 per coglierne punti di forza e debolezza. L'analisi mostra che l'umanesimo digitale su cui si erge la sovranità regolatoria europea e nazionale, basato sul rischio, sulla comprensibilità e sulla supervisione umana, determina un'evoluzione nei principi e negli strumenti giuridici, ma al tempo stesso mostra sfide inedite da affrontare.

Title: Digital humanism and regulatory sovereignty: the governance of artificial intelligence between European and national law
Abstract [En]: The contribution aims to analyse the relationship between legal regulation, artificial intelligence and technological sovereignty. To this end, it examines the model of regulatory sovereignty that emerges in light of European legislation on artificial intelligence, in particular by analysing EU Regulation 2024/1689, which takes an innovative approach to the relationship between humans, law and artificial intelligence. The paper then looks at the national model outlined in Law 132/2025 to identify its strengths and weaknesses. The analysis shows that the digital humanism on which European and national regulatory sovereignty is based, founded on risk, comprehensibility and human supervision, is driving an evolution in legal principles and instruments, but at the same time presents new challenges to be addressed.

Parole chiave: diritto digitale; intelligenza artificiale; sovranità tecnologica; regolazione giuridica; umanesimo digitale
Keywords: digital law; artificial intelligence; technological sovereignty; legal regulation; digital humanism

1. Intelligenza artificiale, regolazione giuridica e geometrie di potere

Nella dimensione digitale i dati costituiscono il fondamento delle attività umane, danno forma alle identità e sono capaci di pervadere ogni aspetto dell'esistenza in modo ubiquo; gli esseri umani, gli oggetti

* Articolo sottoposto a referaggio. Il saggio è stato realizzato nell'ambito delle attività del Centro di Ricerca Interuniversitario "*Centre for Law and Ethics of Innovation, Technology and Artificial Intelligence*" (LEITAI), costituito dalle Università Telematica San Raffaele Roma, Università Telematica Pegaso e Università Telematica Universitas Mercatorum, Centro di cui la Prof.ssa Fernanda Faini è ViceDirettrice.

intelligenti e gli agenti artificiali elaborano e scambiano dati, conoscono e si conoscono grazie alle informazioni.

Nei confronti della dimensione tecnologica, che assume un ruolo costantemente crescente nell'esistenza umana, il diritto è chiamato a governare le tecnologie informatiche, al fine di tutelare i diritti e bilanciare interessi diversi e talvolta contrapposti sulla scena digitale. Nello svolgere la sua funzione il diritto sconta le peculiarità dell'oggetto che mira a regolare, ossia la dimensione digitale, costituita da beni intangibili, i dati; la *data society* è intimamente pervasa dai dati finendo per plasmare l'uomo stesso come un *data subject*[1]. Oggetti e soggetti diventano digitali; i beni si trasformano in servizi; il radicato paradigma della proprietà viene scalzato dal paradigma dell'accesso ai dati, ai servizi, alla propria esistenza digitale[2].

In tale contesto di riferimento assume un ruolo dominante l'intelligenza artificiale, la cui "anima" sono i dati e il "motore" gli algoritmi.

Alla luce del peculiare oggetto di regolazione, il diritto si trova a fare i conti con un ecosistema di regole diverso da quello giuridico, ossia le regole applicate dal codice informatico, che rendono possibili o meno azioni e interazioni, collegano effetti, determinano quali informazioni fornire all'utente e, di conseguenza, il grado di trasparenza e comprensibilità per chi le utilizza[3].

La *lex informatica* (il codice informatico), nel determinare ciò che è possibile tecnologicamente, mostra un ontologico aspetto regolatorio, capace di condizionare il comportamento dell'uomo[4] e, altresì, ogni altra forma di regolazione, compresa quella giuridica. Pertanto l'uomo deve essere capace di governare la *lex informatica* con il diritto, raggiungendo un difficile equilibrio basato sulla flessibilità e sull'adattabilità, al fine di aderire alla specificità tecnica e alla costante dinamicità della dimensione digitale senza limitare le potenzialità dello sviluppo tecnologico, ma, allo stesso tempo, fondato sulla prevedibilità e sulla certezza del diritto, principi solidi del diritto senza determinare il dominio della tecnologia sulla regolazione[5].

Nel caso dell'intelligenza artificiale alcune caratteristiche ontologiche incidono particolarmente nel rapporto con la regolazione giuridica. Il regolamento UE 2024/1689 definisce un sistema di intelligenza artificiale (di seguito anche *Artificial Intelligence* o AI) come «*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*»[6].

---

[1] In merito cfr. F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis Lefebvre, Milano, 2019.

[2] L. FLORIDI, *La rivoluzione dell'informazione*, trad. it., Codice edizioni, Torino, 2012, p. 15.

[3] L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, 1999, pp. 501-546.

[4] Cfr. L. LESSIG, *Code and Other Law of Cyberspace*, Basic Books, New York, 1999. Sul rapporto tra tecnica e diritto cfr. A. IANNUZZI, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale Scientifica, Napoli, 2018.

[5] V. FROSINI, *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981.

[6] Art. 2, par. 1, n. 1, reg. UE 2024/1689.

L'autonomia connota e differenzia gli algoritmi di intelligenza artificiale dalla logica degli algoritmi tradizionali, dove l'impostazione deterministica *if this*, *then that* indica un funzionamento predeterminato nel programma, limitandosi ad applicare regole informatiche predefinite ed espresse in linguaggio di programmazione come tali conoscibili dal programmatore. Nell'apprendimento automatico (*machine learning* e *deep learning*) tipico degli algoritmi di intelligenza artificiale, invece, l'uomo fornisce alla macchina un metodo di apprendimento da applicare ai dati cui ha accesso, per estrarre automaticamente le indicazioni e le nozioni necessarie per l'assunzione di una determinazione e per arrivare al risultato, analizzando grandi quantità di dati ed apprendendo i parametri numerici necessari nella successiva fase di esecuzione[7]. La rappresentazione matematico-numerica, ossia il modello generato dalla macchina nella fase di apprendimento o *training*, solitamente non è direttamente intelligibile da parte dell'essere umano (*black box*), aspetto che rileva particolarmente sotto la lente giuridica[8]. Proprio nella capacità di apprendere in modo autonomo si scorge la natura "intelligente" della macchina.

Di conseguenza emergono problematiche giuridiche strettamente correlate alle caratteristiche dell'intelligenza artificiale, quali il meccanismo di inferenze e correlazioni su cui si basano gli algoritmi, l'opacità e la correlata difficile intelligibilità da parte dell'uomo (*black box*), la connessa difficoltà di motivazione dei risultati cui perviene la macchina, oltre a possibili errori e *bias*, forieri di potenziali discriminazioni e disuguaglianze[9].

Sotto tale profilo rileva il rapporto che lega uomo e macchina, perché accanto ai pregiudizi sistematici presenti nei dati (*data bias)*, dove i dati di addestramento riflettono disuguaglianze storiche, stereotipi o squilibri nella rappresentazione e accanto ai *bias* nel modello e nel funzionamento dell'algoritmo (*algorithmic bias)*, che amplificano o introducono distorsioni anche con dati apparentemente neutrali, emergono i pregiudizi derivanti da processi umani che influenzano i risultati (*human-in-the-loop bias*), ossia pregiudizi inconsapevoli nelle decisioni o annotazioni da parte di chi progetta, seleziona o interpreta dati e modelli, che possono intervenire durante la progettazione, l'addestramento o la validazione del sistema[10]. Nella relazione tra l'uomo e l'intelligenza artificiale, pertanto, il pregiudizio non è sempre necessariamente legato agli elementi costitutivi dell'intelligenza artificiale, ossia dati e algoritmi, ma può derivare anche dall'essere umano stesso, in ciò mostrando che la tecnologia è solo teoricamente "neutrale", dal momento che nella sua valenza strumentale acquisisce il significato che gli uomini le

[7] Il *deep learning* è basato su reti neurali artificiali a molti strati; cfr. F. LAGIOIA, G. SARTOR, *L'intelligenza artificiale per i diritti dei cittadini: il progetto Claudette*, in *Ragion pratica*, fasc. 1, 2020, p. 88 ss.
[8] P. MORO, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *Rivista di diritto dei media*, fasc. 3, 2019, p. 19.
[9] G. CORASANITI, *Tecnologie intelligenti. Rischi e regole*, Mondadori, Milano, 2023, p. 63 ss.
[10] Sui *bias* cfr., *inter alia*, V. BARONE, *La discriminazione ai tempi dell'intelligenza artificiale: la questione algoritmica*, in T. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche*, 2° ed., Cedam, Trento, 2024, pp. 285-296.

conferiscono nell'utilizzarla; pertanto, nel contesto digitale possono emergere le asimmetrie e le disparità tipiche della società.

Queste criticità si aggravano laddove sia oggetto di analisi la *species* maggiormente diffusa di intelligenza artificiale, ossia l'intelligenza artificiale generativa *(Generative Artificial Intelligence – GAI)*, una tipologia avanzata di intelligenza artificiale basata su modelli di *deep learning*, in grado di apprendere dai dati sui cui è stata addestrata e di generare nuovi contenuti originali su richiesta. Si fonda prevalentemente su modelli neurali di tipo generativo (come i modelli Transformer), in grado di produrre *output* autonomi (testo, immagine, audio, video, codice, ecc.), svolgendo così funzioni creative in risposta a richieste dette *prompt*. Il contenuto generato con l'AI generativa può essere difficile da distinguere da quello umano originale con rischi giuridici di particolare peso quali *bias* e discriminazioni; violazione dei dati personali e del diritto d'autore; manipolazione e disinformazione; mancanza di trasparenza algoritmica, comprensibilità e sindacabilità; problematiche di responsabilità per illeciti o danni; utilizzo per scopi illeciti e usi malevoli (frodi, *deepfake*, *phishing*); un possibile *deskilling* (l'eccessiva dipendenza dall'AI può ridurre la capacità di scrittura e apprendimento profondo); dipendenza e riduzione del pensiero critico[11].

