LA TUTELA DELLA *PRIVACY* NELLA PROFILAZIONE ALGORITMICA: SFIDE E PROSPETTIVE DELL'AI ACT*

di Cesaria Claudia Losito **

Sommario. 1. Introduzione: l'intelligenza artificiale come fenomeno giuridico e la risposta europea alla tutela dei diritti fondamentali. – 2. Il fondamento giuridico della *privacy*: un diritto fondamentale stratificato. – 3. AI Act e GDPR: un rapporto di interazione e integrazione. – 4. AI Act come modello basato sulla classificazione del rischio e l'autocertificazione del fornitore: un «vizio genetico» del sistema? – 5. AI Act: tra criticità e prospettive.

1. Introduzione: l'intelligenza artificiale come fenomeno giuridico e la risposta europea alla tutela dei diritti fondamentali. L'avvento dell'IA[1] rappresenta una vera e propria rivoluzione che sta ridefinendo le fondamenta stesse della nostra società, toccando ogni aspetto della vita umana: dall'economia al lavoro, dalla sanità all'educazione, fino al modo in cui si interagisce con le istituzioni pubbliche e private. Questa forza trasformativa, pur portando con sé immense promesse di efficienza, innovazione e miglioramento dei servizi, solleva al contempo interrogativi profondi di natura etica, sociale e giuridica, soprattutto in relazione al suo impatto sui diritti inalienabili dell'individuo[2].

La rapidità con cui tali tecnologie si diffondono, unita alla loro integrazione nei processi decisionali quotidiani, contribuisce inoltre a creare un divario significativo tra la capacità della società di comprenderne i meccanismi e l'idoneità dei sistemi ad evolversi autonomamente.

---

* *Sottoposto a referaggio.*

** Dottoranda in Economia e Finanza delle Amministrazioni Pubbliche – Università degli Studi di Bari Aldo Moro.

[1] Sull'ambiguità della definizione di Intelligenza Artificiale v. G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022. Alcuni autori discutono l'opportunità di usare il termine «intelligenza» per descrivere il fenomeno, proponendo di sostituirlo con «agentività» o «agenzia artificiale priva di intelligenza». Quest'ultimo concetto indicherebbe una forma di agenzia emergente basata su obiettivi programmati e comportamenti appresi che non implica capacità di coscienza o intenzionalità proprie. Tale «agentività» è caratterizzata da un adattamento guidato dai dati e da una funzionalità distribuita, ma priva di coscienza, intenzionalità e intelligenza contrapposta alla capacità di un agente (persona, essere vivente, entità) di agire in modo indipendente, di esercitare un potere causale sul mondo e di fare delle scelte libere. Sul tema, v. L. Floridi, *Artificial Intelligence as a New Form of Agency (not Intelligence) and the Multiple Realisability of Agency Thesis*, in *SSRN Journal*, 2024, che sottolinea come il cambio terminologico sia cruciale per sviluppare politiche adeguate.

[2] Tra gli altri, S. Amato, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Torino, 2020; T. Casadei, S. Pietropaoli, *Intelligenza artificiale: l'ultima sfida per il diritto?*, in T. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Padova, 2024, 259 ss.; M. Durante, *Potere computazionale. L'impatto delle ICT su diritto, società, sapere*, Milano, 2019; L. Floridi, *Etica dell'intelligenza artificiale, sviluppi, opportunità, sfide*, Milano, 2022; L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Roma, 2020; S. Sapienza, *Decisioni algoritmiche e diritto*, Milano, 2024; G. Sartor, *L'intelligenza artificiale e il diritto*, cit.

Tale asimmetria cognitiva tra esseri umani e sistemi algoritmici alimenta un crescente bisogno di strumenti giuridici per governarne l'utilizzo in modo democratico, responsabile e trasparente[3].

La specificità dell'IA, che la distingue nettamente dalle precedenti innovazioni tecnologiche, è qualitativa: non si tratta solo di «velocità di calcolo» o di «potenza elaborativa»[4]; le sue capacità uniche e il modo in cui interagisce con il mondo e con noi esseri umani presentano caratteristiche inedite che sollevano sfide giuridiche ed etiche mai affrontate prima, tanto che alcuni hanno parlato di un «nuovo potere sovrano»[5]. I sistemi di *machine learning*, fulcro di molte applicazioni IA moderne, sono progettati per modificare continuamente i propri meccanismi decisionali, integrando in modo autonomo nuove conoscenze a partire dai dati. Questo dinamismo rende intrinsecamente difficile comprendere le logiche di funzionamento di tali sistemi, dando origine al noto problema della «Scatola Nera»[6]. Tale opacità, spesso legata alla complessità dei modelli algoritmici, rende arduo anche per esperti il sindacato delle decisioni prese dall'IA, minando i principi di trasparenza e *accountability*[7].

Ciò è particolarmente vero nel settore pubblico, dove l'impiego di algoritmi decisionali rischia di incidere su diritti fondamentali quali quelli a un equo procedimento, alla non discriminazione e alla protezione dei dati personali. L'incapacità di comprendere pienamente le logiche sottese ai processi decisionali automatizzati solleva, inoltre, interrogativi sulla legittimità democratica di tali strumenti, soprattutto quando intervengono in ambiti che tradizionalmente appartengono alla discrezionalità amministrativa[8]. A ciò si aggiunga la capacità dell'IA di inferire e fare previsioni con un elevato grado di autonomia, analizzando e correlando vastissime quantità di dati (*Big Data*). Questa capacità predittiva, se da un lato offre opportunità in termini di efficienza, dall'altro comporta rischi significativi e amplificati di violazione della *privacy* e di discriminazione. La profilazione algoritmica, ad esempio, non

---

[3] Sul tema della necessità di una regolazione giuridica dell'intelligenza artificiale e della sua incidenza sui diritti fondamentali, sul sistema delle fonti e sui principi dello Stato costituzionale, si vedano, tra gli altri, A. Pirozzoli, *L'intelligenza artificiale e il diritto: AI ruled ed AI ruler,* in *Consultaonline*, 3, 2025, 1915-1924, che distingue tra l'intelligenza artificiale quale oggetto di regolazione (AI *ruled*) e quale fattore di trasformazione del diritto (AI *ruler*); G. De Minico, *Le fonti del diritto: un argine all'intelligenza artificiale?,* in *Rivista AIC,* 3, 2025, 76-100, che affronta il rapporto tra intelligenza artificiale, tecnica e sistema delle fonti, interrogandosi sulla capacità del diritto di continuare a svolgere una funzione di argine rispetto al crescente potere tecnologico; M. D'Amico, *L'intelligenza artificiale e la sfida regolatoria sul duplice versante, europeo e nazionale*, in M. D'Amico, F. Balaguer Callejón, A. Aguilar Calahorro, P. Gambatesa, S. Di Giovanni (a cura di), *Commentario Tematico del Regolamento (UE) 2024/1689 e della legge italiana 23 Settembre 2025, N. 132,* Torino, 2026, 17 ss., che inquadra la disciplina dell'intelligenza artificiale nella prospettiva della tutela dei diritti fondamentali e dei principi del costituzionalismo multilivello.

[4] A. C. Amato Mangiameli, Intelligenza, *Big Data e nuovi diritti*, in *Rivista Italiana di Informatica e Diritto*, 1, 2022, 93 ss., 97: «Si tratta di una nuova era, nella quale il paradigma dei *big data* riporterebbe il discorso sul piano dell'oggettività, visto che sarebbero gli stessi dati, senza alcuna pregiudiziale e senza essere condizionati dall'orizzonte di attese dell'osservatore, a dirci del *benchmark*, del modello, e della correlazione significativa fra un numero tendenzialmente infinito di variabili».

[5] A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in Roberto Cavallo Perin, Diana-Urania Galetta (a cura di), *Il diritto dell'Amministrazione pubblica digitale,* Torino, 2020, 1ss.

[6] F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, Massachusetts. London, England, 2015.

[7] L. Califano, *La strategia normativa dell'Unione europea per un nuovo ordine digitale*, in L. Califano, F. Fabrizzi, G. Sartor (a cura di), *Information Disorder e sistema democratico*, in *Federalismi.it*, 15, 2025.

[8] B. Ponti, *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità*, Milano, 2023; Id., *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, 517 ss.; Id., *La sfida tecnologica alla legalità amministrativa*, in *Rivista Italiana di Informatica e Diritto*, 2, 2022, 7 ss.; AA.VV., *Intelligenza Artificiale nella PA: opportunità e rischi. Atti del convegno 8 febbraio*, in *Italiastatodidiritto.it*, 2024.

riguarda più pochi individui, ma, se impiegata su larga scala, può incidere su intere comunità, rendendo necessaria una risposta normativa ampia e coordinata.

L'ampiezza dei *dataset*, la granularità delle informazioni raccolte e le possibilità di inferenza predittiva rendono, infatti, sempre più sfumata la distinzione tra dati personali e non personali, con la conseguente difficoltà di applicare i tradizionali strumenti di tutela previsti dal Regolamento generale sulla protezione dei dati (GDPR nel prosieguo)[9]. Inoltre, l'utilizzo congiunto di tecniche di profilazione e sistemi di IA generativa apre scenari del tutto inediti, in cui la capacità dell'algoritmo di produrre contenuti nuovi o prendere decisioni autonome pone ulteriori sfide ai meccanismi di controllo *ex ante* ed *ex post* delineati dalle regolazioni esistenti.

In questo complesso contesto, l'Unione Europea ha scelto di assumere un ruolo di *leadership* nella regolamentazione dell'IA attraverso una serie di iniziative normative inserite nel più ampio contesto della strategia europea sui dati 2030, varata dalla Commissione europea nel 2020[10]. L'idea è quella di realizzare un unico sistema normativo applicabile in tutta Europa che consenta non solo di gestire l'economia dei dati, qui visti come «valuta»[11] il cui scambio viene facilitato dai governi[12], ma consenta anche di prevenire rischi e abusi e di creare uno spazio comune europeo[13].

Questa impostazione riflette la volontà dell'UE di porsi come terzo polo regolatorio globale, in contrapposizione ai modelli statunitense (guidato dal mercato) e cinese (guidato dallo Stato), affermando un paradigma incentrato sui diritti fondamentali, sull'innovazione controllata e sulla fiducia nell'ecosistema digitale. L'impegno di coniugare logiche di mercato e tutela dei diritti, da sempre oggetto di impegno da parte delle istituzioni europee, ha condotto all'approvazione di una serie di riforme legislative volte alla gestione dei dati:

- *Data Governance Act*[14]: mira a creare un mercato unico dei dati nell'UE, rendendone più facile la condivisione e il riutilizzo in modo sicuro e affidabile da parte della PA e consentendo la loro condivisione tra imprese attraverso gli *European Data Spaces*;
- *il Data Act*[15]: integra il Data Governance Act e a partire da una visione dei dati come risorsa economica, mira alla creazione di un vero e proprio mercato. Disciplina l'accesso e l'utilizzo dei dati generati dai dispositivi connessi, dando a privati e imprese il diritto di accedere a tali dati e di condividerli con terze parti;
- *Digital Markets Act* (DMA)[16]: ha l'obiettivo di rendere i mercati digitali più equi e competitivi, impedendo gli abusi da parte delle grandi piattaforme online (*gatekeeper*) attraverso un meccanismo di obblighi e divieti;

---

[9] 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).

[10] Commissione Europea, *Una strategia europea per i dati, COM*(2020)66, 19 febbraio 2020.

[11] M.G. Peluso, *Intelligenza artificiale e tutela dei dati. Prospettive critiche e possibili benefici per una governance efficace*, Torino, 2023

[12] W.D. Eggers, R. Hamill, A. Ali, *Data as currency. Government's role in facilitating the exchange*, in *Deloitte Review*, 13, 2013, 19-31.

[13] P. Falletta, A. Marsano, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista Italiana di Informatica e Diritto*, 1, 2024, 120 ss.

[14] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) n. 2018/1724 (*Regolamento sulla governance dei dati*).

[15] Regolamento (UE) n.2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) n. 2017/2394 e la direttiva (UE) n. 2020/1828 (*Regolamento sui dati*).

[16] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (*Regolamento sui mercati digitali*).

- *Digital Services Act* (DSA)[17]: stabilisce nuove norme per le piattaforme *online* con l'obiettivo di rendere il *web* più sicuro, efficiente e giusto attraverso norme di contrasto a contenuti illegali e difesa dei diritti degli utenti;
- Regolamento (UE) 2024/1689, noto come *Artificial Intelligence Act* (AI Act): entrato in vigore il 10 giugno 2024[18], è volto a creare un quadro giuridico chiaro per garantire un uso sicuro, etico e responsabile dell'AI nell'Unione Europea, promuovendo l'innovazione e tutelando i diritti fondamentali, a cui il presente lavoro è dedicato.

