GIURETA
Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente
Vol. XXIV
2026

ASPETTI GIURIDICI SULL'UTILIZZAZIONE DELL'INTELLIGENZA ARTIFICIALE NEL TRACCIAMENTO DIGITALE DEI PRODOTTI ALIMENTARI. STATO DELL'ARTE E PROSPETTIVE [*]

Marco Gjomarkaj [**]

SOMMARIO: 1. L'AI come fattore di trasformazione dei sistemi produttivi – 1.1 L'impiego di sistemi di AI nella filiera produttiva agro-alimentare – 2. La gestione diffusa dei dati in agricoltura con tecnologie blockchain: criticità e problemi aperti – 3. La disciplina europea sull'intelligenza artificiale: l'AI Act – 3.1 Problemi connessi all'utilizzo di sistemi di IA generativi – 3.2 Profili di responsabilità: la nuova direttiva europea sulla responsabilità per danno da prodotti difettosi - 4. L'evoluzione della normativa nazionale sull'IA: l. 23 settembre 2025, n. 132 – 5. Considerazioni finali.

1. – Nell'era della digitalizzazione dei processi produttivi e della gestione digitale delle attività economiche, l'applicazione dell'Intelligenza Artificiale (IA) nelle dinamiche di mercato costituisce un fenomeno di forte impatto giuridico, che incide innegabilmente sulle modalità di esercizio delle attività imprenditoriali, sull'organizzazione delle filiere e sui rapporti di natura privatistica intercorrenti tra gli operatori economici [1].

A differenza di altre tecnologie di automazione, in termini generali, l'IA introduce forme di elaborazione e decisione basate su modelli di apprendimento automatico, capaci di operare in condizioni di complessità e di incer-

[*] Ricerca finanziata nell'ambito del Progetto "AQuSDIT", PNRR – "SERICS", Spoke 5, Codice Progetto: PRJ- 1636 - CUP: H73C22000880001.

[**] Dottore di ricerca in Diritto agrario e alimentare.

[1] Cfr. A. Aghababaei-F. Aghababaei-M. Pignitter-M. Hadidi, *Artificial Intelligence in Agro-Food Systems: From Farm to Fork*, in *Foods MDPI,* 14, 2025, 411, disponibile all'indirizzo web https://doi.org/10.3390/foods14030411; con specifico riguardo al settore agroalimentare cfr. A. Tommasini, *La rivoluzione tecnologica nell'agroalimentare: algoritmi e innovazione digitale tra rischi e opportunità*, a cura di S. Carmignani-N. Lucifero , in *Le regole del mercato agroalimentare tra sicurezza e concorrenza. Diritti nazionali, regole europee e convenzioni internazionali su agricoltura, alimentazione e ambiente. Atti del convegno di Firenze del 21 e 22 novembre 2019 in onore della Prof.ssa Eva Rook Basile*, Napoli, 2020, 787.

tezza, incidendo direttamente sui processi decisionali rilevanti per l'attività produttiva in generale.

Sotto il profilo economico-organizzativo, l'impiego di sistemi di IA consente una progressiva integrazione tra dati, processi e risultati, in grado di favorire modelli produttivi orientati all'ottimizzazione continua, alla previsione dei rischi e alla gestione anticipata delle dinamiche di mercato. Tale evoluzione determina, come anticipato, un mutamento sostanziale della funzione imprenditoriale, nella misura in cui l'attività decisionale viene in gran parte delegata a sistemi automatizzati, capaci di influenzare (ottimizzare) scelte strategiche e operative.

Dal punto di vista giuridico, questa trasformazione solleva non pochi interrogativi in ordine alla riconducibilità delle decisioni automatizzate all'agire umano, alla distribuzione delle responsabilità lungo la catena produttiva e alla compatibilità dei sistemi di AI con i principi fondamentali di ogni ordinamento, quali la libertà di iniziativa economica, la tutela della concorrenza, la protezione degli interessi collettivi, etc.

L'IA, in tal senso, non si limita a fornire nuovi strumenti per produrre, ma, come vedremo, incide sulle categorie tradizionali del diritto di impresa e dei mercati, imponendo una loro rilettura alla luce dei processi decisionali automatizzati.

Non v'è dubbio, poi, che in un settore come quello agro-alimentare tale impatto risulta accentuato dalla presenza di interessi pubblici qualificati, come la sicurezza alimentare, la tutela della salute, il rispetto dei diritti umani, il bilanciamento tra principi costituzionali, la protezione ambientale, il corretto funzionamento del mercato, etc.

Come vedremo, in questo settore l'impiego di sistemi di AI assume caratteristiche peculiari riconducibili alla natura *biologica* dei processi produttivi stessi, alla dipendenza da fattori naturali e ambientali, e alla presenza – come detto – di interessi pubblici essenziali. Tali elementi distintivi, tipici della economia alimentare, rendono l'applicazione dell'AI particolarmente sensibile sotto il profilo giuridico-regolatorio.

1.1. – Nella gestione della filiera produttiva agro-alimentare, l'impiego di sistemi di AI si configura come uno strumento ormai fondamentale per l'elaborazione e l'interpretazione di grandi volumi di dati eterogenei, generati

lungo le diverse fasi della preproduzione, produzione, trasformazione e distribuzione dei prodotti. Tuttavia, l'efficacia di tali sistemi risulta strettamente dipendente dall'affidabilità, dall'integrità e dalla tracciabilità dei dati sui quali essi operano, elementi che assumono particolare rilievo in un settore caratterizzato da elevata complessità organizzativa e da stringenti esigenze di sicurezza, trasparenza e salubrità.