Tra i rischi necessitano menzione particolare le cosiddette allucinazioni dell'intelligenza artificiale generativa, riscontrabili quando l'intelligenza artificiale genera risposte plausibili o credibili, ma oggettivamente false, inventate o incoerenti producendo di conseguenza dati falsi, fatti inventati, riferimenti errati, leggi inesistenti. Le motivazioni strutturali e funzionali sono svariate, afferiscono alle caratteristiche della tecnologia oggetto di osservazione e vanno dai limiti del set di addestramento statistico (dati incompleti o errati) alla predizione della sequenza più probabile (e non quella più vera); dalla mancanza di accesso a fonti aggiornate e nessuna verifica delle fonti all'assenza di comprensione semantica profonda fino al sovraottimismo nei modelli di completamento, per cui l'intelligenza artificiale generativa tende a riempire con risposte i vuoti di *prompt* ambigui, generici o incompleti, arrivando a inventare per compiacere. In ogni caso, al di là della *ratio* specifica, le allucinazioni espongono l'utilizzo dell'AI generativa ad un rischio elevato proprio in contesti giuridici, oltre che in altri quali quelli sanitari ed educativi.

E non è un caso che si abbiano le prime sentenze che individuano una responsabilità aggravata per lite temeraria legata all'uso non controllato dell'AI generativa da parte di avvocati nella stesura dell'atto processuale che ha determinato l'inserimento di riferimenti errati o irrilevanti.

[11] Sulle sfide poste dall'intelligenza artificiale generativa cfr. M. KOVAK, *Generative Artificial Intelligence: A Law and Economics Approach to Optimal Regulation and Governance*, Palgrave Macmillan, 2024; J. Kaplan, *Generative A.I. Conoscere, capire e usare l'intelligenza artificiale generativa*, Luiss University Press, Roma, 2024; E. MAESTRI (a cura di), *Introduzione e note di sintesi al Regolamento (UE 2024/1689 sull'intelligenza artificiale*, Jovene, Napoli, 2024, p. 52 ss. e p. 263 ss.; U. RUFFOLO, A. AMIDEI, *Diritto dell'intelligenza artificiale. Proprietà industriale e intellettuale. CorpTech. Giustizia predittiva. Transumanesimo. AI generativa. Metaverso*, vol. 2, Luiss University Press, Roma, 2024.

Dopo il Tribunale delle Imprese di Firenze, sezione imprese, ordinanza n. 11053/2024 del 14 marzo 2025, che fermo restando il disvalore relativo all'omessa verifica dell'effettiva esistenza delle sentenze, non individuava colpa grave o malafede[12], il Tribunale di Torino, sezione lavoro, sentenza n. 2120/2025 del 16 settembre 2025[13] e il Tribunale di Latina, sentenza n. 1034/2025 del 23 settembre 2025[14], hanno ritenuto che condotte del genere integrassero gli estremi dell'azione in malafede o, quantomeno, di grave negligenza da parte dell'avvocato riconoscendo responsabilità aggravata e disponendo la condanna della parte al pagamento di una somma. Nella stessa direzione si pone il TAR Lombardia, sezione quinta, sentenza n. 3348 del 21 ottobre 2025[15], secondo cui l'utilizzo di tali strumenti non esime dalla responsabilità del difensore e vale il principio per cui la sottoscrizione dell'atto attribuisce responsabilità al firmatario, indipendentemente dal fatto che abbia utilizzato collaboratori o strumenti di intelligenza artificiale. Di conseguenza l'inserimento di riferimenti errati o irrilevanti comporta una violazione del dovere di lealtà e probità del difensore, in quanto gli atti contenenti tali errori rischiano di influenzare il contraddittorio o rendere gravosa l'attività di controllo giudiziario e difensivo; pertanto il TAR ha previsto la trasmissione della copia all'Ordine degli Avvocati di Milano per valutazioni disciplinari.

Tali aspetti mostrano come le caratteristiche tecniche ontologiche dell'intelligenza artificiale e delle sue *species* come quella generativa incidano in modo significativo a livello giuridico ed evidenziano la conseguente necessità che l'uomo per mezzo del diritto governi l'intelligenza artificiale, al fine di tutelare i diritti del singolo e della collettività.

Alla luce di tale contesto di riferimento, il contributo intende analizzare il rapporto tra regolazione europea, intelligenza artificiale e sovranità tecnologica. A tal fine, il saggio esamina il modello di sovranità regolatoria che emerge alla luce della legislazione europea in materia di intelligenza artificiale, in particolare analizzando il regolamento UE 2024/1689, che mostra un approccio innovativo in merito al

[12] In tale caso nell'elaborazione dell'atto una collaboratrice aveva usato ChatGPT (del cui utilizzo il patrocinatore non era a conoscenza) per individuare precedenti, ma il modello aveva prodotto sentenze inesistenti, generando numeri di Cassazione che sembravano legittimi ma che in realtà non esistevano.

[13] In questo caso l'atto introduttivo dell'opposizione contro ingiunzione di pagamento era stato redatto con il supporto dell'intelligenza artificiale generativa, ma conteneva un «coacervo di citazioni normative e giurisprudenziali astratte, prive di ordine logico e in larga parte inconferenti», senza allegazioni concrete riferite alla vicenda oggetto del giudizio. La parte è stata condannata al pagamento di 500 euro per ciascuna parte convenuta e a rifondere le spese processuali; si tratta del primo caso italiano in cui è stata riconosciuta in modo chiaro la responsabilità aggravata per lite temeraria legata all'uso non controllato dell'AI generativa nella stesura dell'atto processuale.

[14] Nel caso di specie il Tribunale ha rigettato un ricorso proposto da una parte rappresentata da un avvocato il quale aveva depositato atti difensivi che erano stati redatti "a stampone" mediante strumenti di intelligenza artificiale, senza adeguato controllo umano. La sanzione è stata individuata in 1.000 euro in favore della controparte e in ulteriori 1.000 euro a titolo di sanzione alla cassa delle ammende.

[15] Il ricorso verteva sull'annullamento del verbale di scrutinio finale del consiglio di classe con cui un'alunna non era stata ammessa alla classe successiva. Il difensore aveva citato numerose sentenze con estremi che risultavano non pertinenti o non attinenti alla materia del contenzioso: ha dichiarato di aver reperito quelle sentenze «mediante strumenti di ricerca basati sull'intelligenza artificiale che hanno generato risultati errati». Il Tribunale ha qualificato correttamente tale fenomeno come "allucinazioni da intelligenza artificiale".

rapporto tra essere umano, diritto e intelligenza artificiale. Il contributo osserva poi il modello nazionale disegnato dalla legge 132/2025 per coglierne punti di forza e debolezza. L'analisi mostra che l'umanesimo digitale su cui si erge la sovranità regolatoria europea e nazionale, basato sul rischio, sulla comprensibilità e sulla supervisione umana, determina un'evoluzione nei principi e negli strumenti giuridici, ma al tempo stesso mostra sfide inedite da affrontare.

Al fine di svolgere tale analisi, il saggio esamina il quadro regolatorio di riferimento al momento attuale, in particolare il regolamento UE 2024/1689 e la legge 132/2025, al fine di evidenziare il modello di sovranità regolatoria che fa leva sull'umanesimo digitale, evidenziandone i tratti caratteristici, ma altresì le problematiche che solleva. Preme precisare che sia a livello europeo che nazionale il quadro si farà maggiormente chiaro con l'implementazione completa del regolamento europeo, nel primo caso, e con le deleghe del Governo, nel secondo caso, che permetteranno di poter comprendere in modo concreto e maggiormente puntuale conformità e divergenze nel governo dell'intelligenza artificiale da parte della regolazione italiana rispetto alla cornice europea.

2. Il modello europeo di sovranità tecnologica

L'impatto della rivoluzione digitale si determina sotto vari profili che connotano l'esistenza umana, tra cui anche la dimensione dello spazio, e influisce, di conseguenza, sul diritto; si affermano diverse coordinate spaziali, dovute alla realtà globale di riferimento, priva di confini territoriali e "sovrani", che determina la rilevanza in materia del diritto sovranazionale. La *ratio* di tale aspetto si rinviene nell'esigenza di un approccio olistico per affrontare la dimensione digitale, dal momento che la realtà globale della rete implica un mutamento nei confini geografici della regolazione e rende necessario arrivare a soluzioni condivise in merito alla protezione dei diritti; la veste sovranazionale è necessaria a garantire efficacia alle norme, evitando la tensione altrimenti fisiologica tra la connotazione globale delle questioni e la dimensione territoriale delle disposizioni da applicare.

Lo spazio/non spazio digitale, inoltre, porta a ridefinire sfera pubblica e privata e prendono forma nuove geometrie di potere, in cui gli Stati sono depotenziati a causa del territorio globale di azione e della presenza delle aziende *Big Tech*, quali Amazon, Apple, Meta, Google, Microsoft, favoriti dalla stessa dimensione sovranazionale, dalla capacità di utilizzare le tecnologie, dalla libertà di impresa e dalla tutela dello sviluppo economico, dalle maglie ampie o dall'assenza di norme adeguate al mutato contesto. Le aziende Big Tech hanno avuto la capacità di dominare la dimensione globale grazie agli strumenti

dell'autonomia contrattuale privata, regolando l'accesso ai servizi e alle utilità della rete, incidendo così sui diritti e sulle libertà dei singoli[16].