L'AI Act rappresenta a sua volta il primo pilastro della strategia europea sull'Intelligenza Artificiale[19], configurandosi come una normativa a efficacia orizzontale volta a guidare l'armonizzazione della regolamentazione sull'IA all'interno dell'Unione e introducendo una visione dell'IA quale motore di vantaggi competitivi per le imprese e di risultati positivi sul piano sociale e ambientale in settori quali, ad esempio, l'assistenza sanitaria, l'istruzione, la sicurezza dei servizi pubblici. L'AI Act appare funzionale alla ricerca di una *governance* che permetta all'IA di svilupparsi in modo etico e responsabile, al servizio dell'uomo e dei suoi diritti[20]. Peraltro, sullo sfondo, ma non sfocato, rimane l'insieme dei rischi potenziali che il suo utilizzo potrebbe generare.

L'approccio basato sul rischio, che costituisce l'elemento distintivo del Regolamento *de quo*, richiede tuttavia un'interpretazione e un'applicazione coerenti, soprattutto quando si tratta di coordinare gli obblighi previsti dall'AI Act con quelli già esistenti ai sensi del GDPR[21]. Il dialogo tra le due regolazioni diventa quindi cruciale, poiché esse si sovrappongono in numerosi aspetti: dalla definizione dei ruoli soggettivi, alla valutazione d'impatto, dalle misure di trasparenza ai diritti degli interessati.

La presente analisi si propone di esaminare il ruolo e l'efficacia dell'AI Act e la sua interazione con il preesistente GDPR nella tutela del diritto fondamentale alla *privacy*, con una specifica attenzione all'impatto della profilazione algoritmica. Si valuterà come queste due normative europee, operando congiuntamente, mirino a rafforzare la protezione individuale, non tralasciando le potenziali aree di tensione e le sfide di coordinamento tra di esse. L'obiettivo è evidenziare quelle che sono le sfide poste dal nuovo regolamento sull'Intelligenza

[17] Regolamento (UE) 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 2000/31/CE (*Regolamento sui servizi digitali*).

[18] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale). L'entrata in vigore completa è prevista entro il 2 agosto 2026, fatta eccezione per l'applicazione dell'articolo 6, par. 1 (classificazione dei sistemi ad alto rischio), prevista entro il 2 agosto 2027.

[19] Commissione europea, *Legge sull'IA*, consultabile sul portale della Strategia Digitale europea.

[20] AI Act, considerando n. 1: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione». Sul tentativo dell'Unione europea di coniugare sviluppo tecnologico, tutela dei diritti fondamentali e *rule of law* attraverso la disciplina dell'intelligenza artificiale, v. C. Casonato, *L'intelligenza artificiale e il diritto pubblico comparato ed europeo*, in *DPCE Online*, 1, 2022, 169 ss.

[21] Sul rapporto tra GDPR e nuove sfide poste dall'intelligenza artificiale e sulla necessità di strumenti regolatori, v. F. Pizzetti, *Il GDPR nell'era dell'IA non basta più, servono nuovi strumenti*, in *Agendadigitale.eu*, 2025.

Artificiale, come quella derivante dall'opacità degli algoritmi (c.d. *black box*[22]), dalla valutazione del rischio e dalla gestione della qualità dei dati volta alla prevenzione del *bias* algoritmico, nonché dal principio della supervisione umana. In secondo luogo, si prefigge di identificare e approfondire le criticità e le potenziali aree di frizione o incompletezza nel quadro normativo delineato, con particolare riguardo alla valutazione del rischio da parte del fornitore. Una particolare attenzione sarà rivolta al modello *risk-based* e al ruolo del fornitore del sistema di IA ad alto rischio nonché alle possibili criticità del sistema, proponendo anche soluzioni.

2. Il fondamento giuridico della privacy: un diritto fondamentale stratificato. Il diritto alla *privacy* rappresenta una delle conquiste più significative nella protezione dei diritti fondamentali dell'individuo ed è oggi un principio centrale dell'ordinamento giuridico internazionale, europeo e nazionale. La sua evoluzione, inizialmente concepita in termini di protezione della sfera privata da ingerenze indebite, ha subìto un'importante e continua trasformazione con l'avvento della tecnologia digitale e la crescente rilevanza dei dati personali[23]. La stratificazione storica del diritto alla *privacy* appare oggi come la necessaria premessa per comprendere la disciplina della profilazione algoritmica non solo nel GDPR, ma in modo ancora più marcato nell'AI Act, che ne rappresenta la più recente proiezione sistemica. La profilazione non è di per sé negativa, ma se non trattata con le dovute cautele può rivelarsi un'arma a doppio taglio[24].

In questo contesto, l'analisi dei fondamenti giuridici alla base del diritto alla *privacy* porta a esaminare una serie di strumenti internazionali, europei e costituzionali che, nel tempo, hanno progressivamente riconosciuto e tutelato questa sfera fondamentale, adattandosi alle nuove sfide poste dal progresso tecnologico. Ogni livello normativo ha contribuito a rafforzare e precisare lo statuto giuridico dell'individuo nell'ecosistema informativo contemporaneo, adattando ciascun livello normativo alle tecnologie emergenti e alla crescente capacità dei sistemi automatizzati di inferire, aggregare e prevedere informazioni sull'individuo, al punto che si discute se si sia in presenza di uno «sconvolgimento costituzionale» o di un «momento costituzionale»[25] nell'infosfera[26].

La prima stratificazione del diritto alla *privacy*, nella più ampia accezione di tutela della sfera individuale, risale ai primi documenti internazionali che riconoscono la dignità e i diritti dell'individuo. Tra questi, la Dichiarazione Universale dei Diritti Umani (DUDU) del 1948

[22] La spiegabilità dell'algoritmo è da intendere come capacità di comprendere il risultato della decisione. Sul punto si veda G. Lo Sapio, *La black box: l'esplicabilità delle decisioni algoritmiche quale garanzia della buona amministrazione*, in *Federalismi.it*, 2021, 114 ss.

[23] Sul processo di evoluzione del diritto alla *privacy* e alla protezione dei dati personali, nonché sul ruolo svolto dall'evoluzione tecnologica quale fatto propulsivo della loro trasformazione, M. Bassini, *Il diritto costituzionale alla privacy nel prisma dell'evoluzione tecnologica*, in *Diritto Costituzionale*, 1, 2023, 83 ss.

[24] Su come la profilazione della popolazione sia stata utilizzata nel tempo dai governanti per perpetrare discriminazioni e abusi dei diritti umani, v. W. Seltzer, M. Anderson, *The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses*, in *Social Research*, 2001. Emblematico l'esempio del registro olandese contenente dati identificativi dei cittadini come nome, numero di identificazione e altri dati relativi alla loro identità economica, culturale o sociale (dati oggi contenuti nell'art. 4 co. 1 del Regolamento Europeo 2016/679 nella definizione di «dato personale»), che nelle intenzioni avrebbe dovuto facilitare i compiti dell'Amministrazione Pubblica olandese e invece finì per essere utilizzato dai Nazisti ai fini del genocidio, facilitandolo, una volta che questi ebbero invaso i Paesi Bassi.

[25] E. Celeste, *Digital constitutionalism: a new systematic theorisation*, in *International Review of Law, Computers & Technology*, 2019, 33(1), 76–99. Sul *paradigm shift* prodotto dall'IA anche A. Punzi, *L'ordine giuridico delle macchine*, Torino, 2003, 18 e A. D'Aloia, *Il diritto verso il mondo nuovo*, in *Biolaw Journal – Rivista di Biodiritto*, 1, 2019, 3 ss.

[26] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

si pone come un punto di partenza imprescindibile. Sebbene l'articolo 12[27] della DUDU non usi il termine *privacy* nella sua accezione moderna legata alla protezione dei dati, esso stabilisce un principio fondamentale che costituisce il primo riconoscimento universale del diritto a proteggere la propria vita privata[28]. È qui che si rinviene il nucleo dell'idea che l'autonomia personale richiede una zona di non-interferenza, intesa come barriera alle intrusioni che costituirà la matrice di tutte le successive elaborazioni normative e da cui discenderà anche la lettura critica delle interferenze algoritmiche.

Il secondo livello si sviluppa in ambito europeo, con la Convenzione del Consiglio d'Europa n. 108 del 1981 (*Convenzione per la protezione delle persone rispetto al trattamento automatizzato dei dati personali*), primo trattato internazionale vincolante dedicato specificatamente alla protezione dei dai personali, che ha anticipato molte delle categorie concettuali oggi pienamente recepite nel diritto dell'Unione Europea[29]. La Convenzione 108 introduce una prima idea di rischio connesso al trattamento automatizzato, segnando il passaggio dalla *privacy* come diritto «passivo» alla protezione dei dati come diritto «attivo», fondato su principi di qualità, proporzionalità, e finalità del trattamento.

Questo principio, pur nella sua formulazione generica e antecedente all'era digitale, ha rappresentato l'origine concettuale da cui sono derivate successive normative e si sono sviluppate interpretazioni più specifiche in materia di *privacy*, ispirando la legislazione di molti Stati e la redazione di successivi strumenti giuridici internazionali e regionali così riconoscendo un nucleo intangibile di dignità e autonomia individuale. In questo quadro, l'evoluzione interpretativa secondo cui la nozione di *arbitrary interference* contenuta nell'art. 12 è stata progressivamente letta in chiave di protezione dei dati personali dalle Nazioni Unite (fino alle più recenti risoluzioni dell'Assemblea Generale)[30], ponendo così le basi per una concettualizzazione moderna del diritto alla *privacy* che ha informato, rimanendo sullo sfondo, anche le successive interpretazioni della giurisprudenza europea[31].

Un ulteriore consolidamento è stato offerto dalla Convenzione Europea dei Diritti dell'Uomo (art. 8 CEDU) che, attraverso l'interpretazione dinamica della Corte EDU, ha progressivamente incluso la protezione dei dati personali come aspetto fondamentale del diritto alla vita privata, imponendo agli Stati un doppio ordine di obblighi: negativi, di astensione dall'interferire ingiustificatamente nella vita privata; positivi, di adottare misure per proteggere gli individui da ingerenze di terzi, comprese le entità private e le aziende tecnologiche. Questa interpretazione proattiva ha anticipato le sfide poste dalla pervasività dei sistemi di trattamento dei dati e ha posto le basi per un'azione legislativa più incisiva.

Tra i casi più significativi in questa direzione, si colloca *S. and Marper v. United Kingdom* (2008), in cui la Corte EDU ha affermato l'illegittimità della conservazione indifferenziata e

[27] L'art. 12 DUDU afferma che: «Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a attacchi al suo onore e alla sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni».

[28] Assembly general, *Universal Declaration of Human Rights*, 10 December 1948, art. 12.

[29] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108), Strasbourg, 28 January 1981.

[30] UN General Assembly, *Resolution 68/167 The Right to Privacy in the Digital Age*, 2014.

[31] Pur non essendo citato direttamente nelle pronunce della Corte di Giustizia, questo principio internazionale sottende l'interpretazione europea dei diritti alla vita privata e alla protezione dei dati, concretizzata nelle decisioni della Corte sui trattamenti automatizzati. La Corte ha stabilito che qualsiasi interferenza nella vita privata deve essere prevista dalla legge, perseguire un obiettivo legittimo e rispettare i principi di necessità e proporzionalità, con adeguati meccanismi di controllo indipendente, come emerge dalle pronunce *Digital Rights Ireland, Schrems I e II*, *Tele2 Sverige* e *Watson e Privacy International*. Queste decisioni attualizzano il principio di divieto di interferenze arbitrarie e costituiscono il quadro concettuale europeo per la regolazione della profilazione e dei sistemi automatizzati, anticipando i principi poi codificati dal GDPR e dall'AI Act.

generalizzata di dati biometrici. Pur non trattandosi ancora di profilazione algoritmica in senso moderno, è stato chiarito che i dati personali – soprattutto quelli idonei all'identificazione univoca – generano un'ingerenza particolarmente intensa nella sfera personale degli individui, anticipando così il paradigma della «protezione rafforzata» per trattamenti automatizzati ad alto rischio[32]. Il caso *S. and Marper* rappresenta il momento in cui il diritto alla *privacy* si modella esplicitamente sulle modalità tecnologiche del trattamento, prefigurando una dimensione «informazionale» del diritto che sarà poi tematizzata dal GDPR. Accanto al caso *Marper*, vi sono poi diverse pronunce della Corte EDU tra il 2005 e il 2015 che hanno contribuito alla stratificazione del diritto: tra le altre, *Rotaru v. Romania*[33] e *Uzun v. Germany*[34], che hanno affrontato rispettivamente la conservazione di dati in archivi di *intelligence* e l'utilizzo di dispositivi di localizzazione GPS, introducendo la nozione chiave per cui l'intensità dell'ingerenza cresce proporzionalmente alla capacità di tracciare, aggregare e inferire informazioni sull'individuo. In tal modo, pur non trattandosi ancora di profilazione algoritmica, la Corte ha contribuito a stratificare il diritto alla *privacy* come diritto che cresce insieme alla complessità tecnologica, precorrendo i tempi nell'identificare una futura esigenza di disciplina autonoma sulla protezione dei dati.