L'integrazione tra sistemi di IA e tecnologie di gestione distribuita dei dati, come la *blockchain*, appare funzionale a garantire una base informativa verificabile e non facilmente alterabile, idonea a sostenere processi decisionali automatizzati lungo l'intera filiera agroalimentare. La *blockchain* assicurando l'immutabilità e la provenienza dei dati, come vedremo, contribuisce a rafforzare la fiducia nei risultati prodotti dai sistemi di IA, mentre questi ultimi consentono di valorizzare i dati tracciati attraverso analisi predittive e strumenti di supporto decisionale. Ne deriva pertanto una relazione di elevata complessità tecnologica, nella quale la *governance* dei dati costituisce il presupposto giuridico e operativo per un impiego affidabile e responsabile dell'IA lungo la catena agroalimentare [2].

I sistemi di IA generativa basati sul c.d. *machine learning* si fondano sull'addebito tramite enormi quantità di dati elaborati mediante algoritmi matematici avanzati. Questi modelli – spesso denominati *foundation models* o *large language model* – analizzano miliardi di dati e di esempi per individuare schemi ricorrenti e generare regole statistiche utili a fissare nuovi contenuti. Questa fase di apprendimento *implica tipicamente la riproduzione e l'estrazione di informazioni da opere preesistenti* [3].

[2] Sul legame tra sistemi di IA e tecnologie bloclchain cfr. J. Bharany-S. Rani, *et. al.*, *A Systematic Review of Blockchain, AI, and Cloud Integration for Secure Digital Ecosystem*, in *International Journal of Networked and Distributed Computing*, 13, 2025, 28; S. Kayikci-T.M. Khoshgoftaar, *Blockchain meets machine learning: a survey*, in *Journal of Big Data*, 11, 2024, 9; G. Palaiokrassas-S. Bouraga-L. Tassiulas, *Machine Learning on Blockchain Data: A Systematic Mapping Study*, in *ARXIV:2403.17081v1*, 2024, 1; A. Aakula-C. Zhang-T. Ahmad, *Leveraging AI AND Blockchain For Strategic Advantage In Digital Transformation,* in *Journal of Artificial Intelligence Research*, vol. 4, 2024, 356; H. Taherdoost, *Blockchain Technology and Artificial Intelligence Together: A Critical Review on Application*, in *Applied Sciences*, 12, 2022, 12948; F. Cheng-H. Wan-H. Cai-G. Cheng, *Machine learning in/for blockchain: Future and challenges*, in *ARXIV:1909.06189v3,* 2020, 1.

[3] Cfr. in questi termini O. Pollicino-G. Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo par-*

Se da una parte è vero che l'integrazione delle due tecnologie – AI e *Blockchain* – sembra costituire lo strumento più idoneo a perseguire gli obiettivi della c.d. transizione digitale delle produzioni agroalimentari europee, d'altra parte va precisato che, dal punto di vista giuridico, le discipline sottese a regolare l'integrazione dei due sistemi presentano non pochi profili di problematicità.

Nelle pagine che seguiranno, invero, si cercherà di dimostrare che dai sistemi di *governance* dei dati come la *blockchain* emergono criticità legate alla eccessiva rigidità delle piattaforme – che da una parte garantiscono massima certezza circa la immutabilità dei dati ma, indubbiamente, non prendono in considerazione la possibilità di modificare *a posteriori* dei dati errati *ab origine* e già registrati sulla relativa piattaforma – e, invece, con riguardo ai sistemi di IA c.d. *generativi* si attribuiscono elementi di debolezza di opposta natura, che generano incertezza giuridica e, conseguentemente, poca fiducia da parte dei c.d. *deployer* ovvero dei consumatori stessi.

Tracciata questa premessa sulla complementarietà dei sistemi di IA con quelli di *governance* di immense quantità di dati, occorre altresì premettere che l'ascesa dell'AI e della relativa disciplina giuridica si inserisce in un contesto normativo complesso e stratificato, ove coesistono norme di diritto privato, pubblico ed europeo tutte concorrenti nel disciplinare la transizione tecnologica, di pari passo con la transizione verso la eco-sostenibilità delle produzioni e delle filiere dei mercati.

Il quadro appare ulteriormente complicato se si considera la totale assenza di norme specifiche per il settore agroalimentare in materia, dovendosi così ricavare la disciplina dalle regole generali dettate in ambito di AI e di gestione distribuita dei dati, seppure siano sempre più numerosi gli spunti giuridico-programmatori (più o meno concreti) a favore di una agricoltura sempre più intelligente e digitalizzata, oltre che sostenibile. Sul piano internazionale si fa riferimento all'obiettivo 2.4 di Agenda 2030 che mira a *implementare pratiche agricole resilienti che aumentino la produttività e la produzione e che contribuiscano a proteggere gli ecosistemi…* [4], pur senza specificare in concreto gli strumenti di conseguimento dello stesso, e, sul piano europeo,

lamentare e vincoli europei, in *Riv. di diritto dei media*, 2, 2025, 393.