I colossi tecnologici producono regole in un contesto di disintermediazione, in cui, usando una provocazione, danno vita un ordine algoritmico in cui agiscono simultaneamente e pericolosamente quale potere legislativo (dettano le regole), esecutivo (le applicano) e giudiziario (giudicano le violazioni con sanzioni quali la sospensione o la disattivazione dell'account). Si tratta di regole ampiamente accettate, seppur più o meno consapevolmente, capaci di influire sulla vita degli individui quanto le norme con efficacia vincolante prodotte dagli Stati; i nuovi "territori" delle piattaforme sono percepiti dalla collettività come spazi giuridici pubblici, sebbene privi di legittimazione democratica e guidati non dall'interesse pubblico, ma dal profitto economico.

Proprio il fatto che nella società tecnologica il diritto è chiamato a confrontarsi con le peculiarità globali dell'oggetto di regolazione e con mutate geometrie di potere ha determinato negli ultimi anni un articolato *framework* giuridico europeo diretto a disciplinare la dimensione digitale della vita umana, formato inizialmente prevalentemente da atti di *soft law* e in seguito da *hard law*, in particolare da un insieme di regolamenti quali il *Data Governance Act* (regolamento UE 2022/868), il *Digital Markets Act* (regolamento UE 2022/1925), il *Digital Services Act* (regolamento UE 2022/2065), il *Data Act* (regolamento UE 2023/2854) e l'*Artificial Intelligence Act* (regolamento UE 2024/1689; di seguito anche *AI Act*). La sfida dell'intelligenza artificiale impone un'analisi dell'*AI Act* non come atto isolato, ma come tassello di un ecosistema normativo complesso di cui fa parte[17].

Nel contesto europeo si assiste pertanto a un passaggio da un insieme di atti ascrivibili a *soft law*, ossia un sistema di regole non precettive e non vincolanti, comunque caratterizzato da un diverso grado di persuasività, ossia in grado di svolgere effettivamente una funzione di orientamento e di indirizzo nei confronti dei destinatari, sebbene non suscettibili di attuazione giudiziaria, a regolamenti europei, che in quanto tali si iscrivono a buon diritto nella categoria di *hard law*, ossia un sistema di regole giuridiche vincolanti, dotate di piena obbligatorietà in senso giuridico, suscettibili in caso di violazione di applicazione giudiziaria.

Le regole di *soft law*, infatti, seppur rispondano a quelle esigenze di flessibilità, adattabilità, rapidità, che emergono nella dimensione digitale, al tempo stesso scontano limiti nella regolazione della dimensione tecnologica per il fatto che non sono vincolanti, pongono rischi di incertezza interpretativa e, di conseguenza, applicativa, palesando rischi di disomogeneità. I regolamenti europei, tipicamente *hard law*,

[16] Sui poteri digitali cfr. F. OLIVERI, Machina mundi. *Per una regolazione democratica dei poteri digitali*, Mucchi editore, Modena, 2025.

[17] Cfr. A. IANNUZZI, *L'AI Act nell'ecosistema normativo europeo in tema di digitale tra continuità e discontinuità*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3, 2025, pp. 249-256; S. CALZOLAIO, E. LONGO, A. IANNUZZI, M. OROFINO, F. PIZZETTI (a cura di), *La regolazione europea dell'intelligenza artificiale nella società digitale*, Giappichelli, Torino, 2025.

nella loro applicabilità diretta agli Stati membri con la *vis* normativa di disapplicare eventuali norme interne che non siano conformi, superano i limiti delle regole di *soft law*, in quanto rispondono all'esigenza di certezza e prevedibilità, anche se rigidità, mancanza di flessibilità e tendenza alla staticità nel tempo possono essere critiche nel governo della dimensione digitale, motivo per cui questi atti si affidano a meccanismi di compensazione come il rinvio ad atti di *soft law* o meccanismi di flessibilità come gli strumenti di revisione e aggiornamento e gli spazi di sperimentazione normativa[18].

L'eterogeneità della tipologia degli atti deriva proprio dalle caratteristiche dell'oggetto di regolazione: la tecnologia è connotata dalla specificità tecnica, dal progresso scientifico e dall'evoluzione costante, che esigono qualificate competenze e comportano l'esigenza di atti puntuali, regole tecniche e strumenti flessibili, mentre la norma strettamente intesa si caratterizza per essere generale e astratta, frutto di un lungo *iter* scaturente dal processo democratico e tesa a durare nel tempo. Di conseguenza, è necessario un complesso articolato di regole diverse, atte a costruire una disciplina complessivamente sostenibile (e, dunque, efficace) e, a tal fine, tese a garantire flessibilità e adattabilità allo sviluppo e ai cambiamenti della tecnologia, assicurando altresì prevedibilità e certezza, principi solidi del diritto.

Nel *framework* europeo emerge questa tensione continua fra flessibilità e prevedibilità, al fine di garantire efficacia ma anche certezza, tutelando la persona rispetto alla macchina, riuscendo a trovare un virtuoso equilibrio tra interessi diversi ed essendo così capace di esprimere una concreta sovranità regolatoria in materia.

L'esigenza di flessibilità e adattabilità rispetto all'incessante evoluzione tecnologica e la conseguente necessità di aggiornamento determinano meccanismi quali nell'*AI Act* l'obbligo generale di revisione del regolamento e la procedura di modifica degli allegati connessi all'individuazione delle categorie dei sistemi ad alto rischio, anche al di fuori del procedimento legislativo ordinario altrimenti necessario; nella stessa ottica è possibile leggere le previsioni relative alle *regulatory sandboxes,* utili ad adattare le disposizioni a una realtà particolarmente complessa[19], e il ricorso ai codici di buone pratiche e ai codici di condotta, tesi a contribuire alla corretta applicazione delle norme[20]. Al riguardo, in relazione a modelli di intelligenza artificiale generativa, significativi esempi di tale esigenza di flessibilità sono il *General-Purpose AI Code of Practice*, documento volontario formalmente non vincolante, pubblicato il 10 luglio 2025 e redatto da esperti indipendenti con input da oltre 1.000 stakeholder come strumento di autoregolazione, e le successive *Guidelines on the Scope of Obligations of Providers of General-Purpose AI Models under the AI Act*,

[18] Sul ruolo della *soft law* in ambito di intelligenza artificiale cfr. P. INTURRI, *Intelligenza artificiale e soft law. Il ruolo dei codici di comportamento nell'Artificial Intelligence Act*, in *Nuove Autonomie*, fasc. 1, 2025, pp. 475- 495.

[19] L'attivazione delle *regulatory sandboxes* consente agli Stati membri, per un periodo di tempo limitato e sotto il controllo delle autorità competenti nazionali, di sviluppare e sperimentare sistemi di AI innovativi, ai fini di una successiva immissione nel mercato; art. 57 ss., reg. UE 2024/1689.

[20] Art. 56 ss. e art. 95 ss., reg. UE 2024/1689.

pubblicate dalla Commissione europea il 18 luglio 2025 per assistere i fornitori di modelli di AI per finalità generali ad adempiere agli obblighi del regolamento europeo.

L'esigenza di prevedibilità e certezza del diritto determinano il cambiamento stesso di approccio negli ultimi anni da parte dell'Unione europea con la tendenza a "inasprire" la forza degli atti normativi da *soft law* ad *hard law*, al fine di garantirne effettività ed omogeneità; il regolamento europeo con la sua maggiore *vis* sugli Stati membri prende il posto della direttiva nel quadro giuridico dedicato alla dimensione digitale[21]. In ogni caso non si rinuncia all'eterogeneità degli atti, al fine di garantire effettività: in tali disposizioni, infatti, si rinvia anche ad atti di *soft law* necessari per l'applicazione delle norme, come i richiamati codici di condotta. Inoltre, seppur lo strumento formale scelto per regolare la dimensione digitale sia il regolamento, oltre agli esaminati meccanismi di flessibilità, sono lasciati ampi margini di applicazione agli Stati membri, che equilibrano la maggior forza dell'atto con l'esigenza di garantire anche adattabilità ed efficacia, seppur possano causare anche incertezze e potenziali difformità nell'attuazione[22].

Il legislatore europeo, grazie a questi atti e a una maggiore *vis normativa* verso gli Stati membri, oltre ad esercitare un ruolo guida al fine di realizzare un ecosistema digitale sicuro, competitivo, antropocentrico e garantire un approccio comune degli Stati membri, mostra la volontà di costruire un modello etico, filosofico e giuridico di governo della tecnologia e, al tempo stesso, esprime il desiderio di affermare una sovranità digitale regolatoria rispetto ai poteri privati e ad altri blocchi geopolitici.

La sovranità statale, infatti, passa oggi dalla sovranità digitale, fondamento della moderna sovranità. Di conseguenza governare la società tecnologica solleva il problema della sovranità digitale, ossia la capacità dello Stato di avere accesso, controllo, gestione e protezione di dati, software e infrastrutture informatiche all'interno del proprio contesto geopolitico, senza dipendere da potenze, piattaforme o aziende esterne. Di conseguenza la sovranità digitale si esercita sui dati, sulle tecnologie, sulle infrastrutture, sul controllo relativo alle attività compiute nella dimensione digitale e sulla capacità di regolare attraverso norme. Proprio le diverse componenti su cui può esercitarsi danno vita agli attuali volti della sovranità digitale a livello geopolitico internazionale con un diverso approccio tra Stati Uniti, Cina e, appunto, Unione europea.

Mentre il modello statunitense poggia sulla sovranità delle piattaforme private, dotate di ruolo globale e dominio economico sul mercato, caratterizzata da un limitato intervento normativo a livello unitario e

[21] Tale tendenza ad abbandonare la direttiva era già in atto con i regolamenti europei 2016/679 sui dati personali e 2018/1807 sui dati non personali.