Una ulteriore stratificazione, sempre nel contesto dell'Unione Europea, coincide con la disciplina sulla protezione dei dati. Per oltre vent'anni la Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[35] ha rappresentato il primo e più complesso tentativo di normazione organica della materia a livello sovranazionale. La *ratio* della disciplina era quella di un equo bilanciamento tra gli interessi, a volte opposti, alla tutela dei diritti fondamentali degli individui, da un lato, e alla libera circolazione delle informazioni, dall'altro. Qui la protezione dei dati entra nel mercato interno, inaugurando quella tensione fra libertà economiche e tutela dei diritti che riemerge oggi nel confronto tra GDPR e AI Act.

Tale evoluzione si è ulteriormente consolidata nel territorio dell'Unione attraverso la Carta dei Diritti Fondamentali dell'Unione Europea che dedica un diritto autonomo e specifico alla protezione dei dati (art. 8), elevando esplicitamente quest'ultima a diritto fondamentale e riconoscendone la centralità nell'era digitale, distinto dal rispetto della vita privata (art. 7) anche se ad esso intrinsecamente correlato e ha, inoltre, costituito la base per il GDPR[36].

Il carattere innovativo dell'art. 8 è stato evidenziato anche dalla Corte di Giustizia, che già nel caso *Lindqvist* (C-101/01, 2003) ha delineato i confini applicativi della direttiva 95/46/CE, affermando che qualunque trattamento automatizzato di dati personali – anche non complesso – rientra nella tutela europea. Questa decisione ha avuto il merito di chiarire

[32] Corte EDU, *S. and Marper v. United Kingdom*, 4 dicembre 2008.
[33] Corte EDU, *Rotaru v. Romania*, 4 maggio 2000.
[34] Corte EDU, *Uzun v. Germany*, 2 dicembre 2010.
[35] O. Lynksey, *The Foundation of EU Data Protection Law*, Oxford, 2015; L. A. Bygrave, *Data Privacy Law, an International Perspective*, Oxford, 2014.
[36] Sul riconoscimento della protezione dei dati personali quale diritto fondamentale autonomo dell'ordinamento europeo, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea e dall'art. 16 TFUE, nonché sul passaggio dalla direttiva n. 95/46/CE al GDPR quale evoluzione del sistema europeo di tutela, v. F. Pizzetti, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *MediaLaws*, 1, 2018, 104 ss; sul carattere autonomo del diritto alla protezione dei dati personali e sulla sua tutela attraverso un sistema articolato di garanzie e rimedi, G. Bellomo, *Protezione dei dati personali e pluralità dei poteri pubblici: il coordinamento tra tutela inibitoria, sanzioni amministrative e responsabilità civile nel GDPR*, in *DPCE Online*, 4, 2025, 2443 ss.

come la protezione dei dati non è un sottoinsieme della *privacy*, ma un ecosistema distinto con regole proprie, anticipando così il salto concettuale operato dalla Carta[37].
In una prospettiva di stratificazione, *Lindqvist* rappresenta un passaggio fondamentale: il diritto alla *privacy* si sdoppia in una componente «familiare», legata alla vita privata, e in una componente «sistemica», legata alla protezione dei dati, quest'ultima destinata a regolare la dimensione informazionale della persona anche oltre la sua vita privata in senso stretto. La sentenza chiarisce che la *privacy* è legata più al diritto della persona di mantenere riservati determinati aspetti della propria vita[38], mentre la protezione dei dati personali è un concetto più ampio e tecnico che riguarda le regole sul trattamento di dati specifici[39]; è alla tutela di quest'ultimo diritto che fanno riferimento la normativa europea e nazionale sui dati[40].
In seguito è entrata in vigore la direttiva 2002/58/CE (*ePrivacy*), poi modificata dalla direttiva 2009/136/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche), tuttora in vigore.
Questo percorso è sfociato nel Regolamento (UE) 2016/679, che ha armonizzato e rafforzato i principi e i diritti relativi al trattamento dei dati personali in tutta l'Unione Europea. Il GDPR ha introdotto principi rigorosi come liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, e responsabilizzazione (*accountability*).
La responsabilizzazione del titolare, in particolare, rappresenta un elemento di forte discontinuità rispetto alla disciplina della Direttiva 95/46/CE, che si fondava in larga parte su obblighi formali e meno sulla verifica sostanziale delle misure adottate[41].
Ha, inoltre, rafforzato i diritti degli interessati, includendo il diritto di accesso, di rettifica, di cancellazione (diritto all'oblio), di limitazione di trattamento, di portabilità dei dati nonché il diritto di opposizione alle decisioni basate unicamente sul trattamento automatizzato (art. 22). L'articolo 22 rappresenta un baluardo contro le decisioni completamente automatizzate (inclusa la profilazione) che producono effetti giuridici o significativamente analoghi per l'interessato, prevedendo eccezioni stringenti e la necessità di «garanzie adeguate»[42], tra cui il diritto a ottenere un intervento umano. In ottica stratificatoria, esso costituisce il primo riconoscimento normativo europeo del rischio specifico derivante dal trattamento automatizzato e dalla profilazione automatizzata algoritmica, anticipando il terreno su cui interverrà l'AI Act[43].

[37] Corte Giust., 6 novembre 2003, *Lindqvist*, causa C-101/01. Alcune decisioni in materia di *privacy* in chiave evolutiva sono contenute anche in G. De Gregorio, *Digital Constitutionalism, Privacy and Data Protection*, in *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022.
[38] S. Rodotà, *Il diritto di avere diritti,* Bari, 2018.
[39] L'idea è quella che i dati personali finiscono con il costituire un'identità della persona, che dunque rimane in posizione centrale. In questo senso, in tempi più recenti e con particolare riferimento al sistema italiano G. Pino, *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Torino, 2006, 257 ss.
[40] P. Guarda, G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Milano, 2023.
[41] Corte cost., sent. n. 81/1993; Corte cost., sent. n. 372/2006.
[42] La base giuridica per l'adozione di tali «garanzie» è costituita dall'art. 16 TFUE.
[43] Secondo A. D'Aloia, *Il diritto verso il mondo nuovo*, in *BioLaw Journal*, 2019, 3-31, le implicazioni per la *privacy* risultano «evidenti» non solo sotto il profilo della riservatezza, ma soprattutto in relazione alla necessità di prevenire esiti discriminatori nei settori del lavoro, del credito, delle assicurazioni e persino della giustizia penale. La minaccia deriva dall'opacità dei modelli predittivi, capaci di inferire correlazioni non trasparenti e potenzialmente dannose. Ancora più radicalmente, A. Baricco sottolinea come la violazione sistematica della *privacy* appaia ormai «il prezzo da pagare» per la partecipazione all'infosfera governata dalle grandi piattaforme digitali (A. Baricco, *The Game*, Torino, 2018, 239). Tale osservazione illumina un tratto essenziale della stratificazione del diritto alla *privacy*: la centralità assunta dal «potere informazionale» degli intermediari tecnologici, fenomeno destinato a diventare il fulcro regolatorio dell'AI Act.

Focalizzando l'attenzione sul contesto italiano, si può osservare come il testo costituzionale non contenga riferimenti espliciti al diritto alla *privacy* o alla protezione dei dati personali. Tuttavia, il principio della riservatezza e, successivamente, della protezione dei dati è emerso attraverso un'interpretazione evolutiva e sistematica dell'art. 2 in combinato disposto con gli articoli 13, 14, 15 Cost. nonché dell'art. 6 della Convenzione EDU. L'articolo 2 della Costituzione italiana, riconoscendo i «diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità», opera da «clausola aperta»[44] per accogliere nuovi diritti non esplicitamente elencati, tra cui quello alla riservatezza. Questa interpretazione è stata poi arricchita dalla giurisprudenza costituzionale che ha progressivamente ampliato il concetto di autodeterminazione «informativa», intesa come il diritto dell'individuo di controllare le informazioni che lo riguardano e di decidere autonomamente sul loro utilizzo.
Con l'adozione del GDPR a livello europeo e con l'introduzione del d.lgs. n. 101/2018 (che ha adeguato la normativa italiana al GDPR), l'ordinamento italiano ha infine pienamente allineato le sue normative al quadro giuridico europeo, consentendo una protezione più elevata e armonizzata dei dati personali così garantendo il rispetto dei diritti fondamentali sanciti dalla Costituzione e dal diritto europeo[45] e anche la giurisprudenza amministrativa italiana ha contribuito a una lettura evolutiva della *privacy* in relazione ai primi sistemi di sorveglianza intelligente e alle banche dati interconnesse, affrontando il tema del bilanciamento tra efficienza amministrativa e protezione dei dati[46].

3. AI Act e GDPR: un rapporto di interazione e integrazione. Alla luce di questa ricca stratificazione, che va dal diritto alla non-ingerenza fino al riconoscimento del rischio algoritmico, si colloca l'AI Act, che non disciplina la *privacy* in senso stretto ma interviene come strato tecnologico specialistico per regolare i rischi dei sistemi di IA. Il presente lavoro si concentra sulla profilazione nei contesti ad alto rischio[47].
Il Regolamento n. 2024/1689, «che stabilisce regole armonizzate sull'intelligenza artificiale»[48], costituisce la prima normativa orizzontale al mondo in materia[49] e si inserisce nella Strategia Digitale UE come primo atto di un pacchetto di misure politiche europee volte a sostenere lo sviluppo di un'intelligenza artificiale affidabile, che include anche il Pacchetto Innovazione

---

[44] S. Mangiameli, *Il contributo dell'esperienza costituzionale italiana alla dommatica europea della tutela dei diritti fondamentali*, in *Consultaonline*, 2006.
[45] Sul progressivo inserimento della tutela della *privacy* e della protezione dei dati personali nel più ampio processo di adattamento delle categorie costituzionali alla realtà digitale e sul ruolo della regolazione europea quale espressione di una più ampia stagione di costituzionalismo digitale, v. O. Caramaschi, *Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni?*, in *Rivista italiana di informatica e diritto*, 1, 2025, 29 ss.
[46] Consiglio di Stato, sez. VI, n. 8472/2019 (uso degli algoritmi nella PA), Consiglio di Stato, sez. VI, sent. n. 2270/2019 (ammissione dell'intelligenza artificiale nell'attività amministrativa per la sola attività vincolata); apertura del Consiglio di Stato con l'ammissione dell'algoritmo anche nell'attività amministrativa discrezionale, con le sentenze Cons. Stato Sez. VI, sentt. 8472, 8473, 8474/2019, confermate anche da Cons. Stato, sez.VI, sentt. 881/2020 e 1206/2021. Attraverso queste pronunce il giudice amministrativo ha riconosciuto che l'uso di algoritmi nella funzione pubblica impone esigenze rafforzate di trasparenza, comprensibilità e non discriminazione, anticipando il modello di «*accountability* algoritmica» dell'AI Act.
[47] Art. 6 e Allegato III AI Act.
[48] Ai fini di questa analisi si precisa che l'AI Act all'articolo 3 definisce come «sistema di IA: 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», comprendendo dunque anche sistemi di *Big Data Analytics* e *Machine Learning* (BDA/ML).
[49] L'auspicio è che si verifichi il c.d. *Brussels Effect*.

AI e il Piano Coordinato sull'AI di futura adozione[50]. L'analisi delle modalità con cui l'AI Act interagisce con la già esistente normativa sulla protezione dati, in particolare con il GDPR, è funzionale a comprendere come la tutela dei dati tradizionale sia chiamata a ridefinirsi nel nuovo ecosistema regolatorio dell'IA, evidenziando al contempo aree di sovrapposizione, frizione e complementarità tra i due strumenti normativi.