[4] Sui contenuti di Agenda 2030 con riferimento al settore agroalimentare cfr. I. Canfora, *Agenda 2030, Agricoltura e alimentazione*, a cura di P. Borghi-I. Canfora-A. Di Lauro-L. Russo, in *Trattato di diritto alimentare italiano e dell'Unione europea*, seconda edizione, Giuffrè editore, 2024, 25.

nell'ambito della Pac 2023/2027, tra gli altri, il riferimento va al regolamento (UE) n. 2115/2021 [5], che ha assunto quale obiettivo generale quello di *promuovere un settore agricolo intelligente, competitivo, resiliente e diversificato che garantisca la sicurezza alimentare a lungo termine* (articolo 5, lett. *a*), e ha inserito tra gli obiettivi specifici della nuova Pac quello di *migliorare l'orientamento al mercato e aumentare la competitività delle aziende agricole, sia a breve che a lungo termine, compresa una maggiore attenzione alla ricerca, alla tecnologia e alla digitalizzazione* (articolo 6, par. 1, lett. *b*) [6].

A questo punto, possiamo concettualmente suddividere in due grandi canali applicativi le possibili ingerenze dei sistemi di AI nel settore della produzione agro-alimentare.

In una prima prospettiva, riconducibile alla c.d. Agricoltura 4.0 (*smart*

[5] Regolamento (UE) n. 2115/2021 del Parlamento europeo e del Consiglio, del 2 dicembre 2021, recante norme sul sostegno ai piani strategici che gli Stati membri devono redigere nell'ambito della politica agricola comune (piani strategici della PAC) e finanziati dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR) e che abroga i regolamenti (UE) n. 1305/2013 e (UE) n. 1307/2013.

[6] A ben guardare, già dai considerando del regolamento (UE) n. 2115/2021 emergono spunti in tal senso, si pensi tra gli altri al considerando 23, ove è sancito che *una PAC più intelligente, moderna e sostenibile deve contemplare la ricerca e l'innovazione, al fine di esplicare il ruolo polifunzionale dell'agricoltura, della silvicoltura e dei sistemi alimentari dell'Unione, investendo nello sviluppo tecnologico e nella digitalizzazione, nonché migliorando la diffusione e l'efficace utilizzo delle tecnologie, segnatamente delle tecnologie digitali, e l'accesso a conoscenze imparziali, solide, pertinenti e nuove intensificando la loro condivisione*; ovvero al considerando 78 ove è disposto che *nel fornire sostegno agli investimenti, gli Stati membri dovrebbero prestare particolare attenzione all'obiettivo trasversale di modernizzare l'agricoltura e le zone rurali promuovendo e condividendo le conoscenze, l'innovazione e la digitalizzazione nell'agricoltura e nelle zone rurali e incoraggiandone l'utilizzo. Il sostegno agli investimenti nell'installazione di tecnologie digitali nell'agricoltura, nella silvicoltura e nelle zone rurali, come gli investimenti nell'agricoltura di precisione, nei piccoli comuni intelligenti, nelle imprese rurali e nelle infrastrutture delle tecnologie dell'informazione e della comunicazione, dovrebbe essere incluso nella descrizione, figurante nei piani strategici della PAC, del contributo di tali piani all'obiettivo trasversale.* Cfr. in argomento I. Canfora, *Politica agricola comune e digitalizzazione del comparto agroalimentare*, in *Quaderni della Riv. dir. alimentare*, 2023, 1, 11. Con riguardo agli spunti più o meno espliciti verso la digitalizzazione delle filiere agricole europee nell'ambito della strategia *Farm to Fork* (Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico sociale europeo e al Comitato delle regioni – Una strategia "Dal produttore al consumatore" per un sistema alimentare equo, sano e rispettoso dell'ambiente,* COM(2020) 381 final, Bruxelles) cfr. S. Rolandi, *Il ruolo attribuito alla digitalizzazione nella strategia Farm to Fork dell'Unione europea, tra riferimenti espliciti e nascosti. Quali interventi legislativi in quattro anni?*, in *Riv. dir. agr.,* 2024, 1, 636.

farming o agricoltura di precisione), l'AI trova diretta applicazione nelle fasi di produzione primaria come strumento avanzato di supporto alle decisioni dell'imprenditore agricolo. Attraverso l'elaborazione automatizzata di dati agronomici, climatici e ambientali, tali sistemi consentono una gestione più accurata (*precisa*) e predittiva delle attività agricole, ottimizzando l'uso di input produttivi come l'acqua, fertilizzanti ed energia [7]. L'impiego di sistemi di IA nell'ambito dell'agricoltura 4.0 si traduce anche nell'utilizzo, direttamente sul campo, di macchinari e dispositivi automatizzati dotati di capacità di riconoscimento e intervento selettivo. Tali sistemi, integrando sensori, visione artificiale e algoritmi di apprendimento automatico, sono in grado di individuare in modo puntuale i fattori di rischio per le colture e di intervenire in maniera *chirurgica*, riducendo o eliminando l'uso indiscriminato di input chimici [8]. In questo senso, le tecnologie di agricoltura 4.0 tendono a sostituirsi, almeno parzialmente, all'attività manuale dell'agricoltore nelle operazioni sul campo, ridefinendo – come accennato in precedenza – il ruolo umano in chiave di supervisione e controllo, con rilevanti implicazioni sia in termini di efficienza produttiva che, soprattutto, di sostenibilità ambientale