[22] Nell'*AI Act*, ad esempio, l'individuazione dei sistemi a rischio inaccettabile si connota per la presenza di concetti indeterminati ed interpretabili, che implica flessibilità applicativa e margini di manovra a favore degli Stati, ma anche possibile incertezza e correlate potenziali difformità nell'attuazione.

dalla cooperazione tra poteri pubblici e privati[23], diversamente il modello cinese si affida alla sovranità statale che si erge su un controllo diretto e pervasivo dello Stato su dati, infrastrutture, contenuti. Il modello cinese si articola in un approccio centralizzato, nel controllo e nella censura della rete Internet (con strumenti quali *firewall*, filtraggio, tracciamento) e nella costruzione di piattaforme interne autoctone, accompagnata dal blocco delle grandi piattaforme esterne. In tal modo il sistema cinese mira all'autonomia tecnologica, riducendo la dipendenza dall'esterno, oltre a garantire sicurezza e protezione dell'ordine sociale e politico, perseguita anche con la sorveglianza di massa (grazie a *smart cities*, *social scoring*, riconoscimento facciale)[24].

Tra logica liberista e approccio centralizzato l'Unione europea abbraccia una terza via e costruisce una sovranità regolatoria orientata dall'umanesimo digitale, producendo regole e ponendo condizioni giuridiche tramite l'insieme di atti e regolamenti dedicati alla dimensione tecnologica, cercando così di stabilire le regole del gioco a livello globale.

Il modello europeo si affida alla tutela dei diritti, del diritto e della democrazia rispetto al dominio dei poteri privati, esprimendo un'autonomia strategico/politica e mirando a realizzare un mercato digitale equo, interoperabile e sicuro, capace di dare vita a un modello antropocentrico che possa conquistare la fiducia degli utenti, protetti nei propri diritti fondamentali[25]. In questa operazione l'Unione europea si affida al cosiddetto *effetto Bruxelles*, ossia alla capacità di regolare i mercati globali in modo unilaterale grazie a un adeguamento volontario delle aziende alle regole europee al fine di evitare costi[26]. Tale capacità di influenza è in realtà ancora da verificare a livello concreto nel caso di regolamenti come quello sull'intelligenza artificiale, che sconta anzi l'ombra del *chilling effect*, ossia il fatto che le norme europee possano scoraggiare le imprese dall'intraprendere attività innovative nel mercato unico per timore di costi di *compliance* e sanzioni significative.

La sovranità regolatoria emerge da una serie di profili che sinergicamente danno vita al modello europeo di governo della tecnologia, in generale, e dell'intelligenza artificiale, in particolare, orientato all'umanesimo digitale e teso a realizzare un diritto sostenibile e, a tal fine, capace di raggiungere un saggio bilanciamento tra diritti e interessi diversi nella realtà digitale.

---

[23] Riguardo al modello statunitense rilevano gli standard tecnici e le *policy* non vincolanti come il *NIST AI Risk Management Framework* (2023), standard volontario e non prescrittivo, adattabile a diversi settori e dimensioni aziendali.

[24] In merito al modello cinese sono significative le *Interim Measures for the Management of Generative AI Services* (2023), secondo cui i contenuti generati dall'AI devono essere conformi ai "valori socialisti fondamentali" ed è vietato qualsiasi *output* che possa minare il potere statale o la stabilità sociale.

[25] A. D'ATTORRE, *La sovranità digitale. Poteri privati, intervento pubblico e diritti individuali nel cyberspazio*, in T. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche*, 2° ed., Cedam, Trento, 2024, pp. 313-324.

[26] Cfr. A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.

In primo luogo la sovranità regolatoria emerge proprio a livello strettamente giuridico, nel modo di esprimersi del diritto, ossia nella richiamata scelta di avvalersi di atti normativi di peculiare *vis* normativa come i regolamenti e di porsi come pioniera sotto il profilo regolatorio in ambiti come l'intelligenza artificiale. Proprio l'*AI Act* (regolamento UE 2024/1689) denota il fine europeo di porre le regole del gioco a livello globale nella previsione di un ambito di applicazione soggettivo particolarmente esteso, che, sulle tracce del precedente regolamento 2016/679 sulla protezione dei dati personali (*Brussels Effect*), mostra un effetto extraterritoriale rispetto ai confini europei, dal momento che si applica ai fornitori che immettono sul mercato o mettono in servizio sistemi o modelli di AI nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo e, altresì, ai fornitori e *deployer* di sistemi di AI che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'*output* prodotto dal sistema di AI sia utilizzato nell'Unione[27]. La portata extraterritoriale del regolamento mostra la volontà di avere un effetto normativo esteso a livello globale, che possa elevare l'attenzione e la tutela dei diritti fondamentali della persona, in linea con la tradizione normativa europea.

La sovranità regolatoria si declina anche nella costruzione di una solida *governance* per mezzo dell'istituzione di comitati e gruppi di esperti a livello sovranazionale, dedicati a specifici ambiti di azione o tecnologie (intelligenza artificiale, dati, servizi e mercati digitali) e chiamati a fornire assistenza e consulenza alla Commissione europea nell'applicazione uniforme dei regolamenti, quali l'*European Artificial Intelligence Board*[28], l'*European Data Innovation Board*[29], l'*European Board for Digital Services*[30], l'*high-level group for the Digital Markets Act*[31]. Nell'applicazione omogenea delle previsioni giuridiche e nel bilanciamento tra diritti e interessi diversi, il ruolo di questi organismi è fondamentale al fine di rispondere alle istanze di flessibilità e adattabilità, necessarie affinché le regole giuridiche possano essere efficaci, siano capaci di affrontare l'evoluzione tecnologica e diano vita a un diritto sostenibile. Del resto sostenibilità ed efficacia sono le strade lungo le quali è possibile esercitare una concreta sovranità regolatoria da parte dell'Unione europea.

In specifico, per quanto attiene all'intelligenza artificiale, il regolamento europeo prevede un'articolata *governance* a tutela della persona e del modello antropocentrico, che vede l'*European AI Office* all'interno della Commissione, il richiamato *European AI Board*, chiamato a consigliare e assistere la Commissione e gli Stati membri al fine di facilitare l'applicazione coerente ed efficace del regolamento, l'*Advisory forum* chiamato a consigliare e fornire competenze tecniche al Board e alla Commissione per contribuire ai loro compiti e, infine, il Comitato scientifico composto da esperti indipendenti a sostegno delle attività di

[27] Art. 2 reg. UE 2024/1689.
[28] Artt. 65-66, titolo VI, reg. UE 2024/1689.
[29] Art. 29 ss., reg. UE 2022/868 «*Data Governance Act*».
[30] Art. 61 ss., reg. UE 2022/2065 «*Digital Services Act*».
[31] Art. 40, reg. UE 2022/1925 «*Digital Markets Act*».

esecuzione[32]. Nella composizione dei diversi organismi emerge la specificità tecnica dell'intelligenza artificiale che motiva la presenza di competenze tecniche ed esperti indipendenti accanto a organismi maggiormente istituzionali e rappresentativi. Inoltre, in considerazione del modello *multilevel* previsto, il regolamento europeo prevede l'istituzione o la designazione di autorità nazionali competenti chiamate ad agire in modo indipendente e imparziale in materia.

In questa esigenza di g*overnance* emerge la volontà di recuperare uno spazio giuridico pubblico nei confronti dei poteri privati, al fine di ridurre asimmetrie e squilibri a protezione dei diritti della persona. Il pericolo, però, consiste nel rischio di far pendere la bilancia verso l'uno o l'altro diritto a protezione del quale o verso la tecnologia per la quale lo specifico organismo è istituito e conseguentemente si muove, perdendo l'approccio olistico necessario per affrontare la complessità della realtà digitale, caratterizzata dalla necessità di trovare un complesso equilibrio tra diritti e interessi diversi. La previsione di organi sovranazionali chiamati a contribuire all'applicazione efficace ed omogenea delle norme, pertanto, determina la necessità conseguente di una sinergica cooperazione tra loro, superando l'ambito settoriale di azione che rischia altrimenti di far smarrire il richiamato approccio complessivo necessario alla luce delle evidenti intersezioni tra i diversi regolamenti; esemplificativamente se si parla di intelligenza artificiale verrà in gioco anche la *data governance*, seppur siano oggetto di distinti regolamenti e di diversi organismi, che pertanto dovranno necessariamente cooperare tra loro.

La *governance* si configura come un sistema multilivello composto da organismi europei e autorità nazionali, dove l'impatto regolatorio del *Brussels Effect* deve armonizzarsi con le specificità istituzionali degli Stati membri. Tale aspetto, insieme alla concreta implementazione nei diversi Stati membri, evidenzia il rischio di una frammentazione regolatoria qualora le autorità nazionali non riescano a dialogare in modo simmetrico, potendo arrivare a minacciare l'efficacia stessa delle tutele previste. Il passaggio da una sovranità formale a una sostanziale richiede non solo un corretto recepimento normativo, ma la creazione di "ecosistemi di fiducia" dove il diritto europeo possa fungere da cornice assiologica e infrastruttura giuridica comune e le norme nazionali da leva operativa, garantendo l'effettività della norma[33].

Il fine di affermare la sovranità regolatoria europea, costruendo un diritto sostenibile, si manifesta altresì nell'esaminata eterogeneità degli atti che ospitano le regole, che si coniuga all'esaminata eterogenea *governance*: non solo *hard law*, ma anche *soft law* come atti di indirizzo, linee guida e strategie di soggetti istituzionali, autorità indipendenti, comitati, fino anche a gruppi di esperti nominati *ad hoc*; la complessità dei fenomeni è affrontata con strumenti eterogenei prodotti non solo dalle istituzioni pubbliche, ma anche da soggetti privati. Al fine di disciplinare la tecnologia in modo efficace e sostenibile, infatti, il

[32] Art. 64 ss., titolo VI, reg. UE 2024/1689.