Giova precisare in premessa che mentre il GDPR sembra tendere verso la tutela dei diritti fondamentali degli individui[51], nell'AI Act si precisa sin dall'inizio che «lo scopo…è migliorare il funzionamento del mercato interno», e che «il presente regolamento garantisce la libera circolazione transfrontaliera dei sistemi e servizi basati sull'IA, impedendo così agli Stati Membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa previsione del presente regolamento»[52].

L'AI Act incorpora, dunque, la logica di uno strumento di regolamentazione del mercato[53], volto a bilanciare innovazione e tutela[54], attraverso un approccio *risk-based*. Il fatto che la disciplina sia contenuta in un Regolamento indica come la volontà di armonizzarla da parte del legislatore europeo sia massima, in accordo con l'idea di un mercato unico dei dati.

L'AI Act e il GDPR non si pongono come strumenti alternativi[55]; operano in sfere qualitativamente diverse e sono concepiti per interagire tra loro ed essere intrinsecamente complementari: laddove un sistema di IA tratti dati personali, il GDPR continua ad applicarsi pienamente, senza eccezioni o deroghe[56]. Ciò risulta evidente ad esempio dal Considerando 6 dell'AI Act, a tenore del quale il regolamento «non pregiudica l'applicazione del diritto dell'Unione in materia di protezione dei dati personali». La disposizione dell'articolo 2, par. 4, dell'AI Act è ancora più esplicita, stabilendo che il Regolamento si applica «fatto salvo il diritto dell'Unione relativo alla protezione dei dati personali e alla vita privata, compresi il regolamento (UE) 2016/679 (GDPR) e la direttiva (UE) 2016/680». Inoltre, i principi di trasparenza, equità, vita privata, robustezza tecnica e sicurezza dei sistemi AI di cui al Considerando 27 dell'AI Act risultano in forte continuità con i principi di trasparenza, liceità, correttezza, sicurezza e riservatezza dei dati personali *ex* art. 5 del GDPR.

L'AI Act aggiunge ulteriori strati di obblighi e requisiti specifici per affrontare i rischi peculiari per la protezione dei dati generati dai sistemi di Intelligenza Artificiale, in particolare quelli classificati «ad alto rischio», integrando le garanzie già previste dal GDPR con requisiti aggiuntivi pensati per la natura unica dei sistemi AI.

Un esempio significativo di sinergia tra i due regolamenti è costituito dalla nozione di «profilazione» adottata nell'AI Act, che richiama direttamente la definizione riportata nell'articolo 4, punto 4, del GDPR, in base al quale per profilazione si intende «qualsiasi

---

[50] Commissione europea, *Comunicazione sulla Strategia europea per l'intelligenza artificiale*, COM(2018); Commissione europea, *AI Innovation Package*, COM(2024) 4 final.

[51] Si veda ad. es. Reg. (UE) 2016/679, Considerando 2.

[52] Reg. (UE) 2024/1689, Considerando 1.

[53] In maniera critica sul punto D. Tafani, *GDPR could protect us from the AI Act. That's why it's under attack*, in *Bollettino telematico di filosofia politica*, 2024: «In the AI Act, the very concept of fundamental rights is operationally redefined in such a way as to reduce it to an empty shell».

[54] Sul *trade-off* tra regolazione e innovazione, J. Arnal, *AI at Risk in the EU: It's Not Regulation, It's Implementation*, in *European Journal of Risk Regulation*, Cambridge, 2025,1168-1177, in cui si parla in particolare dei casi Meta e Deepseek, nonché del frammentato panorama europeo che rende difficile l'operare delle imprese, fino al punto che molte *start up* decidono di cessare le operazioni.

[55] Sulla inutilizzabilità del principio di specialità per regolare l'applicazione dell'una o dell'altra normativa si veda P. Falletta, A. Marsano, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista Italiana di Informatica e Diritto*, 1, 2024; G. Contaldi, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 5, 2021, 1193-1213.

[56] L'art. 50(6) dell'AI Act fa salvi eventuali ulteriori obblighi di trasparenza imposti agli utilizzatori di sistemi di intelligenza artificiale da parte di diverse normative UE o nazionali.

forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

Tuttavia, mentre il GDPR qualifica la profilazione in termini di trattamento automatizzato di dati personali, l'AI Act ne inserisce l'uso all'interno di un modello regolatorio basato sul rischio, classificando espressamente come sistemi ad alto rischio quelli che, in determinati contesti sensibili, realizzano valutazioni o attribuzioni di punteggi ai soggetti (art. 6 e Allegato III). In particolare, il dettato dell'articolo 6 fornisce i criteri di classificazione, mentre l'elenco contenuto nell'Allegato III mira a proteggere gli individui in situazioni in cui le decisioni algoritmiche possono avere un impatto significativo sulla loro vita, sui loro diritti fondamentali e sulle loro opportunità. Si tratta, ad esempio, della valutazione dell'affidabilità finanziaria, della selezione per l'accesso a servizi essenziali o dell'allocazione di benefici pubblici. In tali casi, la profilazione algoritmica può produrre un impatto significativo sui diritti delle persone, giustificando l'applicazione di requisiti stringenti per fornitori e utilizzatori[57].

In questo contesto, aree di interazione e criticità sono legate alla trasparenza e alla *explainability* dei sistemi di IA, alla prevenzione del *bias* e al principio della supervisione umana, soprattutto nel settore pubblico[58].

L'*explainability* e la trasparenza sono ormai requisiti fondamentali per sistemi di intelligenza artificiale affidabili nell'ambito dell'Unione Europea, tanto che il GDPR già obbliga i titolari del trattamento a fornire «informazioni significative» sul processo decisionale automatizzato (artt. 13-15) interpretato da parte della dottrina come un embrionale «diritto alla spiegazione»[59] del modo in cui un algoritmo raggiunge un determinato risultato[60]. Tuttavia, nel GDPR permane qualche lacuna contenutistica a tal proposito[61] che l'AI Act interviene a colmare, imponendo ai *provider* di sistemi di IA ad alto rischio la produzione di documentazione tecnica, la conservazione di registri e la fornitura di spiegazioni orientate agli utenti, in grado di chiarire la logica, i limiti e le finalità del sistema anche a un pubblico non specialistico[62], tanto che in dottrina si è affermata l'idea che debba esservi una

---

[57] AI Act, art. 6(2).

[58] H. Palmer Olsen, J. Livingston Slosser, T. Troels, Hildebrandt, *What's in the Box?The Legal Requirement of Explainability in Computationally Aided Decision-Making in Public Administration*, 219 ss in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (a cura di), *Constitutional Law in the Algorithimc Society*, Cambridge, 2021.

[59] Sul possibile riconoscimento di un diritto alla spiegazione degli output algoritmici e di un diritto al controllo umano sulle decisioni automatizzate quale risposta alle sfide poste dall'intelligenza artificiale ai diritti fondamentali, v. L. Rinaldi, *Intelligenza artificiale, diritti e doveri nella Costituzione italiana*, in *DPCE Online*, 1, 2022, 201 ss.

[60] AI Act, Considerando 71; European Data Protection Board (EDPB), *Guidelines 03/2019 on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, versione 2*.0, 11 febbraio 2020. Sul punto non si dimentichi che l'art. 22, par. 3, del GDPR sancisce anche il diritto dell'individuo a non essere sottoposto a una decisione automatizzata.

[61] T. Tzimas, *Algorithmic Transparency and Explainability under EU Law*, in *European Public Law*, 4, *29*, 385–411; S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR*, in *International Data Privacy Law*, 2017; L. Edwards, M. Veale, *Slave to the Algorithm?*, in *Duke L. & Tech. Review*, 2017, 18-84.

[62] AI Act, art. 16.

trasparenza «qualificata», che miri ad un equilibrio tra *accountability* e segreti commerciali, evitando un sovraccarico informativo[63].

In tema di spiegabilità degli algoritmi, si evidenziano tre «assi»[64] fondamentali: spiegabilità dei dati, intesa in termini di pubblicità e conoscibilità dei dati e della loro origine; spiegabilità del modello, con informazioni sui meccanismi che governano le previsioni; infine, la c.d. spiegabilità *post-hoc*, cioè quella del modello dopo l'implementazione per il controllo dei risultati e l'attribuzione delle responsabilità[65].

La ricerca sull'Explainable AI (XAI) evidenzia come metodi *post-hoc*, visualizzazioni *model-agnostic* e *dashboard* interattive possano rappresentare strumenti efficaci per tradurre in pratica tali obblighi di conoscibilità senza sacrificare le prestazioni algoritmiche [66]. Nel loro insieme, progressi tecnici e obblighi normativi mirano a garantire che le decisioni prese dall'IA siano al contempo comprensibili e verificabili, rafforzando la fiducia degli utenti e tutelando i diritti fondamentali.

L'AI Act, nel cercare di mitigare[67] il problema della «scatola nera»[68], cioè l'opacità[69] dei processi decisionali algoritmici, all'art. 13 richiede che i sistemi di IA ad alto rischio siano

---

[63] B. Selbst, S. Barocas, *The Intuitive Appeal of Explainable Machines*, in *Fordham Law Review*, 2018, 1035-1139; R. Bygrave, *Automated Decision-Making and Privacy*, in *Computer Law & Security Review*, 2020.

[64] I. Ahmad, A. Amelio, D. H. Gernsback, D. F. Sivilli, *Intelligenza artificiale spiegabile: sicurezza informatica, usabilità, metaverso e sfide giuridiche*, in *FOCUS – "Neurodiritti" tra virtuale e reale, federalismi.it*, 6, 2024.

[65] I. Ahmad, A. Amelio, D. H. Gernsback, D. F. Sivilli, *ibidem*.

[66] G. Chaudhary, *Unveiling the Black Box: Bringing Algorithmic Transparency to AI*, in *Masaryk University Journal of Law and Technology*, *18*(1), 2024, 93–122.

[67] Si dà conto del dibattito in dottrina tra chi ritiene che i sistemi di IA abbiano dei *bias* intrinseci e come tali ineliminabili (D. Tafani, *Predictive optimisation systems do not work, and they infringe rights. So why do we use them?*, in *Journal of Law, Market & Innovation*, vol. 2, n.3, 2023) e chi invece ritiene che i *bias* algoritmici possano essere gestiti attraverso l'etica dell'IA (A. Agarwal, A. Beygelzimer, M. Dudík et al., *A reductions approach to fair classification, in Proceedings of the 35th International Conference on Machine Learning*, vol. 80, 2018; P. Hacker, *Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under eu law*, in *Common Market Law Review,* vol. 55, n. 4, 2018; B. Ponti, *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024). L'AI Act si inserisce evidentemente nella seconda corrente di pensiero.

[68] F. Pasquale, *The Black Box Society,* cit.

[69] Il termine «opacità» non si riferisce solo alla mancanza di accesso al codice sorgente, ma, più profondamente, all'incapacità di comprendere le logiche interne e le correlazioni complesse che portano un algoritmo a una determinata decisione, soprattutto nel caso dei modelli di *deep learning* in cui l'*output* non è prevedibile. Rispetto all'opacità come fenomeno multi-agente situato interno al sistema, J. Burrell, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 3.1, 2016. L'Autrice individua tre forme di opacità: «*opacity as intentional corporate or state secrecy*» legata al segreto industriale, alla proprietà intellettuale, e alla protezione dei vantaggi competitivi; «*opacity as technical illiteracy*» e «*opacity that arises from the characteristics of machine learning algorithms*». Si rende conto anche della dottrina secondo la quale l'opacità può derivare anche da elementi esterni all'algoritmo: A. Facchini, A. Termine, *Towards a Taxonomy for the Opacity of AI Systems*, in V. C. Müller (a cura di), *Philosophy and Theory of Artificial Intelligence*, 2021, *Studies in Applied Philosophy, Epistemology and Rational Ethics*, 63 (2022): gli Autori elaborano una tassonomia articolata su tre distinti livelli logicamente indipendenti. L' *Access opacity*: si riferisce ai limiti epistemici nel comprendere struttura e funzionamento di un sistema AI. Può derivare da tre fattori: *policy* di *non-disclosure* adottate dai progettisti; insufficiente alfabetizzazione tecnica dei soggetti coinvolti; complessità intrinseca dell'architettura computazionale. La *link opacity*: si riferisce all'incapacità del modello appreso di fornire elementi esplicativi, predittivi e di controllo riguardo al fenomeno oggetto di modellizzazione. Tale opacità compromette la comprensione scientifica e si suddivide in tre forme: *causal opacity*, relativa all'incapacità di ricostruire catene causali; *mechanisms opacity*, ovvero l'impossibilità di ipotizzare meccanismi sottostanti al fenomeno*; laws opacity*, l'incapacità di inferire leggi strutturali che connettano osservabili e variabili latenti. La *semantic opacity*: concerne l'opacità semantica dei contenuti informativi appresi dal sistema, ovvero la difficoltà, per i soggetti umani, di attribuire un significato comprensibile alle informazioni immagazzinate o manipolate. Essa si divide in: (a*) content opacity*, dovuta al formato strutturale dei dati (es. vettori numerici senza mappatura semantica); (b*) inferential opacity*, derivante dalla natura dei processi inferenziali interni al sistema (ad es. calcoli numerici non riconducibili a inferenze logiche

progettati e sviluppati in modo da consentire agli utenti umani (compresi gli operatori e, in parte, gli interessati) di comprenderne il funzionamento e le decisioni. Questa conoscibilità è assicurata attraverso trasparenza degli *input* e *output*; informazioni chiare e comprensibili; documentazione tecnica esaustiva. Tali requisiti mirano a superare la fiducia cieca nell'algoritmo, promuovendo una trasparenza procedurale e, almeno in parte, una trasparenza algoritmica sostanziale. Essi rafforzano l'obbligo di trasparenza già presente nel GDPR (artt. 12, 13 e 14), che richiede ai titolari del trattamento di fornire informazioni chiare e accessibili sul trattamento dei dati personali, inclusa la logica sottostante a eventuali decisioni automatizzate[70].