[7] In particolare, l'integrazione di algoritmi di *Machine learning* (ML - metodi matematici e informatici che permettono ai computer di imparare dai dati e migliorare le loro prestazioni senza essere programmati passo per passo) nei sistemi IA può incidere notevolmente sulle quattro fasi principali che compongono il ciclo della catena produttiva agricola – pre-produzione, produzione, trasformazione e distribuzione – incidendo sulle modalità di organizzazione e gestione delle attività agricole in chiava tecnologicamente avanzata. In particolare, nella fase di pre-produzione, tali strumenti risultano centrali per la previsione delle rese colturali, la valutazione delle caratteristiche del suolo e la determinazione del fabbisogno irriguo, collocandosi nell'ambito delle pratiche di agricoltura di precisione. Nella fase di produzione, il ML viene impiegato per il rilevamento delle patologie vegetali e per l'analisi predittiva delle condizioni meteorologiche, mentre nella fase di trasformazione esso contribuisce all'ottimizzazione dei processi produttivi e al controllo della qualità e sicurezza alimentare. Nella fase di distribuzione, infine, gli algoritmi di ML assumono rilievo nella gestione dello stoccaggio, nella logistica e nell'analisi dei comportamenti dei consumatori. Cfr. su questo A. Aghababaei-F. Aghababaei-M. Pignitter-M. Hadidi, *Artificial Intelligence in Agro-Food Systems: From Farm to Fork*", in *Foods,* 14(3), 2025, 411, disponibile all'indirizzo web https://doi.org/10.3390/foods14030411; O. Ahumada-J.R. Villalobos, *Application of Planning Models in the Agri-Food Supply Chain: A Review*, in *Eur. J. Oper. Res.*, 1, 2009, 196.

[8] Cfr. S. Wolfert-L. Ge-C. Verdouw-M.J. Bogardt, *Big Data in Smart Farming – A review,* in *Agricultural System*, 153, 2017, 69; Eip-Agri, *Data Revolution: Emerging New Data-driven Business Models in The Agri-food Sector*, Seminar Report, 2016; Id., *Precisione Agriculture. The European Innovation Partnership Agricultural Productivity and Sustainability Focus Group*, Final Report, Bruxelles, 2015.

ed economica [9].

In una seconda prospettiva, di natura prevalentemente giuridico-economica, l'IA (anche in questo caso con il supporto di tecnologie di gestione distribuita dei dati) può essere impiegata lungo le fasi della catena agroalimentare per la gestione dei rapporti tra i diversi attori della filiera e per fini di tracciabilità (avanzata e immediata) dei singoli prodotti agroalimentari. In tale contesto, l'IA consente di analizzare e valorizzare i dati tracciati lungo la filiera al fine di rafforzare l'automazione o il monitoraggio dell'esecuzione delle obbligazioni contrattuali,

[9] Con specifico riferimento alla pre-produzione, numerosi studi evidenziano l'importanza della previsione delle rese colturali quale strumento di supporto alle decisioni agronomiche. Attraverso l'integrazione di dati relativi a input produttivi, nutrienti e fertilizzanti, vengono sviluppati modelli predittivi basati su una pluralità di algoritmi – tra cui reti *bayesiane*, modelli di regressione, *decision tree*, metodi di *clustering*, *deep learning* e reti neurali artificiali – funzionali alla promozione di tecniche di agricoltura intelligente. Cfr. su questo R. Ben Ayed-K. Ennouri-F. Ben Amar-F. Moreau-M.A. Triki-A. Rebai, *Bayesian and Phylogenic Approaches for Studying Relationships among Table Olive Cultivars*, in *Biochem. Genet*., 55, 2017, 300 in cui l'A. dimostra che mediante l'impiego di una rete bayesina è possibile evidenziare l'incidenza della tolleranza colturale (capacità di una coltura di tollerare condizioni avverse) sul contenuto di olio in diverse varietà di olive da tavola (il *Bayesian Network* è un modello matematico e probabilistico che serve a rappresentare e analizzare relazioni di dipendenza tra variabili, anche in presenza di incertezza); cfr. anche D. Elavarasan-D.R. Vincent.-V. Sharma-A.Y. Zomaya-K. Srinivasan, *Forecasting Yield by Integrating Agrarian Factors and Machine Learning Models: A Survey*, in *Comput. Electron. Agric.*, 2018, 155, 257; C. Zhang-J. Liu-J. Shang-H. Cai, *Capability of Crop Water Content for Revealing Variability of Winter Wheat Grain Yield and Soil Moisture under Limited Irrigation*, in *Sci. Total Environ.,* 2018, 631 e 677. Analogamente, diversi algoritmi di IA sono stati applicati all'analisi delle proprietà del suolo, come dimostrano, tra gli altri, negli studi A. Morellos-X.E. Pantazi-D. Moshou-T. Alexandridis-R. Whetton-G. Tziotzios-J. Wiebensohn-R. Bill-A.M. Mouazen, *Machine Learning Based Prediction of Soil Total Nitrogen, Organic Carbon and Moisture Content by Using VIS-NIR Spectroscopy*, in *Biosyst. Eng.*, 2016, 152, 104, e R. Kumar-M.P. Singh-P. Kumar-J.P. Singh, *Crop Selection Method to Maximize Crop Yield Rate Using Machine Learning Technique. In Proceedings of the 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials*, in ICSTM, Avadi, India, 6–8 May 2015, 138. Con riguardo alla gestione/ottimizzazione delle risorse idriche mediante sistemi di AI cfr. S. Choudhary-V. Gaurav-A. Singh-S. Agarwal, *Autonomous Crop Irrigation System Using Artificial Intelligence*, in *Int. J. Eng. Adv. Technol.*, 2019, 8, 46; G. Arvind-V.G. Athira-H. Haripriya-R.A. Rani-S. Aravind, *Automated Irrigation with Advanced Seed Germination and Pest Control.* in *Proceedings of the 2017 IEEE Technological Innovations in ICT for Agriculture and Rural Development*, TIAR, Chennai, India, 7–8 April 2017, 64; J.R.D. Cruz-R.G. Baldovino-A.A. Bandala-E.P. Dadios, *Water Usage Optimization of Smart Farm Automated Irrigation System Using Artificial Neural Network*, in *Proceedings of the 2017 5th International Conference on Information and Communication Technology*, ICoIC7, Melaka, Malaysia, 17–19 May 2017.