[33] Cfr. A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020; M. HILDEBRANDT, *Law for Computer Scientists and Other Folk*, Oxford University Press, Oxford, 2020.

diritto deve tener conto ed integrare ecosistemi di regole diverse, come quelle informatiche, che dettano "legge" nella dimensione digitale, e, altresì, quelle poste dall'autonomia privata dai colossi tecnologici, che regolano i "territori" costituiti dalle estese piattaforme digitali su cui esercitano il proprio dominio.

Di conseguenza, la regolazione necessita di una genesi *multilevel*, di un approccio *multistakeholder* e dell'integrazione di fonti eterogenee, al fine di avvalersi dei diversi portatori di interessi e di una conseguente corresponsabilità da parte dei differenti produttori di regole, giuridiche o meno, della nostra contemporaneità. Pertanto, accanto alle norme poste dalle autorità pubbliche, rilevano forme di *co-regulation* e di *self-regulation*; gli Stati sono chiamati a nuove forme di cooperazione e collaborazione.

In coerenza con queste istanze che muovono il modello europeo, l'*Artificial Intelligence Act*, il regolamento UE 2024/1689, mostra a livello sostanziale un approccio innovativo in relazione al rapporto tra essere umano, diritto e intelligenza artificiale.

L'*AI Act* abbraccia un modello di umanesimo tecnologico teso a porre al centro la persona per mezzo di un approccio preventivo e proattivo basato sul rischio e sulla sua categorizzazione preventiva, in linea con la *legal protection by default e by design*, basata sull'*accountability*, che emerge già pienamente anche nel regolamento europeo 2016/679 in materia di protezione dei dati personali. L'individuazione dei sistemi a rischio inaccettabile, alto, basso, minimo viene basata sulla funzione, sulle modalità e sugli scopi delle diverse soluzioni di intelligenza artificiale; tale approccio proporzionato al rischio e teso a differenziare parallelamente il regime regolatorio di riferimento è consapevole della pluralità ed eterogeneità delle soluzioni di intelligenza artificiale, in cui può variare sensibilmente l'autonomia che le connota, la trasparenza che è possibile garantire e il controllo umano esercitabile.

Mentre i sistemi a rischio inaccettabile rappresentano il confine invalicabile dell'umanesimo digitale europeo, dal momento che l'intelligenza artificiale in tali casi è considerata una minaccia alla sicurezza e ai diritti dell'uomo e di conseguenza sono vietati, i sistemi ad alto rischio sono sottoposti a norme che seguono l'approccio di *accountability*, che pervade il regolamento europeo 2016/679. Nei casi "ad alto rischio", il regolamento europeo prevede, infatti, un insieme integrato di strumenti e requisiti da rispettare nel sistema di gestione dei rischi come documentazione tecnica adeguata, *data governance* e qualità dei *dataset* di addestramento, valutazione e dichiarazione di conformità, registrazione e tracciabilità, monitoraggio e vigilanza, misure appropriate di sorveglianza umana, oltre ad obblighi di trasparenza, accuratezza, robustezza e sicurezza, prevedendo sanzioni in caso di mancato rispetto di quanto previsto, che si atteggiano come strumenti di *enforcement* della disciplina. Pertanto in tali casi si fa leva su obblighi di conformità, obblighi di informazione e controlli tesi a verificare il rispetto dei requisiti[34]. Infine il

[34] Art. 8 ss., reg. UE 2024/1689. Cfr. G. ALPA, *Quale modello normativo europeo per l'intelligenza artificiale?*, in *Contratto e impresa*, fasc. 4, 2021, p. 1011.

regolamento europeo prevede obblighi specifici di trasparenza in caso di sistemi di AI a basso rischio, mentre consente il libero sviluppo ed uso in caso di sistemi di AI a rischio minimo[35].

L'approccio del regolamento europeo è preventivo e proattivo, ma in caso di mancato rispetto di quanto previsto sono previste sanzioni effettive e dissuasive, proporzionate al fatturato annuo globale.

Il modello di umanesimo digitale emerge con forza altresì nell'attenzione che le disposizioni pongono alla persona in alcuni strumenti normativi che mostrano parimenti l'approccio preventivo e proattivo che caratterizza l'*AI Act*: la valutazione d'impatto sui diritti fondamentali degli individui in relazione alla progettazione di sistemi di intelligenza artificiale ad alto rischio[36]; la previsione di requisiti obbligatori per tutti i sistemi di AI ad alto rischio e controlli di conformità prima e dopo l'immissione sul mercato, includendo l'obbligo di monitorare questi sistemi e affrontare tempestivamente potenziali rischi; l'indicazione nella documentazione tecnica per tali sistemi del rischio di discriminazione in considerazione della finalità prevista del sistema di AI.

Lo sviluppo e l'ascesa dell'AI generativa impatta sul concetto di sovranità regolatoria, spostando l'attenzione dai rischi puntuali ai rischi sistemici quali disinformazione di massa, rischi per la cybersicurezza o minacce ai diritti dell'essere umano. La regolazione europea si mostra consapevole delle caratteristiche peculiari dell'intelligenza artificiale generativa e gradua diversamente gli obblighi correlati. L'AI Act introduce, infatti, una distinzione fondamentale tra sistemi *General-Purpose AI* – GPAI (l'applicazione finale) e modelli *General-Purpose AI* – GPAI (l'architettura di base come i *Large Language Models*), imponendo obblighi che riflettono la posizione degli attori nella catena del valore. Mentre i sistemi GPAI sono soggetti alle regole basate sull'uso specifico, i modelli GPAI devono rispettare requisiti di base (trasparenza, documentazione tecnica e sintesi sul rispetto del diritto d'autore). Per i modelli che presentano un rischio sistemico (identificato dal parametro della potenza di calcolo superiore a una certa soglia), gli obblighi si fanno più stringenti[37].

Sotto tale profilo mentre l'approccio europeo con le disposizioni dell'AI Act sui modelli *general-purpose* mira anche in tal caso a una *governance* proattiva e a una logica preventiva definendo il perimetro di

[35] Queste categorie di sistemi risultano residuali rispetto a quelli a rischio inaccettabile e ad alto rischio; la loro circolazione è libera, salva l'ipotesi in cui, per le loro caratteristiche, non debbano essere stabiliti specifici obblighi di trasparenza.

[36] Art. 27, reg. UE 2024/1689, secondo cui prima di utilizzare un sistema ad alto rischio, salve eccezione, i *deployer* effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre, che comprende una descrizione dei processi del *deployer* in cui il sistema ad alto rischio sarà utilizzato in linea con la sua finalità prevista; una descrizione del periodo di tempo entro il quale ciascun sistema ad alto rischio è destinato a essere utilizzato e con che frequenza; le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone; una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla *governance* interna e ai meccanismi di reclamo.

[37] Art. 51 ss., reg. UE 2024/1689.

legittimità, la logica statunitense *market-oriented* si sta orientando verso forme di *self-regulation* guidata o responsabilità civile rafforzata. Questa divergenza riflette due visioni dell'umanesimo digitale: una, quella europea, proattiva e tesa alla tutela dei diritti, l'altra, quella statunitense, maggiormente reattiva e orientata al mercato[38].

3. Il modello nazionale di governo dell'intelligenza artificiale

Il modello europeo, teso a realizzare un diritto sostenibile nella dimensione digitale e nel governo dell'intelligenza artificiale, mostra pertanto la volontà di esprimere una sovranità regolatoria in materia, basata sull'umanesimo digitale e su un approccio antropocentrico, differenziandosi dal modello statunitense e dal modello cinese.

Al riguardo, seppur la dimensione sovranazionale sia quella adeguata alla regolazione in materia, non mancano atti a livello nazionale, per lo più strategici e stimolati dalla stessa Unione europea, cui da ultimo si è però sommato un vero e proprio atto normativo, la legge 132/2025.

Dopo una serie di strategie dedicate, la prima del 2018 con il Libro Bianco "*L'intelligenza artificiale al servizio del cittadino*" per poi arrivare alla Strategia italiana del 2020 e quella attuale del 2024-2026[39], nel settembre 2025 viene approvata la legge n. 132 in materia di intelligenza artificiale, che interviene in diversi ambiti.

Oltre a definizioni, ambito di applicazione, finalità e principi[40], le norme spaziano su diversi aspetti: si prevedono disposizioni di settore in ambiti significativi (ambito sanitario; lavoro; professioni intellettuali; pubblica amministrazione; attività giudiziaria)[41]; è prevista la necessità di una strategia nazionale; si designano quali autorità nazionali per l'intelligenza artificiale con correlata divisione di competenze AgID, competente per promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale, e l'Agenzia per la cybersicurezza nazionale (ACN), competente per la vigilanza e la promozione e sviluppo dell'AI relativamente alla cybersicurezza; si prevedono una serie di ampie deleghe al Governo; sono dedicate disposizioni alla tutela del diritto di autore; si introduce la sanzione penale dell'illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale.

Questa operazione mostra, a somiglianza di quanto avviene a livello europeo, la volontà di esprimere una sovranità regolatoria nazionale, pur dovendo necessariamente rimanere nei limiti di quanto previsto a

[38] Cfr. l'*Executive Order on Safe, Secure, and Trustworthy AI*, 2023.