L'AI Act, in questo senso, specifica e rafforza gli strumenti per adempiere a tale obbligo nel contesto complesso dell'IA. Tuttavia, è lecito chiedersi se questi requisiti, pur essenziali, siano sufficienti, soprattutto innanzi a sistemi estremamente complessi. La trasparenza formale (documentazione, istruzioni) non sempre si traduce in trasparenza sostanziale[71] (reale comprensione del «perché» una decisione è stata presa) e una vera «spiegabilità» (*explainability*) richiede spesso un approccio *explainable by design*, dove il sistema è progettato fin dall'inizio per essere interpretabile, la presenza di linee guida e idealmente *best practices* osservate a livello globale, oltre a importanti considerazioni in termini di bilanciamento di interessi[72]. Si tratta un punto di frizione che la comunità scientifica e la pratica applicativa dovranno affrontare[73] e rappresenta uno dei nodi più delicati dell'applicazione pratica del quadro europeo.

Un altro pilastro fondamentale dell'AI Act è l'obbligo per i fornitori di sistemi ad alto rischio di implementare un robusto sistema di gestione della qualità dei dati e del rischio di *bias* algoritmici (artt. 9-10 AI Act). Si tratta di un aspetto cruciale per la profilazione algoritmica, data la sua intrinseca dipendenza dai dati e il rischio di perpetuare o amplificare discriminazioni.

La Commissione Europea, già nel *White Paper on Artificial Intelligence* del 2020, aveva sottolineato come la gestione del rischio fosse un requisito essenziale per prevenire effetti distorsivi causati da *dataset* imperfetti[74]. L'articolo 9 dell'AI Act impone oggi l'adozione di un *risk management system*[75], un sistema di gestione della qualità per assicurare la conformità del sistema di IA ai requisiti del Regolamento. Il sistema deve includere un processo iterativo di identificazione, analisi e mitigazione dei rischi (art. 9(2) AI Act), con particolare attenzione ai rischi di discriminazione indiretta[76].

---

esplicite). La distinzione effettuata è in questo caso funzionale ad approntare strumenti diversificati per ridurre il *bias*. In questo senso anche P. Sansò, *Opacità algoritmica e sovranità epistemica nel contesto del capitalismo delle piattaforme*, *i-lex*, Bologna, 18(2), 2025, 36-49.

[70] Art. 12–14 GDPR; EDPB, *Guidelines on Transparency*, 2018.

[71] F. Faini, *Big Data, Algoritmi e diritto*, in *DPCE Online*, 3, 2019.

[72] J. B. Rajendra, A. S. Thuraisingam, *The role of explainability and human intervention in AI decisions: jurisdictional and regulatory aspects*, in *Information & Communications Technology Law*, 1–32, 2025; I. Kusche, *Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk*, in *Journal of Risk Research*, 1, 2024.

[73] L. Longo, M. Brcic, F. Cabitza, J. Choi, R. Confalonieri, J. Del Ser, R. Guidotti, Y. Hayashi, F. Herrera, A. Holzinger, R. Jiang, H. Khosravi, F. Lecue, G. Malgieri, A. Páez, W. Samek, J. Schneider, T. Speith, S. Stumpf, *Explainable Artificial Intelligence (XAI) 2.0: A manifesto of open challenges and interdisciplinary research directions*, in *Information Fusion*, 106, 2024.

[74] European Commission, *White Paper on Artificial Intelligence: a European approach to excellence and trust*, 19 febbraio 2020.

[75] J. Schuett, *Risk Management in the Artificial Intelligence Act, in European Journal of Risk Regulation*, 15, Special Issue 2: Special Issue on the *Future of Food Law*, June 2024, 367 – 385.

[76] AI Act, Considerando 44: «[…] *Among the key shortcomings of such systems are the limited reliability, the lack of specificity and the limited generalisability. Therefore, AI systems identifying or inferring emotions or intentions of natural persons on the basis of their biometric data may lead to discriminatory outcomes and can be intrusive to the rights and freedoms of the concerned persons.*

L'articolo 10, invece, si concentra sulle qualità e *governance* dei dati utilizzati per l'addestramento, la validazione e il test dei modelli di IA. I dati devono essere pertinenti, rappresentativi, sufficientemente completi e privi di errori e i fornitori sono tenuti ad adottare misure per evitare pregiudizi storici, culturali o sociali che si riflettano nelle prestazioni di modello. È fondamentale inoltre prevenire i *bias* algoritmici e la discriminazione, assicurando che i dati riflettano la diversità della popolazione e non perpetuino pregiudizi storici o sociali[77]. I fornitori devono eseguire test rigorosi per individuare e mitigare tali *bias*, garantendo che il sistema di IA sia robusto, accurato e non discriminatorio.

L'AI Act richiede l'uso di «*appropriate statistical properties*» dei *dataset* (art. 10(3)) e impone che i fornitori documentino i rischi residui tramite registrazioni tecniche ed evidenze verificabili (art. 11). Questo approccio si allinea e rafforza i principi di minimizzazione dei dati, esattezza e integrità e riservatezza del GDPR (art. 5). Questo richiede, infatti, che i dati personali siano esatti e, se necessario, aggiornati, e che siano trattati in modo lecito, corretto e trasparente[78]. L'AI Act specifica come questi principi debbano essere applicati nel contesto dei sistemi di IA, richiedendo un approccio strutturato alla gestione del ciclo di vita dei dati e del modello di IA, introducendo requisiti più dettagliati e tecnici rispetto al GDPR, come:

- la necessità di un *data governance plan* documentato (art. 10(2))
- l'obbligo di monitoraggio *post-market* delle prestazioni del sistema (art. 61)
- la tracciabilità del *dataset* e la documentazione delle sue fonti (art. 12).

Per la profilazione, questo significa che i *dataset* di addestramento devono essere attentamente curati e monitorati per identificare e correggere eventuali disparità che potrebbero portare a esiti iniqui. Ad esempio, se un sistema di profilazione è addestrato su dati storici che mostrano una sotto-rappresentazione di determinati gruppi in posizioni lavorative di alto livello, l'algoritmo potrebbe imparare a discriminare involontariamente quei gruppi, replicando e amplificando lo svantaggio[79]. L'AI Act impone la mitigazione di tali rischi, chiedendo ai fornitori di dimostrare di aver adottato misure per ridurre i *bias*. Pertanto, si può dedurre che mentre il GDPR stabilisce principi generali contro la discriminazione basata su trattamenti automatizzati, l'AI Act introduce obblighi tecnici concreti e verificabili che rendono tali principi operativi. La combinazione dei due strumenti normativi crea un quadro integrato di tutela contro il *bias* algoritmico, rafforzando sia la fase di raccolta dei dati sia quella di addestramento e validazione dei modelli.

Un altro principio fondamentale dell'AI Act è l'obbligo di garantire un'adeguata supervisione umana per i sistemi di IA ad alto rischio. Questo requisito è cruciale per mantenere il

---

Considering the imbalance of power in the context of work or education, combined with the intrusive nature of these systems, such systems could lead to detrimental or unfavourable treatment of certain natural persons or whole groups thereof …».

[77] Linee guida EDPB-EDPS sul *targeting* dei *social media* (2021) e Linee guida EDPB sul trattamento automatizzato (2022), le quali richiamano la necessità di usare *dataset* rappresentativi e continuamente verificati.

[78] I. Mendoza, L.A. Bygrave, *The Right Not to be Subject to Automated Decisions Based on Profiling*, in T.E. Synodinou, P. Jougleux, C. Markou, T. Prastitou (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer, 2017. Il Considerando 71 GDPR (il cui contenuto riguarda anche l'art. 22 GDPR sulle decisioni automatizzate) richiama espressamente il rischio di discriminazioni derivanti da profilazioni: «Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato […] è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato […]». Invita inoltre a mettere in atto misure tecniche e organizzative adeguate per evitare effetti discriminatori basati su razza, opinioni politiche, religione, appartenenza sindacale, stato genetico, stato di salute e orientamento sessuale.

[79] Un noto caso di discriminazione è quello del sistema di *recruiting* di Amazon che, nel 2018, mostrava *bias* di genere a causa di dati storici distorti (J. Dustin, *Insight - Amazon scraps secret AI recruiting tool that showed bias against women*, in *Reuters*, 2018).

controllo umano sulla tecnologia e per prevenire che le decisioni algoritmiche diventino incontestabili o incomprensibili[80]. L'art. 14 dell'AI Act stabilisce che i sistemi di IA ad alto rischio devono essere progettati e sviluppati in modo da consentire un'efficace supervisione da parte delle persone fisiche[81]. Ciò significa che gli operatori umani devono essere in grado di mantenere un controllo significativo sul sistema (che consenta loro di annullare o ignorare una decisione presa da un sistema di AI), sia termini di comprensione dei limiti e delle capacità del sistema, sia in termini di monitoraggio[82]. Questo requisito rafforza e specifica il «diritto a ottenere un intervento umano» già presente nell'art. 22 del GDPR. Le eccezioni a questo diritto richiedono «garanzie adeguate» che l'AI Act ora dettagliatamente specifica per i sistemi di IA ad alto rischio.

La supervisione umana non è intesa come una mera convalida passiva delle decisioni algoritmiche, ma come la capacità di un operatore di comprendere il contesto, di valutare le implicazioni etiche e sociali delle decisioni dell'IA e di intervenire attivamente quando necessario[83]. L'intervento umano, dunque, essere «effettivo» e non meramente formale, richiedendo una capacità reale dell'operatore di comprendere e valutare la decisione automatizzata[84]. Ciò comporta la necessità di una formazione adeguata degli operatori umani e di interfacce utente chiare, accessibili e trasparenti, che facilitino una supervisione efficace e intuitiva e riducano il rischio di errori[85]. Un «controllo significativo» da parte dell'essere umano in allineamento con il principio di *human oversight* (supervisione umana)[86], uno dei requisiti per l'IA affidabile promossi dalla Commissione Europea[87], ma anche dalla letteratura sulla responsabilità algoritmica, secondo cui il concetto di *meaningful human control* deve

[80] La centralità del fattore umano era già stata evidenziata dalla *High-Level Expert Group on AI* nelle *Ethics Guidelines for Trustworthy AI* del 2019, che individua la supervisione umana come uno dei sette requisiti fondamentali dell'IA affidabile. V. anche F. M. Zanzotto, *Viewpoint: Human-in-the-loop Artificial Intelligence*, in *Journal of Artificial Intelligence Research*, 64, 2019, 243ss., 251 il quale paragona l'HIL AI (Human in the Loop AI) a un Robin Hood «*that gives back what it steals*».