nonché di introdurre meccanismi di allocazione/ripartizione del valore economico fondati su parametri oggettivi e facilmente verificabili. Ancora, l'integrazione tra sistemi di IA e *blockchain* rafforza i dispositivi di tracciabilità, controllo e auditabilità dei prodotti, contribuendo in modo significativo a garantire la sicurezza alimentare, la conformità agli standard normativi (compresi quelli contenuti nei disciplinari di qualità) e la trasparenza informativa nei confronti dei consumatori e delle autorità di vigilanza. In tal senso, l'utilizzo congiunto di tali tecnologie si configura non solo come strumento di potenziamento economico della filiera, ma anche come fattore di rafforzamento della fiducia del mercato e di riequilibrio delle relazioni tra gli operatori, coerente con le esigenze di equità, sostenibilità e innovazione che caratterizzano questo settore.

2. – L'Unione europea ha da tempo avviato i lavori per la centralizzazione del flusso digitale di dati incentivando la creazione di "spazi comuni" nel mercato unico europeo, con l'obiettivo di garantire e bilanciare principi quali riservatezza, trasparenza e sicurezza dei dati nel tempo [10]. È indubbio poi che ogni settore del mercato presenta le proprie specificità che richiedono apposite accortezze nella gestione, trasmissione e protezione di alcune categorie di dati piuttosto che altre.

A tal riguardo, nella Comunicazione *Una strategia europea per i dati*, la Commissione ha previsto di sostenere la creazione, nell'elenco dei nove *spazi europei comuni dei dati*, di uno *spazio comune europeo di dati sull'agricoltura, per rafforzare la sostenibilità, il rendimento e la competitività del settore agricolo mediante l'elaborazione e l'analisi di dati di produzione e di altri dati, che consentano un'applicazione precisa e mirata degli approcci di produzione a livello di azienda agricola* [11].

[10] Si fa riferimento ai documenti della Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Verso una florida economia basata sui dati*, COM(2014) 442 final; Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Costruire un'economia dei dati europea*, COM(2017) 9 final; Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Comunicazione verso uno spazio comune europeo dei dati*, COM(2018) 232 final, Bruxelles; Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Una strategia europea per i dati*, COM(2020) 66 final, Beuxelles, 5.

[11] Cfr. nota precedente.

Ancora, il Parlamento europeo con una risoluzione del 25 marzo 2021 [12] (sostenuta da 24 Stati membri che a loro volta hanno firmato una dichiarazione di cooperazione per *Un futuro digitale intelligente e sostenibile per l'agricoltura e le zone rurali europee*) ha nuovamente ribadito che lo spazio dei dati, attualmente in fase di progressiva definizione, è concepito come strumento volto a promuovere l'accesso, la circolazione e il riutilizzo delle informazioni tra agricoltori, imprese, prestatori di servizi e autorità pubbliche, al fine di sostenere l'adozione di pratiche innovative e sostenibili, contenere gli oneri amministrativi e l'impatto ambientale del comparto produttivo, rafforzare le performance economiche e garantire ai consumatori un livello più elevato di trasparenza in ordine alle caratteristiche dei prodotti e alle modalità di produzione [13].

Nel sistema agroalimentare contemporaneo, i dati agricoli — relativi alle pratiche colturali, all'impiego degli input produttivi, alle condizioni climatiche, alle fasi di trasformazione e di circolazione dei prodotti, nonché agli assetti contrattuali, alla ripartizione del valore lungo la filiera e alle informazioni destinate ai consumatori — assumono una valenza giuridica che va ben oltre la loro dimensione meramente tecnica o informativa. Essi costituiscono, infatti, i presupposti indispensabili per l'adempimento di obblighi normativi che incidono direttamente sulla responsabilità degli operatori del settore alimentare, in materia di sicurezza, tracciabilità e informazione lungo la filiera.

In tale prospettiva il regolamento (CE) n. 178/2002 [14], pone i dati relativi a questi aspetti al centro del sistema europeo di sicurezza alimentare: in particolare, l'articolo 17 sancisce la responsabilità primaria degli operatori del settore alimentare e dei mangimi nel garantire la conformità normativa, mentre l'articolo 18 introduce un obbligo generale di rintracciabilità *in tutte le fasi della produzione, della trasformazione e della distribuzione*, imponendo

[12] Cfr. Parlamento europeo, *Risoluzione del Parlamento europeo del 25 marzo 2021 su una strategia europea per i dati* (2020/2217(INI)), par. 39.

[13] Cfr. European Commission, *Commission Staff Working Document on Common European Data Space,* SWD(2024) 21 final, Bruxelles, 18. Cfr. su questo L. Leone, *"Big data e intelligenza artificiale nell'agricoltura europea 4.0: una lettura etico-giuridica"*, in *Riv. dir. agroal.*, 2024, 3, 505.

[14] Regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare. GU L 31 del 1.2.2002.

la capacità di identificare fornitori e destinatari dei prodotti. A ciò si aggiunge l'articolo 19, che obbliga gli operatori a intervenire tempestivamente in caso di alimenti non conformi, presupponendo la disponibilità di informazioni accurate, aggiornate e immediatamente accessibili.