[39] Si tratta dei seguenti atti: il Libro Bianco "*L'intelligenza artificiale al servizio del cittadino*", curato dall'AgID e dalla Task Force sull'IA composta da esperti nel marzo 2018; la Strategia italiana per l'intelligenza artificiale 2020, basata sulle proposte elaborate dal gruppo di esperti sull'AI nominato dal Ministero dello Sviluppo Economico 2019; la Strategia italiana per l'intelligenza artificiale 2024-2026, prodotta da parte del Comitato di Coordinamento per l'aggiornamento delle strategie sull'utilizzo dell'AI, istituito presso il Dipartimento per la Trasformazione digitale, composto da 13 componenti nominati ad ottobre 2023.

[40] Capo I, legge 132/2025.

[41] Capo II, legge 132/2025.

livello europeo dall'*AI Act*, che in quanto regolamento si applica direttamente agli Stati membri, disapplicando eventuali norme nazionali in contrasto.

Parimenti chiara è la volontà di sposare il modello di umanesimo digitale europeo e il volto antropocentrico dell'IA, come si desume già dalla disposizione di apertura, l'art. 1 della legge 132/2025. In linea con l'approccio europeo e con l'*AI Act*, la legge infatti dichiara espressamente che intende promuovere un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità e garantire la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali. L'atto normativo precisa, altresì, in modo opportuno che le norme si interpretano e si applicano conformemente al regolamento (UE) 2024/1689: del resto, non potrebbe essere altrimenti, data la tipologia di atti normativi di cui si parla.

L'umanesimo digitale e il correlato approccio antropocentrico emerge anche in norme maggiormente settoriali della legge 132/2025: l'art. 7, ai sensi del quale l'utilizzo dell'intelligenza artificiale in ambito lavorativo «deve essere sicuro, affidabile, trasparente e non può svolgersi in contrasto con la dignità umana né violare la riservatezza dei dati personali»; l'art. 13 secondo cui «l'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera» e, ancora, l'art. 14 secondo cui in caso di impiego nella pubblica amministrazione «l'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale». Stesso approccio nel settore della giustizia, dal momento che secondo l'art. 15 «nei casi di impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria è sempre riservata al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti».

In questo approccio aderente al modello europeo non mancano però criticità, scaturenti dalla scelta stessa del nostro Paese di legiferare in materia, che meritano qualche riflessione proprio in relazione alla sovranità regolatoria.

Al riguardo, infatti, la Commissione europea ha trasmesso all'Italia il 5 novembre 2024 un parere circostanziato (C(2024) 7814) circa potenziali criticità e sovrapposizioni tra l'allora disegno di legge nazionale e il regolamento europeo *AI Act*, solo in parte superate nelle modifiche apportate lungo l'iter parlamentare. Inoltre perplessità emergono sull'opportunità stessa di una legge nazionale in un momento in cui il regolamento non è ancora pienamente implementato e con cui possono aprirsi pericolose discrasie; quanto meno la tempistica non pare congrua. Più ampiamente, alla luce del modello europeo di sovranità regolatoria che l'Unione europea, come esaminato, cerca di affermare, la stessa approvazione

di una norma nazionale può risultare critica, perché può portare a una potenziale differenziazione con altri Stati e quindi a una frammentazione, in direzione diametralmente opposta alle finalità europee di uniformazione, che vengono perseguite con una *vis* normativa quale quella del regolamento, dotato anche di effetti extraterritoriali proprio al fine di imporsi a livello globale.

Le perplessità aumentano alla luce delle ampie deleghe al Governo, il cui esame, una volta prodotte, permetterà di cogliere la sostanziale portata dell'atto, e della clausola di invarianza finanziaria, secondo cui dall'attuazione non devono derivare nuovi o maggiori oneri a carico della finanza pubblica, che rischia di rendere le disposizioni mere dichiarazioni di intenti, senza che si traducano in norme effettive ed omogeneamente attuate, problematica che affligge tradizionalmente le disposizioni italiane in materia di innovazione e trasformazione digitale, si pensi al d.lgs. 82/2005 (codice dell'amministrazione digitale) e alle sue numerose riforme " a costo zero".

Anche la prevista *governance* duale con la designazione di AgID e ACN come autorità nazionali non risulta convincente, alla luce di una prevedibile difficoltà di distinzione delle rispettive competenze e conseguenti conflitti e sovrapposizioni. Lo snodo della *governance* è però cruciale per costruire la sovranità regolatoria europea, come precedente esaminato. Peraltro, date le rilevanti competenze già agite da tali autorità e la complessità dell'intelligenza artificiale, sommare questa competenza ad organismi esistenti potrebbe non rivelarsi la soluzione ottimale al momento dell'implementazione. Un'autorità terza e indipendente rispetto a quelle esistenti avrebbe verosimilmente garantito maggiore efficacia, neutralità e imparzialità, oltre ad assicurare un monitoraggio effettivo degli impatti etico-giuridici-sociali[42].

Pertanto la direzione italiana disvela alcune criticità alla luce della sovranità regolatoria europea, che a livello sostanziale cerca di affermarsi costruendo un modello di umanesimo tecnologico, basato su paradigmi e strumenti innovativi, che è necessario esaminare.

4. Umanesimo tecnologico e *digital law*

Nella regolazione europea, che mostra un inedito volto del diritto nella peculiare tipologia di sovranità digitale, sono contenuti strumenti e direzioni, che costituiscono paradigmi nuovi a livello sostanziale, permettendo di ravvisare un contenuto innovativo del diritto.

Innanzitutto, muta significativamente l'approccio sostanziale, dal momento che si sceglie di regolare e influire sulle geometrie di potere incidendo sui poteri privati, giacché, seppur si promuova lo sviluppo

[42] Inoltre, sotto il profilo della *governance*, al fine di garantire un approccio olistico nel governo dell'AI, sarebbe stato opportuno prevedere meccanismi stringenti di stretto coordinamento con altre autorità esistenti che esercitano indiscutibilmente funzioni in relazione all'intelligenza artificiale, al fine di realizzare strategie condivise in modo orizzontale, evitando verticalizzazioni, come il Garante per la protezione dei dati personali e l'Autorità Garante per le garanzie nelle comunicazioni; si prevedono invece solo generici e poco chiari concetti di "coordinamento e collaborazione".

economico e il progresso tecnologico, si mira a proteggere in modo più efficace gli utenti, istituendo un quadro di regole in materia di responsabilità e individuando, di conseguenza, obblighi di diligenza e trasparenza a carico delle aziende private, come nel caso del *Digital Services Act* e del *Digital Markets Act*.

Il legislatore europeo si mostra consapevole che, al fine di costruire un solido modello di governo della tecnologia, ispirato ai principi degli ordinamenti democratici, è necessario superare le problematiche relative al rapporto tra diritto e tecnologia, che trovano fondamento nelle esaminate criticità legate alle geometrie di potere e al funzionamento di dati e algoritmi, come la significativa asimmetria tra le parti in gioco e l'opacità dei processi di gestione. Il modello europeo di governo della tecnologia fa leva su alcuni strumenti, soluzioni e paradigmi, capaci di innovare profondamente i paradigmi tradizionali e minimizzare tali rischi, riequilibrando le asimmetrie a favore della collettività e proteggendo la persona, seppur non siano scevri da criticità.

Nella regolazione europea il rapporto tra diritto e tecnologia matura nella costruzione di un umanesimo digitale[43] e di una *governance* antropocentrica, capace di conferire piena centralità alla persona, per tutelare la quale è necessario un adeguato contesto istituzionale e un bilanciamento mobile tra diritti in una logica che mantenga la tecnologia strumento nelle mani dell'uomo; tale approccio è abbracciato dagli atti di *soft law* e *hard law* relativi all'intelligenza artificiale[44].

La *governance* umanocentrica, guidata da un approccio etico-filosofico-giuridico, può essere realizzata sfruttando la tecnologia stessa e la relazione tra regole giuridiche e informatiche; il diritto si avvale della tecnica per garantire il suo rispetto[45] e, di conseguenza, l'approccio preventivo e proattivo prende forma in due profili sinergici e connessi: il *legal protection by default* e *by design* e il *risk-based approach*.

L'incorporazione preventiva di principi etici e giuridici, norme e rimedi nella tecnologia stessa, ossia una *legal protection by default* e *by design*, basata sull'*accountability*, presente fin dal regolamento europeo 2016/679[46], emerge negli atti europei dedicati a dati e algoritmi quale paradigma capace di risolvere o quanto meno minimizzare le problematiche afferenti al rapporto tra diritto e tecnologia. Il diritto può

[43] Cfr. A. PUNZI, *Difettività e giustizia aumentata. L'esperienza giuridica e la sfida dell'umanesimo digitale*, in *Ars Interpretandi*, fasc. 1, 2021, p. 113 ss.

[44] Sulle problematiche poste dalla regolazione e dagli aspetti giuridici dell'AI cfr., *inter alia*, L. FLORIDI, *La differenza fondamentale. Artificial Agency: una nuova filosofia dell'intelligenza artificiale*, Mondadori, Milano, 2025; E. MAESTRI (a cura di), *op. cit.*; G. PASCUZZI, *Il diritto dell'era digitale*, 6° ed., il Mulino, Bologna, 2025, p. 303 ss.; G. SARTOR, *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022; F. CASA, S. GAETANO, G. PASCALI (a cura di), *Intelligenza artificiale: diritto, etica e democrazia*, il Mulino, Bologna, 2025; C. NOVELLI, F. CASOLARI, A. ROTOLO, M. TADDEO, L. FLORIDI, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in *Digital Society*, vol. 3, 2024, pp. 1-29; C. SARRA, *Dignità umana nell'era dell'intelligenza artificiale e della datificazione*, Kront, 2025.