[81] Sul paradigma antropocentrico sotteso alla disciplina europea dell'intelligenza artificiale e sul ruolo della supervisione umana quale strumento di garanzia dei diritti fondamentali e dei principi dello Stato di diritto, v. O. Pollicino, *Stato di diritto, diritto costituzionale e intelligenza artificiale*, in *Lecostituzionaliste.it*; G. De Minico, E. Palomba, M. Parente, *AI Act e Legge italiana sull'Intelligenza artificiale: un'armonizzazione "fin troppo perfetta"*, in *Lecostituzionaliste.it*, 2025; O. Pollicino, *Semplificare l'AI senza arretrare sui diritti: la sfida costituzionale europea*, in *Agendadigitale.eui,* 2025.

[82] Il Considerando 71 dell'AI Act chiarisce che la supervisione deve permettere all'operatore di intervenire, sospendere o ignorare le decisioni dell'IA quando necessario, superando il rischio di *automation bias,* ossia l'accettazione passiva delle decisioni prese dalla macchina.

[83] B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica,* in *BioLaw Journal – Rivista di Biodiritto*, 2, 2021. In questi termini, cfr. anche S. Tranquilli, *Rapporto pubblico-privato nell'adozione e nel controllo della decisione amministrativa robotica*, Napoli, *passim*, 298.

[84] S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, *passim*, 2017.

[85] Sul tema dell'importanza di interfacce che consentano all'utente umano di verificare le basi fattuali della decisione, evitando l'opacità tecnica tipica dei modelli complessi EDPB–EDPS, *Joint Opinion 5/2021 on the proposal for an Artificial Intelligence Act*, 2021.

[86] Sul ruolo dei principi costituzionali di trasparenza, uguaglianza e autodeterminazione nell'orientare la disciplina dell'intelligenza artificiale e sulla possibile emersione del principio di human oversight quale nuova categoria interpretativa funzionale al bilanciamento dei rischi derivanti dall'impiego dell'IA, v. M. Fasan, *I principi costituzionali nella disciplina dell'Intelligenza Artificiale. Nuove prospettive interpretative,* in *DPCE Online*, 1, 2022, 181 ss.

[87] AI HLEG 2019.

includere consapevolezza, capacità di intervento e *accountability* individuale[88], anche se ciò può comportare rallentamenti in alcuni ambiti[89].
L'AI Act non è dunque una normativa a sé stante che ignora o sostituisce il GDPR. Al contrario, laddove il GDPR fornisce i principi fondamentali e i diritti generali relativi al trattamento dei dati personali, l'AI Act aggiunge un livello di specificità e di obblighi operativi per i sistemi di IA, in particolare per quelli ad alto rischio che utilizzano la profilazione. Un approccio di questo tipo potrebbe generare confusione nelle sfide per l'attuazione armonizzata tra le due normative, ad esempio in relazione ai dati personali da utilizzare per addestrare[90] i modelli.

4. AI Act come modello basato sulla classificazione del rischio e l'autocertificazione del fornitore: un «vizio genetico» del sistema? Nonostante l'ambizione e l'approccio *human-centric* dell'AI Act, la sua implementazione non è esente da criticità in particolare rispetto alla figura del fornitore[91]. L'approccio basato sul rischio che caratterizza l'AI Act, infatti, categorizza i sistemi di IA in base al potenziale impatto negativo sulla salute, sulla sicurezza e sui diritti fondamentali.
Il proposto Regolamento europeo sull'Intelligenza Artificiale (AI Act) istituisce un sistema di *enforcement* a due livelli per i sistemi di IA ad alto rischio: una valutazione di conformità *ex ante* e un piano di monitoraggio *ex post* sul mercato. Le valutazioni di conformità possono essere svolte internamente dal fornitore oppure esternamente da un organismo notificato, rispecchiando i modelli di audit interni ed esterni. Una valutazione conclusa con successo comporta il rilascio di una dichiarazione UE di conformità e l'apposizione del marchio CE sul prodotto (il sistema di IA), che consente la libera circolazione del sistema nel mercato interno. Il monitoraggio sul mercato richiede che i fornitori documentino continuamente le prestazioni del sistema, segnalino incidenti gravi e consentano alle autorità di intervenire durante tutto il ciclo di vita del prodotto.
L'approccio basato sul rischio dell'AI Act si allinea quindi alle valutazioni d'impatto sulla protezione dei dati del GDPR (*Data Protection Impact Assessment*, DPIA[92]), ma aggiunge le Valutazioni d'Impatto sui Diritti Fondamentali (*Fundamental Rights Impact Assessment*, FRIA)

---

[88] F. Santoni de Sio, J. van den Hoven, *Meaningful Human Control over Autonomous Systems: A Philosophical Account*, Frontiers in *Robotics and AI*, 2018, in cui si cerca di definire il concetto di «*meaningful human control*» con particolare riferimento al tema delle armi autonome.
[89] B. Crook, M. Schlüter, T, Speith, *Revisiting the Performance-Explainability Trade-Off in Explainable Artificial Intelligence (XAI)*, in IEEE 31st International Requirements Engineering Conference Workshops (REW), 2023, 316. Il caso è quello dell'utilizzo dei LLMs (Large Language Models) in campi come quello oncologico, in cui la tecnologia spesso performa meglio degli attori umani; in questi casi, privilegiare la spiegabilità dell'algoritmo, può creare rallentamenti e rendere i trattamenti meno effettivi. In senso parzialmente diverso anche C. Rudin, *Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead,* in *Nature Machine Intelligence*, 1, 2019, 206–215.
[90] Il GDPR principalmente all'art. 5 richiede infatti il rispetto dei principi di minimizzazione e limitazione della finalità nell'utilizzo dei dati personali. Potrebbero porsi interrogativi rispetto ai modelli di *deep learning*, in cui il modello è addestrato in base alla maggior quantità possibile di dati di alta qualità disponibili.
[91] In base all'AI Act, art. 3 punto 3, il fornitore è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito».
[92] F. Faini, *Big Data, Algoritmi e diritto*, in *DPCE Online*, 3, 2019, 1869 ss., 1880 : «Nella disciplina in materia di *data protection* il diritto si avvale della tecnica per assicurare il suo rispetto e tutelare la persona per mezzo dei principi *data protection by default e by design* e di strumenti come il *data protection impact assessment*: la tecnologia si pone quale rimedio preventivo a possibili violazioni delle norme, proteggendo la persona fin dalla progettazione, per impostazione preventiva e per mezzo della valutazione d'impatto».

e le Valutazioni di Conformità (*Conformity Assessment*, CA) per affrontare rischi etici più ampi. Questo doppio quadro regolatorio crea obblighi sovrapposti per le organizzazioni che operano sia come titolari del trattamento ai sensi del GDPR sia come fornitori di sistemi di IA secondo l'AI Act. Armonizzare DPIA, FRIA e CA può semplificare la *compliance*, ridurre duplicazioni e favorire una strategia coerente di gestione del rischio[93].

La criticità principale dei sistemi ad alto rischio, uno degli aspetti più dibattuti dalla dottrina pubblicistica, riguarda la valutazione iniziale del rischio[94] e la conformità, che, per la maggior parte dei sistemi ad alto rischio, è affidata al fornitore (produttore) del sistema di IA, con controlli esterni previsti solo in alcuni casi[95]. Tali applicazioni dei sistemi di IA sono tutt'altro che infallibili e neutre, suscettibili di incidere negativamente sui diritti fondamentali dei cittadini, determinando violazioni della *privacy*, minacce alla sicurezza e discriminazioni. Di qui una serie di obblighi[96] che il fornitore deve rispettare, tra cui una *governance* e una qualità adeguate dei dati (art. 10), una sufficiente trasparenza nei confronti dell'utilizzatore (art. 13) e la garanzia di una costante sorveglianza umana (art. 14), per scongiurare decisioni esclusivamente automatiche. La previsione dell'insieme dei requisiti implica che l'ingresso del sistema ad alto rischio (o la sua utilizzazione) non possa avvenire se prima non se ne sia verificata la conformità. Il sistema di verifica è affidato alla procedura di marcatura CE, già impiegata per regolare l'ingresso e la circolazione di altri prodotti nell'Unione: non è dunque stabilito un regime autorizzatorio affidato alle autorità pubbliche, come è previsto ad esempio per i medicinali o per i prodotti OGM, ma il regolamento affida il controllo di conformità al fornitore stesso o, in ipotesi eccezionali, ad un organismo certificatore terzo (è il caso dei sistemi biometrici)[97]. A seguito della verifica, sul prodotto viene apposto il marchio e si procede alla registrazione[98].

Questo assetto regolatorio si inserisce in una più ampia tendenza del diritto pubblico contemporaneo verso modelli di autoregolazione e co-regolazione, nei quali l'intervento pubblico tende a collocarsi prevalentemente a valle, lasciando agli operatori privati un ruolo centrale nella definizione e nell'attuazione degli standard di conformità, con un conseguente ripensamento del ruolo delle autorità amministrative[99].

Nel quadro delineato dall'Articolo 3(2) dell'AI Act, il processo di valutazione della conformità assume una forma molto precisa per il fornitore di sistemi di IA ad alto rischio. Egli è infatti il soggetto primariamente responsabile dell'intero ciclo di verifica, indipendentemente dal fatto che la valutazione possa in alcuni casi essere eseguita anche dal

[93] P. (Shemy) Gruchala, L. Nicosia, M. Zięciak, *Harmonising risk assessments for high-risk AI systems under the GDPR and the AI Act*, in *Journal of Data Protection & Privacy*, 7(4), 2025, 359–371; E. Thelisson, V. Himanshu, *Conformity assessment under the EU AI act general approach,* in *AI and Ethics* 4, 2024, 113–121.

[94] A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law*, 2020, 1, 2020, 66.

[95] Un modello di *preliminary self*-assessment a cui fanno seguito controlli esterni obbligatori in caso di sistemi ad alto rischio è contenuto in F. Pasquale, G. Malgieri, *From Transparency to Justification: Toward Ex Ante Accountability for AI,* in *Brussels Privacy Hub Working Papers*, vol. 8 n. 33, 2022.

[96] Sulla possibilità di una strategia integrata tra il *risk assessment* stabilito dal GDPR e dall'AI Act — *specifically* DPIAs, FRIAs and CAs — P. (Shemy) Gruchala, L. Nicosia, M. Zięciak, *Harmonising risk assessments for high-risk AI systems under the GDPR and the AI Act*, in *Journal of Data Protection & Privacy*, 7(4), 2025, *passim*, 359–371.

[97] Sulla verifica di conformità v. E. Thelisson, H. Verma, *Conformity Assessment under the EU AI Act General Approach*, 2024.

[98] Gli obblighi relativi alla marcatura CE e alla registrazione, rispettivamente contenuti negli artt. 48 e 49, diventeranno pienamente vincolanti per i sistemi di IA ad alto rischio a partire dal 2 agosto 2026.

[99] Sul tema v. C.P. Guarini, *La regolazione quale meccanismo di governo dell'economia. Premesse epistemologiche*, in F. Gabriele et al., *Costituzione, diritti sociali ed economia*, Bari, 2020. Sui modelli di regolazione decentrata e sul progressivo spostamento di funzioni di garanzia verso soggetti privati nel diritto pubblico del digitale, v. E. Cocchiara, *Nuove autonomie e regolazione amministrative nell'ecosistema digitale, in Nuove Autonomie,* 1, 2025.

fabbricante del prodotto che integra l'IA, dal distributore o dall'importatore. Il fornitore deve predisporre e mantenere un sistema di gestione della qualità[100] e assicurarsi che il modello, il *software* e i dati soddisfino i requisiti essenziali di cui agli articoli 8–15 dell'AI Act (*governance* del rischio, qualità dei dati, documentazione tecnica, *log*, trasparenza, *cybersecurity*, ecc.). Inoltre, secondo l'art. 43, spetta al fornitore scegliere e applicare la procedura di conformità appropriata (autovalutazione o intervento di un organismo notificato), preparare la documentazione tecnica e rendere disponibile tutto il materiale necessario per i controlli successivi. A differenza degli altri operatori della filiera, il fornitore non può limitarsi a verifiche formali: deve garantire che il sistema sia progettato e sviluppato in modo conforme e che tale conformità sia dimostrabile in ogni momento[101].