La gestione digitale dei dati mediante tecnologie *blockchain* appare, sotto il profilo funzionale, particolarmente idonea a rafforzare l'effettività degli obblighi giuridici già previsti dal legislatore, in quanto consente di garantire l'integrità, la non alterabilità, la sequenzialità temporale e la verificabilità delle informazioni registrate lungo la filiera agroalimentare. Tuttavia, l'adozione di registri distribuiti solleva rilevanti interrogativi di ordine giuridico, poiché il quadro normativo vigente è stato concepito in un contesto tecnologico profondamente diverso rispetto a quello attuale, e cioè fondato su sistemi centralizzati di gestione del dato [15].

L'elemento di maggiore discontinuità rispetto ai database tradizionali risiede nella natura *decentralizzata* della *blockchain*, che opera, almeno nei modelli più puri (*permissionless*), in assenza di un'autorità centrale o di un soggetto supervisore chiaramente individuabile. Ciò rende giuridicamente problematica l'attribuzione delle responsabilità in caso di inesattezza, incompletezza o mancato aggiornamento delle informazioni, nonostante i dati siano sottoposti a meccanismi di validazione preventiva e, una volta iscritti, siano resi disponibili in forma distribuita e tendenzialmente immutabile [16].

[15] Il meccanismo di aggiornamento del diritto vigente come conseguenza della evoluzione sociale (che nel caso di specie ha riguardato l'era della digitalizzazione delle produzioni industriali e, successivamente, anche di quelle agricole) richiama l'idea di A. Morrone, *L'ambiente nella Costituzione. Premesse di un nuovo "contratto sociale*, in *La riforma costituzionale in materia di tutela dell'ambiente,* Collana AIDA Ambiente, Editoriale Scientifica, Napoli, 2022, 91, in cui l'A. ha definito, in ambito Costituzionale, la c.d. funzione *riflessiva* delle opere di aggiornamento normativo (proprio in quanto riflette il sentire sociale che si è evoluto rispetto al passato), per contrapporla alla c.d. funzione *performativa* delle revisioni normative che, all'opposto, vede il diritto come uno stimolo per l'evoluzione sociale.

[16] Cfr. L. Russo, *L'uso della blockchain nella lotta alle p.c.s. nei contratti di cessione*, in Atti del Convegno *La rilevanza della digitalizzazione per un mercato agroalimentare sostenibile*, a cura di G. Pisciotta Tosini, 2023, 109; P. Gallo, *L'applicazione del sistema blockchain e degli smart contract per la tracciabilità e il controllo della filiera vitivinicola sostenivile: esperienze, criticità e prospettive di sviluppo*, in Atti del convegno *Comunicazione di sostenibilità e blockchain. Strumenti giuridici e prospettive tecnologiche per il settore vitivinicolo*, a cura di G. Pisciotta Tosini, Palermo University Press, 2022, 85; L. Parola-P. Merati- G. Gavotti, *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti,* n. 6, 2018, 681. Cfr. anche G. Sisto, *Blockchain in agrifood supply chain.*

Tali criticità si riflettono sul valore giuridico delle informazioni registrate su piattaforme *blockchain*.

Né il regolamento (UE) 2017/625 sui controlli ufficiali [17] – in particolare, agli articoli 9 e 14, relativi ai poteri di verifica e acquisizione delle informazioni da parte delle autorità competenti – né la normativa settoriale in materia di sicurezza e igiene degli alimenti [18] attribuiscono un riconoscimento normativo espresso alle inscrizioni su registri distribuiti.

Se è vero che la *blockchain* potrebbe assolvere a una funzione probatoria raf-

Achieving traceability and sustainability under the UN 2030 agenda, in *Jour. Of Law, Market & Innovation*, Vol. 4 – Issue 2/2025, 220, in cui l'A. evidenzia che la tecnologia *blockchain* è organizzata in insiemi di dati di dimensione fissa, noti come blocchi. Il collegamento tra i vari blocchi (precedente-successivo) è garantito da una funzione crittografata (*Hash*) che comprime le informazioni in codice alfanumerico univoco. Con la crescita della catena, ogni blocco contiene l'*hash* dei precedenti, creando così una catena immutabile o, per meglio dire, una catena nella quale qualsiasi alterazione renderebbe immediatamente evidente una manomissione. Quanto invece alla registrazione, prima che i dati possano considerarsi registrati in modo immutabile sulla piattaforma *blockchain*, devono essere validati almeno sei blocchi successivi, poiché solo dopo tale soglia qualsiasi alterazione dell'ultimo blocco diventa economicamente irrealizzabile per un eventuale *aggressore*. In altri termini, per quanto non sia matematicamente impossibile che i dati subiscano un'alterazione, i dati immessi in tecnologie *blockchain* possono essere considerati *virtualmente irreversivili*. Nonostante questo *deficit* (meramente potenziale) di immutabilità dei dati, in ogni caso, tutti i blocchi successivi a quello risalente alla manomissione risulterebbero facilmente identificabili.