[45] In merito al rapporto tra etica e diritto in materia di AI cfr., *inter alia*, F.H. LLANO-ALONSO, *L'etica dell'intelligenza artificiale nel quadro giuridico dell'Unione europea*, in *Ragion Pratica*, fasc. 2, 2021, p. 327 ss.; M. CATANZARITI, *Etica "artificiale": un nuovo modello regolatorio?*, in *Ars Interpretandi*, fasc. 1, 2021, p. 165 ss.

[46] Si tratta dei principi *data protection by design* e *by default*, cui si affianca il *data protection impact assessment* (artt. 25 e 35, reg. UE 2016/679).

avvalersi della tecnologia per garantire il suo rispetto, generando un modello di "diritto nella tecnica" (*code is law – law is code*). Si tratta di un approccio proattivo, che tutela la persona fin dalla progettazione, per impostazione predefinita e per mezzo della valutazione d'impatto sui diritti, capace di far leva sulla conformazione dei sistemi tecnologici e sulla sicurezza informatica, da una parte, e sulla responsabilizzazione e sulla consapevolezza dei soggetti, dall'altra, al fine di confinare le repressioni prevalentemente alla tutela sanzionatoria successiva, senza reprimere eccessivamente la libera circolazione dei dati e lo sviluppo economico; tale modello pervade il regolamento europeo 2024/1689 (*AI Act*).

Proprio l'*AI Act* sviluppa ulteriormente questa prospettiva, abbracciando un approccio proattivo basato sul rischio coadiuvato anche da un correlato sistema sanzionatorio, che si articola nella categorizzazione preventiva del rischio stesso, distinguendo quattro categorie (inaccettabile, alto, basso, minimo), cui si collega una regolazione differenziata.

Il *risk-based approach*, che mira a una protezione preventiva, capace di ridurre o eliminare la probabilità stessa che possano verificarsi violazioni, ha la capacità di raggiungere un equilibrio nella tutela dei diversi interessi in gioco, dal momento che è teso alla tutela dei diritti, ma è anche orientato alla crescita economica, giacché il produttore può considerare la *legal compliance* come un costo di produzione che entra nel costo economico della propria attività piuttosto che affrontare l'alea di dover eventualmente rispondere di possibili violazioni[47]. Il sistema di responsabilità distingue in base alle categorie di operatori di sistemi di intelligenza artificiale ad alto rischio o meno, motivando la responsabilità dell'operatore con il fatto che sta controllando un rischio associato alla specifica tecnologia; tale modello proporzionato al rischio è consapevole dell'eterogeneità delle soluzioni tecnologiche di intelligenza artificiale, in cui può variare sensibilmente l'autonomia che le connota, la trasparenza che è possibile garantire e il controllo umano esercitabile.

Al fine di rendere efficace l'approccio proattivo basato sul rischio, molto significativo, oltre che concreta leva della sovranità regolatoria europea, è l'*enforcement* costruito dal regolamento europeo, che poggia su un solido meccanismo sanzionatorio basato sul *turnover* annuo globale, che prevede sanzioni amministrative pecuniarie che possono raggiungere i 35 milioni di euro o il 7% del fatturato mondiale totale annuo dell'esercizio precedente, a seconda di quale sia l'importo più elevato per le violazioni relative alle pratiche vietate[48].

L'approccio proattivo, che prende vita nell'incorporazione preventiva del diritto nella tecnica e nel *risk-based approach*, non è però scevro da criticità, quali la "rigidità" ontologica del codice informatico, che si scontra con la flessibilità necessaria al bilanciamento "mobile" idoneo a una tutela efficace dei diritti, oltre

[47] Cfr. F. FAINI, *Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina*, in *federalismi.it*, n. 2, 2023, pp. 1-29.
[48] Art. 99 reg. UE 2024/1689.

all'opacità linguistica, che deriva dal fatto che il linguaggio è informatico e non è quello naturale delle norme giuridiche. Risulta complesso anche individuare quali principi etici e giuridici incorporare in tecnologie per lo più destinate a utilizzi transnazionali, dato il pluralismo etico e giuridico che caratterizza i diversi blocchi geopolitici e i differenti ordinamenti. Ulteriore significativa problematica di tale prospettiva si annida nel fatto che in tal modo il rispetto dei principi giuridici e l'equilibrio tra diritti sono di fatto delegati a coloro che sono chiamati a sviluppare le soluzioni tecnologiche e alle categorie di operatori nel mercato con conseguenti possibili problematiche.

Accanto al *risk-based approach*, nella regolazione dedicata all'intelligenza artificiale un paradigma significativo emerge nell'attenzione che viene tributata al rapporto tra uomo e macchina, che deve prevedere la supervisione umana e la non esclusività della decisione algoritmica, al fine di mantenere servente la tecnologia rispetto all'uomo. Supervisione e sorveglianza umana, tese a prevenire e minimizzare rischi e pericoli, risultano in linea con l'approccio proattivo e preventivo che connota il modello di *governance* della tecnologia. Al fine di costruire un modello antropocentrico, infatti, è necessario mantenere equilibrio tra uomo e macchina attraverso la garanzia dello "*human in the loop*"; al riguardo rileva il fatto che la tecnologia non è più soltanto un mezzo per realizzare azioni, ma sempre più spesso è essa stessa a prendere autonomamente decisioni significative per la persona umana, laddove impiegata per tali scopi.

L'*AI Act* prevede misure atte a consentire a chi è affidata la sorveglianza umana di comprendere e interpretare il sistema, intervenire sul funzionamento del sistema o interromperlo, decidere in modo autonomo se utilizzarlo e «restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema ad alto rischio ("distorsione dell'automazione")»[49].

Le misure concrete previste dall'*AI Act* sono tese a garantire una sorveglianza umana sostanziale ed evitare il rischio che la decisione umana possa essere "attratta" dai risultati della macchina; il problema, infatti, si annida nelle influenze e nella capacità "attrattiva" a livello pratico della soluzione offerta dall'intelligenza artificiale e nella correlata difficoltà per l'uomo di discostarsi con la propria valutazione da quanto emerge dal sistema, finendo per conformarsi al risultato suggerito: in tal modo, di conseguenza, si svuota sostanzialmente l'autonomia della decisione umana.

Al riguardo però occorre interrogarsi se e come sia possibile conciliare supervisione e sorveglianza umana con gli algoritmi di *machine* e *deep learning*, atti ad apprendere autonomamente e ad operare secondo processi decisionali opachi e non prevedibili per gli stessi programmatori, rispetto ai quali pertanto

[49] Art. 14, reg. UE 2024/1689.

devono essere verificate le effettive possibilità per l'uomo di mettere in discussione i risultati cui perviene la macchina, controllare la correttezza dei dati e correggere gli *output*.

A ben vedere costituisce condizione necessaria per la supervisione umana l'*explainability*, dal momento che, solo se l'essere umano è in grado di comprendere il modo in cui l'intelligenza artificiale decide, può operare un controllo effettivo e, se necessario, correggerne gli *output*. E, infatti, comprensibilità e sindacabilità sono ulteriori paradigmi su cui si concentra la regolazione europea. In particolare si tratta di garantire una declinazione rafforzata della trasparenza, che assicuri conoscibilità, comprensibilità e sindacabilità, rendendo gli algoritmi oggetto di cognizione e sindacato da parte dell'uomo, al fine di superare l'opacità: tale principio si traduce nell'assicurare non solo informazioni e accesso ai dati, ma anche la conoscenza della logica che governa gli algoritmi, accompagnata dalla consapevolezza in merito alle conseguenze e all'impatto sulla persona.

Nei confronti di dati, algoritmi e intelligenza artificiale, pertanto, devono essere attribuiti e riconosciuti il diritto alla comprensibilità, capace di rendere consapevole l'interessato, e il diritto alla contestabilità, idoneo a consentire all'interessato, anche per mezzo di un giudice, di valutare e di sindacare la decisione a cui perviene la tecnologia. Tali diritti si traducono nel diritto del singolo di mantenere autonomia, autodeterminazione e libertà nei confronti della macchina, che a sua volta comporta l'esigenza di comprensione dei meccanismi di funzionamento e una sorta di correlato dovere di "spiegare" in capo all'intelligenza artificiale o, meglio, in capo a chi ne è responsabile[50]. In linea con l'umanesimo tecnologico l'*explainability* assicura che l'intelligenza artificiale rimanga strumentale rispetto a quella umana e la tecnologia mantenga la sua funzione "servente" rispetto all'uomo e alle sue decisioni, soprattutto laddove incida su diritti e libertà[51].

L'*AI Act* mostra particolare attenzione per la trasparenza, prevedendo che siano fornite informazioni chiare e adeguate all'utente sia in caso di sistemi "ad alto rischio", sia in caso di sistemi "a basso rischio". Ogni sistema ad alto rischio deve essere disegnato e sviluppato in modo da assicurare un appropriato livello di trasparenza (*sufficiently transparent*), mostrando in tal modo consapevolezza circa la necessità di misure proporzionate, senza imporre obblighi irrealizzabili alla luce delle caratteristiche tecnologiche, come tali destinati ad una concreta inefficacia[52]; emerge con evidenza l'esigenza di sostenibilità del diritto. Alla trasparenza algoritmica si accompagna la necessaria trasparenza da parte di chi governa gli algoritmi, coniugandosi pertanto l'esigenza di comprensibilità delle macchine con la necessità di una correlata trasparenza da parte degli uomini che le gestiscono; in tal senso rileva il *Digital Services Act*, che impone

[50] M. PALMIRANI, Big Data *e conoscenza*, in *Rivista di Filosofia del diritto*, fasc. 1, 2020, p. 73 ss. In merito cfr. *inter alia*, S. SAPIENZA, *Decisioni algoritmiche e diritto*, Giuffré Francis Lefebvre, 2024

[51] Cfr. U. PAGALLO, *Algoritmi e conoscibilità*, in *Rivista di Filosofia del diritto*, fasc. 1, 2020, p. 93 ss.