Questo approccio, basato sul *self-assessment* o auto-certificazione da parte del produttore, solleva serie e fondate preoccupazioni, in primo luogo per il potenziale conflitto d'interessi in capo al fornitore che, in quanto soggetto economico operante in un mercato competitivo, ha un interesse primario a immettere il proprio prodotto sul mercato nel modo più efficiente, rapido e vantaggioso possibile. La dottrina pubblicistica ha messo in luce come modelli di regolazione fondati prevalentemente sull'autovalutazione degli operatori economici rischino di tradursi in una progressiva privatizzazione della funzione di tutela degli interessi generali, soprattutto nei settori in cui sono coinvolti diritti fondamentali e interessi costituzionalmente rilevanti[102]. La valutazione del rischio, in tale contesto, può essere intrinsecamente influenzata da logiche di mercato, soprattutto con riferimento agli algoritmi nel settore pubblico[103], portando a una possibile minimizzazione dei rischi percepiti o a un'interpretazione delle soglie di «alto rischio» più favorevole ai propri interessi commerciali anche in settori in cui si elaborano dati personali. Affidare a un attore privato una valutazione così cruciale per i diritti fondamentali può generare una potenziale situazione di *regulatory capture*[104], in cui gli interessi dell'industria rischiano di prevalere sulla tutela pubblica[105].

La critica non è al principio di autoregolamentazione in sé, che può avere la sua validità in altri contesti (es. standard tecnici meno impattanti sui diritti), ma alla sua applicazione in un settore con un potenziale di impatto così elevato sui diritti individuali e collettivi. Il produttore detiene il *know-how* tecnico, le informazioni sui dati di addestramento e i risultati dei test interni, rendendo difficile per un osservatore esterno o per un'autorità pubblica replicare o verificare completamente la sua valutazione, senza un accesso diretto e profondo[106]. Si tratta dunque di una potenziale debolezza strutturale intrinseca al *design* stesso

---

100 Artt. 8-15 AI Act.

101 E. Thelisson, H. Verma, *Conformity Assessment under the EU AI Act General Approach*, 4, 2024, 113–121.

102 Sul rischio di indebolimento del controllo pubblico e di «cattura regolatoria» nei modelli fondati sull'autovalutazione degli operatori economici, v. E. Cocchiara, op. cit.; nonché C.P. Guarini, *Contributo allo studio della regolazione "indipendente" del mercato*, Cacucci, 2005, 240 ss.

103 P. Alston, *The Digital Welfare State –Report of the Special Rapporteur on Extreme Poverty and Human Rights, UN Human Rights Council,* 2019.

104 T. Metcalf, *AI safety and regulatory capture*, in *AI & Society*, 2025: «*Arguably, some of the people who know the most about AI safety would be the AI entrepreneurs and engineers themselves.3 However, there is a potential conflict of interest. Suppose that a prominent AI entrepreneur is a political ally of the president of a major economy. The AI entrepreneur could be in the enviable position of advising the government on the legal regulation of the AI market in that nation. This would allow this AI entrepreneur to use regulations to secure benefits for their own firm and allies' firms, while harming competing AI firms and the general public*».

105 Sulla posizione delle pubbliche amministrazioni rispetto all'IA e la mancanza di autonomia piena rispetto al fornitore dell'algoritmo v. B. Ponti, *Il fornitore dell'algoritmo quale soggetto estraneo all'amministrazione,* in *Rivista Italiana di Informatica e Diritto*, 2, 2024.

106 O. Pollicino, *The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism*, in *European Law Journal*, 29, 2023, 10 ss., 11: *«within the new algorithmic society, private transnational corporations (operators) are de facto increasingly performing public functions through the "governance" of digital spaces (space)».*

della norma legata all'idea che, se il primo e più critico filtro per la sicurezza e la conformità (la valutazione del rischio) è nelle mani del soggetto direttamente interessato (il produttore), il rischio di compromissioni alla tutela dei diritti è insito nella genesi stessa del sistema di regolamentazione. Ciò non implica mala fede del produttore, ma piuttosto una propensione naturale a ottimizzare i propri processi e costi, che potrebbe non coincidere con la massima prudenza e rigorosità richieste per la protezione dei diritti fondamentali.

Il fornitore mantiene una posizione centrale e spesso determinante anche nel rapporto con gli altri operatori economici. Gli artt. 16–26 dell'AI Act definiscono, infatti, obblighi specifici per ciascun attore, ma questi obblighi si innestano quasi sempre sulle responsabilità originarie del fornitore. Il prodotto finale che incorpora l'IA può essere immesso sul mercato da un fabbricante, distribuito da un rivenditore o importato da un soggetto terzo, ma tutti costoro dipendono dalla qualità e completezza del lavoro svolto dal fornitore: la documentazione tecnica, le istruzioni d'uso, le misure di monitoraggio e gli aggiornamenti sono predisposti dal fornitore e costituiscono la base dell'intero sistema di compliance. Di conseguenza, anche se il fabbricante può essere considerato *provider* quando integra l'IA nel proprio prodotto e ne determina la finalità, nella pratica operativa la qualità dell'algoritmo e della documentazione del fornitore influenza in modo decisivo la possibilità degli altri operatori di rispettare i loro obblighi di cui agli artt. 23–26[107]. E questo solleva questioni fondamentali sulla distribuzione del potere e della responsabilità. In un sistema di diritto pubblico, la tutela dei diritti è un compito primario dello Stato e delle sue autorità. Quando un'attività privata può incidere così profondamente sui diritti, lo Stato deve garantire un controllo effettivo e indipendente fin dalle fasi iniziali.

Inoltre, quando il sistema di IA ad alto rischio richiede la valutazione da parte di un organismo notificato, il fornitore è l'attore chiamato a sostenere l'intero dialogo tecnico. Secondo l'articolo 43, il fornitore deve consegnare la documentazione tecnica, dimostrare la conformità del sistema ai requisiti essenziali, consentire *audit*, prove e ispezioni e integrare eventuali prescrizioni correttive. Mentre gli altri operatori si limitano generalmente a custodire informazioni o a garantire che il sistema venga utilizzato conformemente alle istruzioni, solo il fornitore possiede e controlla la progettazione del modello e dei *dataset*, e quindi solo il fornitore può rispondere pienamente alle domande tecniche avanzate dagli organismi notificati.[108]

La dimensione *post-market* è un ulteriore ambito in cui il fornitore gioca un ruolo fondamentale. Gli articoli 61 e 62 impongono al fornitore l'obbligo di implementare un sistema di *post-market monitoring*[109] continuo, capace di raccogliere, analizzare e valutare dati reali sul funzionamento del sistema di IA. Deve quindi monitorare il comportamento del modello, individuare anomalie, malfunzionamenti, effetti degradanti o rischi emergenti e intervenire rapidamente con aggiornamenti tecnici o misure correttive. Deve inoltre segnalare gli incidenti gravi o i malfunzionamenti sistemici alle autorità competenti entro i termini previsti. Gli altri attori della filiera contribuiscono solo trasmettendo le informazioni di cui vengono a conoscenza, ma tutta l'architettura di monitoraggio, analisi e risposta rimane prerogativa del fornitore. È il fornitore che conosce l'algoritmo, che può modificarlo e che può prevenire o mitigare i rischi[110]. Infine, lungo l'intero ciclo di vita del sistema di IA, il

[107] E. Thelisson, H. Verma, op. cit.
[108] E. Thelisson, H. Verma, op.cit.
[109] Sul fatto che l'AI Act possa costituire una proposta di stabilire un ambiente per condurre *auditing* sui sistemi di IA a livello europeo: J. Mökander, M. Axente, F. Casolari, L. Floridi, *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation*, in *Minds and Machines,* 32, 2024, 241–268.
[110] E. Thelisson, H. Verma, op.cit.

fornitore è responsabile della gestione degli aggiornamenti, dell'evoluzione del modello e dell'adeguamento continuo ai requisiti normativi. L'articolo 15 impone requisiti di *cybersecurity* e *robustness*; l'articolo 17 riconosce al *provider* la responsabilità di mantenere e aggiornare la documentazione tecnica; e, come già visto, l'articolo 61 stabilisce il monitoraggio durante l'uso reale. Ogni modifica significativa al modello può riattivare obblighi di valutazione della conformità e deve essere documentata in modo rigoroso. Anche in questa fase, il ruolo del fornitore è insostituibile: è l'unico soggetto con la capacità tecnica e giuridica di garantire che il sistema rimanga conforme e sicuro anche dopo la sua immissione sul mercato[111].

Il *self-assessment* del fornitore, pur snellendo i processi per l'innovazione, sposta gran parte dell'onere di controllo a posteriori sulle autorità di vigilanza previste dagli artt. 70–72 dell'AI Act che garantiscono il controllo della conformità dei sistemi di IA ad alto rischio dopo la loro immissione sul mercato. Nel rapporto con il fornitore dell'algoritmo, esse possono richiedere l'accesso alla documentazione tecnica (artt. 11 e 17), ai log (art. 12), ai risultati del monitoraggio post-commercializzazione (art. 61) e alle segnalazioni di incidenti gravi (art. 62). Il fornitore deve cooperare pienamente, fornendo informazioni, adottando misure correttive e, se necessario, ritirando o sospendendo il sistema. In questo modo, si realizza un controllo continuo sul rispetto dei requisiti essenziali (artt. 8–15), assicurando che il sistema di IA mantenga nel tempo livelli adeguati di sicurezza, affidabilità e conformità normativa. Questo approccio di «autoregolamentazione vigilata» deve essere attentamente bilanciato per evitare che la vigilanza sia insufficiente, trasformandosi in una mera ratifica di scelte già compiute.

Una delle conseguenze più gravi delle criticità delineate è la crescente difficoltà per l'individuo di ottenere una tutela effettiva in caso di violazioni o danni causati dai sistemi di IA, specialmente da quelli che impiegano la profilazione algoritmica.

La prima grande difficoltà deriva dalla moltiplicazione dei decisori e, quindi, dalla concreta attribuzione delle responsabilità. Il GDPR ha già introdotto una complessa ripartizione delle responsabilità tra titolare del trattamento, responsabile del trattamento e altri attori (es. co-titolari). L'AI Act aggiunge un ulteriore elemento di complessità e nuovi attori, introducendo le figure del fornitore, dell'utilizzatore (o *deployer*), dell'importatore, del distributore e del rappresentante autorizzato. Questa moltiplicazione dei soggetti coinvolti nel ciclo di vita di un sistema di IA, dalla sua progettazione e addestramento fino all'utilizzo finale, rende estremamente arduo per il cittadino identificare chi sia il responsabile effettivo di un eventuale danno o di una violazione dei diritti. La nebulosità nell'attribuzione della responsabilità crea un «vuoto di *accountability*» che può lasciare l'individuo senza un interlocutore chiaro e il silenzio sulla tutela *ex post* (evidentemente lasciata ai governi nazionali) potrebbe rendere sempre più difficile per il cittadino ottenere giustizia. Anche qualora si riesca a identificare il potenziale responsabile, l'asimmetria informativa gioca un ruolo cruciale, talvolta insormontabile perché il cittadino è spesso privo delle conoscenze tecniche necessarie per comprendere il funzionamento dell'algoritmo, i dati su cui si basa, le logiche decisionali che hanno portato a una determinata conclusione e, in definitiva, le ragioni della decisione automatizzata che lo ha pregiudicato. La conseguenza diretta di tutti questi fattori è una significativa difficoltà nell'accesso al rimedio. Il diritto a un ricorso giurisdizionale effettivo e a un equo processo, garantito dall'art. 47 della Carta dei Diritti Fondamentali dell'UE e dall'art. 6 della CEDU, rischia così di svuotarsi di significato e i requisiti di trasparenza dell'AI Act, pur costituendo un passo nella giusta direzione, potrebbero non essere sufficienti a colmare questo divario informativo.

[111] E. Thelisson, H. Verma, op.cit.

In tale prospettiva, la frammentazione delle responsabilità e l'asimmetria informativa che caratterizzano questi modelli regolatori rischiano di compromettere l'effettività delle garanzie pubbliche, spostando il baricentro della tutela dai diritti sostanziali alla mera osservanza formale degli obblighi procedurali. Questa dinamica riflette una tensione strutturale tipica della regolazione del digitale, in cui la frammentazione delle responsabilità e il ruolo centrale dei privati rendono difficile ricondurre l'esercizio di poteri incidenti sui diritti a forme effettive di controllo pubblico[112].

5. AI Act: tra criticità e prospettive. Alla luce delle criticità delineate, è imperativo che il percorso intrapreso dall'Unione europea prosegua con un approccio proattivo, adattivo e strutturalmente orientato al continuo rafforzamento delle garanzie per i diritti fondamentali. L'AI Act rappresenta una pietra miliare, ma la sua piena efficacia dipenderà dalla capacità di affrontare e mitigare le debolezze intrinseche del sistema, garantendo una supervisione indipendente, una implementazione robusta e la continua evoluzione di meccanismi che assicurino una tutela effettiva e accessibile per l'individuo nell'era digitale. La sfida è quella di costruire un «ecosistema di fiducia» e non semplicemente un quadro di conformità tecnica[113], perciò le prospettive future devono orientarsi verso diverse direzioni, che richiedono un impegno congiunto di legislatori, autorità di vigilanza, sviluppatori, utenti e società civile.