[17] Regolamento (UE) 2017/625 del Parlamento europeo e del Consiglio, del 15 marzo 2017, relativo ai controlli ufficiali e alle altre attività ufficiali effettuati per garantire l'applicazione della legislazione sugli alimenti e sui mangimi, delle norme sulla salute e sul benessere degli animali, sulla sanità delle piante nonché sui prodotti fitosanitari, recante modifica dei regolamenti (CE) n. 999/2001, (CE) n. 396/2005, (CE) n. 1069/2009, (CE) n. 1107/2009, (UE) n. 1151/2012, (UE) n. 652/2014, (UE) 2016/429 e (UE) 2016/2031 del Parlamento europeo e del Consiglio, dei regolamenti (CE) n. 1/2005 e (CE) n. 1099/2009 del Consiglio e delle direttive 98/58/CE, 1999/74/CE, 2007/43/CE, 2008/119/CE e 2008/120/CE del Consiglio, e che abroga i regolamenti (CE) n. 854/2004 e (CE) n. 882/2004 del Parlamento europeo e del Consiglio, le direttive 89/608/CEE, 89/662/CEE, 90/425/CEE, 91/496/CEE, 96/23/CE, 96/93/CE e 97/78/CE del Consiglio e la decisione 92/438/CEE del Consiglio (regolamento sui controlli ufficiali).

[18] Oltre al regolamento (CE) n. 178/2002 (*General Food Law*), fa riferimento ai regolamenti (CE) n. 852/2004 del Parlamento europeo e del Consiglio, del 29 aprile 2004, sull'igiene dei prodotti alimentari; n. 853/2004 del Parlamento europeo e del Consiglio, del 29 aprile 2004, che stabilisce norme specifiche in materia di igiene per gli alimenti di origine animale; n. 854/2004 del Parlamento europeo e del Consiglio, del 29 aprile 2004, che stabilisce norme minime per l'organizzazione dei controlli ufficiali sui prodotti di origine animale destinati al consumo umano, n. 882/2004 del Parlamento europeo e del Consiglio, del 29 aprile 2004, relativo ai controlli uf-

forzata, consentendo una più agevole ricostruzione delle operazioni compiute lungo la filiera e riducendo le asimmetrie informative tra operatori e autorità pubbliche, tale funzione non può tuttavia operare in modo automatico, in assenza di una disciplina che attribuisca *ex lege* un valore giuridico privilegiato alle registrazioni su *blockchain*. Ne deriva che l'affidabilità di tali strumenti rimane, allo stato, subordinata alle ordinarie regole in materia di prova e alla responsabilità degli operatori del settore alimentare, con il rischio che la *blockchain* si configuri come tecnologia avanzata ma giuridicamente non autosufficiente.

In altri termini, ciò che si vuole dire è che senza un adeguato aggiornamento normativo in ambito di gestione distribuita dei dati, si corre il rischio che *blockchain* si configuri come uno strumento tecnologicamente avanzato ma non indipendente dal punto di vista giuridico, la cui affidabilità rimane subordinata a valutazioni discrezionali delle autorità competenti.

Le criticità si ampliano ulteriormente se si prende in considerazione il più recente quadro normativo europeo in materia di *governance*, accesso e circolazione dei dati, come delineato dal *Data Governance Act* [19] e dal *Data Act* [20], i quali perseguono l'obiettivo di creare un mercato unico dei dati fondato su condizioni di fiducia, equità e controllo giuridico dei flussi informativi, così come si accennava in apertura di questo paragrafo.

Il *Data Governance Act*, in particolare, definisce all'articolo 2 le nozioni chiave di *servizi di intermediazione dei dati* e in generale di *intermediazione dei dati*, e, agli articoli 10, 11 e 12, introduce un complesso di obblighi in capo agli intermediari, tra cui i principi di neutralità, trasparenza, separazione funzionale e assenza di utilizzo dei dati per fini propri.

Tali disposizioni presuppongono l'esistenza di soggetti giuridicamente identificabili, responsabili dell'organizzazione, della gestione e del controllo dei flussi informativi, nonché assoggettabili a obblighi di registrazione, vigilanza e, se del caso, a sanzioni amministrative. Questa impostazione entra in potenziale

ficiali intesi a verificare la conformità alla normativa in materia di mangimi e di alimenti e alle norme sulla salute e sul benessere degli animali.

[19] 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) 2018/1724 (Regolamento sulla governance dei dati).

[20] Regolamento (UE) 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) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

tensione con i modelli *blockchain* caratterizzati da una *governance* distribuita, nei quali le funzioni di validazione, conservazione e messa a disposizione dei dati sono ripartite tra una pluralità di nodi, senza un centro decisionale unitario chiaramente riconducibile alle categorie giuridiche tradizionali [21].

È questo l'esempio dei modelli di *blockchain* c.d. *permissionless*, connotati appunto da accesso aperto e non selettivo alla rete e dalla possibilità, per una pluralità indifferenziata di soggetti, di partecipare ai meccanismi di validazione della transazione; ai quali si contrappongono i modelli di *blockchain* c.d. *permissioned* nei quali l'accesso, nonché i poteri di scrittura e di veridica dei dati, sono riservati a operatori previamente autorizzati, consentendo così un più elevato grado di controllo, di *governance* del sistema e di ripartizione delle responsabilità [22].

È indubbio che l'adozione di sistemi di *blockchain permissioned* consentirebbe di attenuare alcune le criticità legate anche alla disciplina sulla protezione dei dati personali di cui al regolamento (UE) 2016/679 (GDPR) [23], a partire proprio dalla nozione stessa di *titolare del trattamento* prevista ex articolo 4, n. 7, del GDPR [24]. Purtuttavia, tale configurazione solleva non poche questioni in materia di concorrenza sleale, poiché l'accesso selettivo alla rete

[21] Cfr. in argomento M.F. De Tullio, *Intelligenza artificiale, sovranità alimentare e data governance*, in *Biolaw* Journal, 1, 2024, 193; A. Iannuzzi, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi parlamentari e di politica costituzionale*, 209, 2021, 31; M. Veale-F.Z. Borgesius, *Demystifying the Draft EU Data Governance Act*, in *European Law Review*, 22(4), 2021, 97.