[52] Art. 13, reg. UE 2024/1689.

alle piattaforme doveri di trasparenza e diligenza in merito agli algoritmi utilizzati, essendo tenute ad obblighi di motivazione nei confronti degli utenti e alla valutazione dei rischi sistemici collegati[53].

Mentre il dibattito di matrice nordamericana e britannica tende a inquadrare l'*accountability* algoritmica attraverso il prisma dell'efficienza, della correttezza e della mitigazione dei *bias*, la letteratura europea sottolinea come l'*explainability* rappresenti un diritto "abilitante" prodromico all'esercizio degli altri diritti e a mantenere l'autonomia e la libertà dell'uomo: senza la comprensione della logica decisionale, il soggetto è declassato da fine a mezzo del processo tecnologico, mentre l'obiettivo è proprio mantenere la tecnologia servente rispetto all'uomo in linea con l'approccio antropocentrico[54].

Al riguardo, però, la natura degli algoritmi pone il problema se esista sempre una logica comprensibile, dato il funzionamento degli stessi e la conseguente possibile non intelligibilità secondo criteri logico-razionali. L'intelligenza artificiale si affida a connessioni e inferenze tra dati e poggia sull'approccio statistico e probabilistico, determinando talvolta difficoltà di comprensione circa le motivazioni (il "perché") delle risposte fornite, aspetto che rileva particolarmente anche in caso di utilizzo dell'intelligenza artificiale generativa che può incorrere in allucinazioni[55]. Pertanto garantire trasparenza può essere particolarmente complesso a fronte di una congenita opacità degli algoritmi, che si declina in un'opacità strutturale, derivante dal funzionamento e dal fatto che resta non comprensibile persino ai programmatori l'iter logico seguito dalla macchina per giungere al risultato partendo dai dati a disposizione, cui si somma l'opacità linguistica dovuta al linguaggio informatico[56]. Tale aspetto può risultare particolarmente problematico in caso di utilizzo dell'intelligenza artificiale in ambiti giuridici quali l'amministrazione pubblica e la giustizia, dal momento che sia i provvedimenti amministrativi (art. 3, legge 241/1990) sia quelli giurisdizionali (art. 111, comma 6, Costituzione) devono essere necessariamente accompagnati da una motivazione[57].

Inoltre la declinazione dell'*explainability* non è un concetto unitario, ma si articola su diversi livelli di granularità e occorre distinguere tra spiegabilità *ex ante* e *ex post*. La prima riguarda la trasparenza statica del sistema, che si basa sulla documentazione tecnica e sulle logiche del modello, mentre la seconda attiene

[53] Artt. 4, 34 e 35, reg. UE 2022/2065.

[54] Cfr. F. PASQUALE, *The Black Box Society*, Harvard University Press, Harvard, 2015; L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina, Milano, 2022.

[55] P. MORO, *op. cit.*, p. 19.

[56] Cfr. G. FIORIGLIO, *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici*, in *Ars Interpretandi*, fasc. 1, 2021, p. 53 ss.; A. IANNUZZI, *Lingua del diritto, lingua dell'Intelligenza Artificiale. Una prima riflessione*, in *Rivista italiana di informatica e diritto*, fasc. 2, 2025, che propone l'uso dell'AI generativa come i *Large Language Models* (LLM) per facilitare la comunicazione tra questi due mondi, migliorando la comprensione del diritto e la trasparenza delle decisioni dell'AI nell'ambito giuridico.

[57] Sugli strumenti di garanzia e controllo per un umanesimo digitale cfr. L. DURST, *Diritto e predittività: spunti introduttivi in tema di sistemi decisori automatizzati*, in F. FABRIZZI, L. DURST (a cura di), *Controllo e predittività. Le nuove frontiere del costituzionalismo nell'era dell'algoritmo*, Editoriale scientifica, Napoli, p.11 ss.

alla capacità di fornire una motivazione specifica per una singola decisione automatizzata, fondamentale per assicurare i diritti[58]. Se manca la spiegabilità *ex ante*, il problema è l'imprevedibilità sistemica, ossia l'incapacità strutturale di prevedere come il sistema si comporterà nel tempo e in contesti reali, ma se il sistema è spiegabile *ex ante* ma non fornisce la motivazione della singola scelta (*ex post*), il problema risiede nell'impossibilità della difesa, che determina per l'individuo il rischio di subire una decisione "oracolare" con un conseguente vuoto di tutela derivante dalla mancata comprensibilità e contestabilità. In tal modo la tecnologia cessa di essere uno strumento e l'utente perde la dignità di essere un cittadino con diritti per divenire un "dato" processato da una macchina.

5. Riflessioni e sfide filosofico-giuridiche

Alla luce di tali profili, il modello giuridico di umanesimo digitale, che prende forma nella sovranità regolatoria europea e nella legislazione nazionale in materia, si serve della tecnologia, chiamata a implementare previamente principi etico-giuridici, ad essere comprensibile e connotata dalla sorveglianza umana sostanziale, oltre a basarsi sul *risk-based approach* e sull'*accountability* da parte di chi governa la tecnologia. Gli strumenti disegnati dal *framework* europeo, teso ad dare vita a una sovranità regolatoria in materia, infatti, permettono di affrontare le problematiche che affliggono il rapporto tra diritto e tecnologia, giacché intervengono sulle asimmetrie e sull'opacità contribuendo a "svelare" preventivamente problemi, consentendo di progettare la soluzione tecnologica diversamente, e, laddove il problema non sia emerso prima, permettono, altresì, di intervenire anche *ex post* grazie a trasparenza e contestabilità, tutelando la persona, oltre che per mezzo di un severo sistema sanzionatorio.

Nello sforzo regolatorio europeo si assiste a un rinnovamento del diritto che passa da una costruzione di matrice *multistakeholder* ed è guidato da un approccio filosofico-giuridico, orientato verso la tutela dei diritti. In tale contesto è condivisibile l'individuazione di organismi sovranazionali europei dedicati al governo della tecnologia, dotati di un certo grado di indipendenza rispetto a quei poteri che possono avere svariati interessi a orientarlo verso specifiche direzioni (poteri pubblici e privati). A questo si somma una logica *multilevel* negli spazi di autonomia lasciati agli Stati membri e nella previsione di una *governance* interna dedicata all'intelligenza artificiale, profili che nel caso italiano hanno portato a una vera e propria legge.

Del resto il cambiamento pervasivo determinato dallo sviluppo delle tecnologie come l'intelligenza artificiale investe gli equilibri tra diritti, il bilanciamento tra interessi, il rapporto tra poteri e la tenuta dei principi democratici fondamentali, influenzando le direttrici etiche e giuridiche del futuro. Di conseguenza le scelte filosofiche, etiche e giuridiche del modello europeo di governo della tecnologia

[58] Art. 86, reg. UE 2024/1689.

coinvolgono la relazione tra uomo e macchina, ma altresì il rapporto tra pubblico e privato. Tali scelte generano alcuni interrogativi. Quale forma del diritto è necessaria per assicurare effettività? Quale modello è adeguato al mutato contesto? Quali sfide deve affrontare il modello di sovranità regolatoria digitale?

Nel quadro europeo emerge la sfida di trovare un punto di caduta tra certezza/prevedibilità e flessibilità/adattabilità, garantendo equilibrio tra tutela della persona e promozione dello sviluppo economico, al fine di costruire un diritto efficace e sostenibile. Sotto tale profilo la sfida fondamentale si articola nella concreta capacità di implementare l'umanesimo digitale, senza essere freno o rallentamento allo sviluppo tecnologico e assicurando la sostenibilità del modello per piccole e medie imprese e, più ampiamente, per il mercato. L'approccio, i paradigmi e gli strumenti di *legal protection by design*, *risk-based approach*, sorveglianza umana e trasparenza algoritmica toccano e ruotano sul rapporto tra diritto e tecnologia, da un lato, e su quello tra essere umano e tecnologia dall'altro, con il comune scopo di riuscire a controllare e governare l'intelligenza artificiale, mantenendola strumento servente nelle mani dell'uomo, al fine di tutelare diritti e valori europei.

L'Unione europea esprime la propria sovranità regolatoria con un rafforzamento dello spazio giuridico pubblico, perduto nel dominio dei poteri privati e nella correlata asimmetria con gli utenti che caratterizza la realtà digitale, rafforzamento che si cerca di affermare anche grazie a organismi indipendenti, capaci ontologicamente di trovare quell'equilibrio tra certezza e flessibilità e creare così un diritto sostenibile. Di conseguenza la riflessione deve concentrarsi anche sull'opportunità di creare nuovi modelli di governo della tecnologia, dando vita a un'applicazione normativa congiunta e a una forte collaborazione tra gli organismi sovranazionali, abbracciando il necessario approccio olistico conforme alla complessità digitale e all'intreccio tra interessi diversi, oltre che garantendo ruoli diversi e complementari tra Unione europea e Stati membri nell'implementazione del modello disegnato a livello normativo.

Il modello di governo dell'intelligenza artificiale cui siamo e dovremmo essere diretti vede una nuova relazione tra diritto e tecnologia orientata dall'umanesimo digitale e capace di garantire prevedibilità e certezza, riuscendo al tempo stesso a tutelare in modo efficace l'uomo con strumenti dotati di flessibilità e adattabilità: un diritto sostenibile, capace di tutelare la libertà dell'uomo grazie a un saggio equilibrio tra diritti, facendo leva su un approccio olistico, al cui centro situare l'essere umano rispetto al quale la tecnologia, in generale, e l'intelligenza artificiale, in particolare, conservino la natura ontologica e necessaria di strumento nelle sue mani.