Il nodo cruciale resta la prima valutazione del rischio da parte del fornitore: un dispositivo che, pur rispondendo all'esigenza di efficienza regolatoria, espone l'intero impianto a un possibile sbilanciamento verso regole di mercato[114]. Per mitigarne gli effetti è fondamentale rafforzare in modo significativo la supervisione indipendente, in un'ottica di *co-regulation*[115]. Ciò significa in primo luogo potenziare gli organismi notificati e i meccanismi di audit indipendente, non solo in termini di competenze avanzate e risorse disponibili, ma anche considerando un ampliamento delle categorie di sistemi per cui l'autovalutazione del fornitore debba essere integrata dall'intervento di un organismo terzo, oppure con l'introduzione di audit indipendenti periodici per tutti i sistemi ad alto rischio, anche quelli inizialmente auto-certificati. Tale audit dovrebbe essere sia tecnico che etico-giuridico, verificando non solo la conformità alle specifiche tecniche, ma anche il rispetto dei principi di equità, non discriminazione e trasparenza[116].

In secondo luogo, le Autorità nazionali competenti dovrebbero essere in grado di condurre audit tecnici sui sistemi di IA, di richiedere documentazione e spiegazioni dettagliate e di imporre misure correttive effettive. L'investimento nella formazione di personale specializzato (giuristi con competenze tecniche, tecnologi con competenze giuridiche)[117] è indispensabile anche in caso di risorse limitate in capo alle autorità stesse.

Si impone, infine, la necessità di armonizzazione delle prassi e la cooperazione tra le varie Autorità a livello europeo e nazionale. In questo senso il Comitato Europeo per l'Intelligenza Artificiale (AI Board), istituito dall'AI Act, e il Comitato Europeo per la Protezione dei Dati

---

[112] Sulle implicazioni che i modelli regolatori multilivello e multi-attore producono in termini di effettività della tutela e di *accountability* nel diritto pubblico contemporaneo v. E. Cocchiara, op. cit.

[113] L. Floridi, *The Ethics of Artificial Intelligence*, Oxford, 2023.

[114] Sulla possibilitá di sviluppare soluzioni «socio-tecniche» sviluppate *in house* dalle pubbliche amministrazioni nel settore pubblico per le funzioni pubbliche che non possono essere lasciate ai privati, N. Bharosa, *The rise of GovTech: Trojan horse or blessing in disguise? A research agenda,* in *Government Information Quarterly*, Volume 39, Issue 3, 2022.

[115] E. Fosch Villaronga, A. JR Golia, *Robots, standards and the law: Rivalries between private standards and public policymaking for robot governance*, *passim*, *Computer Law & Security Review*, 35, 2, 2019, 132 s. In senso conforme G. Mobilio, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica,* in *Biolaw Journal*, 2, 2020.

[116] Alta Commissione Europea, *Ethics Guidelines for Trustworthy AI*, 2019.

[117] T. Metzger, J. Powles, *A New Digital Constitutionalism?*, in *International Journal of Constitutional Law,* 2021.

(EDPB) dovranno lavorare in stretta sinergia per sviluppare linee guida comuni, armonizzare le prassi di applicazione e risolvere i casi transfrontalieri[118] che coinvolgono sia aspetti di conformità AI Act che di protezione dati. Solo una cooperazione efficace potrà prevenire «lacune di responsabilità» e garantire una tutela coerente in tutta l'Unione, evitando che le aziende possano sfruttare le differenze interpretative o applicative tra i vari Stati membri. Questa prospettiva dovrebbe auspicabilmente essere estesa al livello internazionale, promuovendo la diffusione di standard etici e buone pratiche collaborando con paesi terzi e organizzazioni multilaterali (come ONU, OCSE, ecc)[119] nonché lavorando sui meccanismi di interoperabilità tra le normative.

Il percorso verso una *governance* dell'IA pienamente etica e conforme ai diritti fondamentali è ancora in salita perché, anche in presenza di una «tutela integrata» tra AI Act e GDPR[120], affidare a soggetti privati la prima e cruciale valutazione della conformità, quand'anche poi soggetta a controlli *ex post*, introduce una tensione tra logiche di mercato e prioritaria tutela dei diritti, rischiando di compromettere l'indipendenza e l'efficacia del controllo pubblico. Questa impostazione, unita alla persistente opacità degli algoritmi («scatola nera») e alla pervasività del trattamento massivo di dati (che alimenta la sorveglianza algoritmica)[121], crea un terreno fertile per effetti distorsivi. Tali effetti possono manifestarsi non solo come discriminazioni involontarie o *bias* sistemici, ma anche come una sottile limitazione delle opportunità e delle alternative di scelta dell'individuo, minandone l'autodeterminazione e la libertà[122].

La conseguenza più preoccupante di queste criticità è lo svuotamento del diritto come conseguenza dello «scollamento» tra lo *status* di utente/cittadino e la possibilità di ottenere tutela effettiva[123]. La moltiplicazione degli attori nella catena di sviluppo e utilizzo dell'IA rende complessa l'attribuzione della responsabilità; l'asimmetria informativa e la complessità tecnica impediscono all'individuo di comprendere e contestare efficacemente le decisioni algoritmiche e gli oneri processuali possono rendere l'accesso alla giustizia molto difficoltoso[124]. Questo è particolarmente vero nel contesto della pubblica amministrazione dove l'uso di algoritmi per la profilazione richiede un'attenzione ancora maggiore ai principi di legalità, imparzialità e sindacabilità: senza trasparenza effettiva, tali principi rischiano di rimanere puramente formali[125].

Le prospettive future chiamano a un impegno continuo e multilivello. È indispensabile rafforzare la supervisione indipendente delle autorità di vigilanza, dotandole di risorse e competenze adeguate per audit tecnici e giuridici. Si deve promuovere un approccio di *open*

[118] Art. 56 ss. AI Act.
[119] OCSE, *OECD Framework for the Classification of AI Systems*, 2022.
[120] G. Sartor, F. Lagioia, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, European Parliament Research Service, 2020.
[121] S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR*, in *International Data Privacy Law*, op. cit.
[122] F. Pasquale, *The Black Box Society*, Cambridge (Massachussetts), 2015.
[123] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà,* in *Biolaw Journal - Rivista di Biodiritto*, 1, 2019, 63 ss., 89: «dinanzi alla promessa di sostituire le attività umana pesanti (non solo in senso fisico, ma anche cognitivo) con una serie di processi automatici, scambiando così l'autonomia con l'automazione, il rischio è che le libertà fondamentali non vengano negate o violate, semplicemente divengano inutili».
[124] C. O'Neil, *Weapons of Math Destruction*, New York, 2016.
[125] Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472 (caso «logaritmo INPS») sul rilievo della trasparenza e della conoscibilità dell'algoritmo utilizzato nell'ambito dell'attività amministrativa.

by design per la trasparenza e la spiegabilità degli algoritmi[126], investendo nella ricerca su XAI e in metodologie per la mitigazione dei *bias*. È cruciale garantire un accesso effettivo alla giustizia attraverso meccanismi di ricorso chiari, accessibili e che tengano conto dell'asimmetria informativa. Non meno importante è l'*empowerment* del cittadino attraverso programmi di alfabetizzazione digitale e lo sviluppo di un pensiero critico sull'IA. Infine, la cooperazione tra autorità nazionali ed europee è vitale per armonizzare gli standard e affrontare una tecnologia che per sua natura non conosce confini. La cooperazione tra autorità nazionali ed europee dovrà diventare un pilastro strutturale, capace di affrontare una tecnologia che evolve con ritmi esponenziali.
L'AI Act rappresenta dunque un inizio promettente, ma non un punto d'arrivo[127]. La sua applicazione e la futura evoluzione richiederanno una costante vigilanza, una capacità di adattamento e un dialogo costruttivo tra tutte le parti interessate per assicurare che l'Intelligenza Artificiale contribuisca a una società più giusta, equa e rispettosa della dignità umana. La sfida è complessa, ma la posta in gioco – la tutela dei diritti fondamentali nell'era algoritmica[128] – richiede vigilanza costante e capacità di adattamento, attraverso un dialogo aperto tra istituzioni, tecnici, giuristi e società civile.

Abstract. L'*Artificial Intelligence Act* introduce un modello di regolazione dell'intelligenza artificiale fondato sulla classificazione del rischio, volto a garantire un elevato livello di tutela dei diritti fondamentali nel mercato europeo. Il contributo sostiene che, con specifico riferimento alla profilazione algoritmica, tale modello presenti una criticità strutturale, nella misura in cui l'affidamento della valutazione iniziale del rischio al fornitore del sistema di IA può incidere negativamente sull'effettiva protezione dei diritti fondamentali. Muovendo dal diritto alla protezione dei dati personali e alla privacy nel diritto pubblico europeo, il contributo esamina il rapporto tra l'AI Act e il GDPR, mettendo in luce le tensioni sistemiche che emergono con riferimento ai sistemi di profilazione qualificati come ad alto rischio. L'articolo sostiene che tale scelta regolatoria configuri un potenziale «vizio genetico» del modello, idoneo a favorire fenomeni di privatizzazione delle decisioni regolatorie.

Abstract. The *Artificial Intelligence Act* introduces a risk-based regulatory model for artificial intelligence, aimed at ensuring a high level of protection of fundamental rights within the European market. This article argues that, with specific regard to algorithmic profiling, such a model reveals a structural concern, in that entrusting the initial assessment of risk to the AI

[126] Sulla possibilità di affiancare alla *black box* dei sistemi *white box* predisposti per fornire spiegazioni sulle decisioni prese dall'algoritmo, F. Zambonelli, *Algocrazia. Il governo degli algoritmi e dell'intelligenza artificiale,* Trieste, 2020.
[127] Sul ruolo dell'AI Act quale strumento volto a ricondurre lo sviluppo dell'intelligenza artificiale entro una cornice di tutela dei diritti fondamentali e della dignità della persona, nella prospettiva del passaggio dalla «funzione regolamentare della tecnica» (*Lex*) alla valorizzazione della «funzione ordinante del diritto» (*Ius*), v. M.P. Mantovani, *Intelligenza artificiale e tutela dei diritti fondamentali nella prospettiva europea: il passaggio da Lex a Ius*, in *Annali della Facoltà Giuridica dell'Università di Camerino*, 2025. In senso analogo, sul ruolo della regolazione dell'intelligenza artificiale nella tutela dei diritti fondamentali e nel quadro del costituzionalismo multilivello, v. M. D'Amico, *L'intelligenza artificiale e la sfida regolatoria sul duplice versante, europeo e nazionale*, cit.; sul ruolo del diritto e del sistema delle fonti quale possibile argine al crescente potere della tecnica, v. G. De Minico, *Le fonti del diritto: un argine all'intelligenza artificiale?*, cit.
[128] A. Pajno *et al.*, *Focus: Profili giuridici, etici e tecnologici dell'Intelligenza Artificiale,* in *Biolaw Journal – Rivista di Biodiritto*, 3, 2019: «Appare dunque necessario che, a fronte dell'erompere dei sistemi di intelligenza artificiale, i giuristi profondano gli sforzi per restituire un ecosistema antropocentrico, nel quale il fattore tecnologico non sovrasti e non si imponga sui valori, primo fra tutti la dignità, su cui si incentra la tutela dell'individuo. In tal senso, si avverte la necessità che il diritto "guidi" e "orienti" la tecnologia, onde permetterle di percorrere binari rispettosi di un sistema assiologico di valori riflesso nelle costituzioni degli stati moderni e nei trattati internazionali».

system provider may undermine the effective protection of fundamental rights. Starting from the right to the protection of personal data and privacy in European public law, the contribution examines the relationship between the AI Act and the GDPR, highlighting the systemic tensions that emerge in relation to profiling systems classified as high-risk. The article contends that this regulatory choice constitutes a potential «genetic flaw» of the model, capable of fostering the privatization of regulatory decision-making.

Parole chiave. Artificial Intelligence Act – profilazione algoritmica – diritti fondamentali – regolazione del rischio – accountability algoritmica.

Key words. Artificial Intelligence Act – algorithmic profiling – protection of fundamental rights – risk-based regulation – algorithmic accountability.