[22] Cfr. E. Alston-W. Law-I. Murtazashvili-M. Weiss, *Can permissionless blockchains avoid governance and the law?*, in *Notre Dame Journal on Emerging Technologies*, 4, vol. 2, 2021; R. Van Pelt-S. Jansen-D. Baars-S. Overbeek, *Defining Blockchain Governance: A Framework for Analysis and Comparison*. in *Information Systems Management*, 38(1), 2021. 21; S. Solat-P. Calvez, *Permissioned vs. Permissionless Blockchail: How and Why there is only one right choice*, in *Journal of Software*, 2020, 106.

[23] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 17 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 95/46/CE (regolamento generale sulla protezione dei dati).

[24] «Titolare del trattamento»: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*.

potrebbe certamente tradursi in una barriera all'ingresso per le imprese agroalimentari non ammesse al sistema, con il rischio di determinare forme di esclusione dal mercato, asimmetrie informative e vantaggi competitivi indebiti a favore degli operatori già integrati nella piattaforma. Così, la *blockchain permissioned*, pur rispondendo a esigenze di certezza giuridica e di controllo, può incidere negativamente sulla parità delle condizioni concorrenziali, imponendo al legislatore e alle autorità competenti di valutare attentamente il bilanciamento tra efficienza tecnologica, apertura del mercato e tutela della concorrenza [25].

Analoghe criticità emergono con riferimento al *Data Act*, che rafforza in modo significativo i diritti all'accesso, utilizzo e portabilità dei dati generati dall'uso di prodotti connessi e servizi digitali. In particolare, gli articoli 3 e 4 riconoscono agli utenti il diritto di accedere ai dati e di metterli a disposizione di terzi, mentre l'articolo 5 impone ai detentori dei dati obblighi di condivisione a condizioni eque, ragionevoli e non discriminatorie. Tali previsioni postulano una gestione dinamica, adattabile e reversibile dei flussi informativi, che consenta di modulare nel tempo l'accesso ai dati in funzione dei diritti degli utenti e delle esigenze di riequilibrio contrattuale [26].

Anche questa logica si confronta criticamente con sistemi *blockchain* fondati sull'immutabilità delle registrazioni e sulla difficoltà di modificare, limitare o revocare *ex post* l'accesso ai dati già iscritti nel registro distribuito.

Si aggiunge ai suesposti elementi di vulnerabilità, il conflitto strutturale tra il principio di immutabilità delle registrazioni sulle tecnologie *blockchain* e i diritti alla rettifica e alla cancellazione dei dati personali sanciti dagli arti-

[25] Cfr. Russo, *L'uso della blockchain nella lotta alle p.c.s. nei contratti di cessione*, in Atti del Convegno *La rilevanza della digitalizzazione per un mercato agroalimentare sostenibile*, cit., 109.

[26] Cfr. L. Xu-Z. Li, *Enhancing Systematic Interoperability: Convergences and Mismatches between Web 3.0 and the EU Data Act*, in *2025 International Conference on Future Communications and Networks (FCN)*, Belgrade, Serbia, 18-22 August 2025; L. Olivieri-L. Pasetto-L. Negrini-P. Ferrara, *European Union Data Act and Blockchain Technology: Challenges and New Directions*, in *6th Distributed Ledger Technologies Workshop (DLT2024)*, Torino, 14 – 15 maggio 2024; L. Olivieri-L. Pasetto, *Towards Compliance of Smart Contracts with the European Union Data Act*, in *CEUR Workshop Proceedings*, vol. 3629, 2023, 7; F. Casolari-C. Buttaboni-L. Floridi, *The EU Data Act in context: a legal assessment*, in *International Journal of Law and Information Technology*, Vol. 31, Issue 4, 2023, 399; S. Torregiani, *Il Data Act: una versione europea del Data Nazionalism?*, in *Riv. It. Di informatica e diritto*, 2, 2023, 131.

coli 16 e 17 del GDPR [27], nonché il rispetto dei principi di minimizzazione e limitazione della conservazione di cui all'articolo 5, par. 1, lett. *c*) ed *e*) del GDPR. In particolare, con riguardo a quest'ultimi, secondo il principio di minimizzazione i dati personali devono essere *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati* (lett. *c*), invece il principio di limitazione della conservazione impone che essi siano *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati* (lett. *e*). Anche sotto questo profilo, l'archiviazione permanente tipica delle tecnologie *blockchain*, funzionale anche alla fase di *training* dei sistemi di IA generativi, solleva interrogativi circa la proporzionalità e la durata del trattamento, ma su questo torneremo meglio in seguito [28].

Soluzioni architetturali fondate sulla distinzione tra dati *on-chain* e *off-chain*, unitamente all'applicazione dei principi di *privacy by design* e *by default* ex articolo 25 del GDPR, appaiono comunque idonee a ricondurre l'uso della *blockchain* entro i limiti della disciplina europea, senza sacrificare le esigenze di tracciabilità e affidabilità del dato.

In particolare, la possibilità di integrare la dimensione *off-chain* con la *blockchain* può essere fornita dagli *smart contracrt*, consistenti in sequenze di codice che si auto-eseguono secondo schemi predefiniti e programmati, con l'obiettivo di minimizzare, o addirittura eliminare, l'intervento umano nella creazione delle condizioni contrattuali e nella loro successiva esecuzione, utilizzando il linguaggio binario quale strumento assemblativo di base [29].

[27] In particolare, l'art. 16 GDPR sancisce il «diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo», mentre l'art. 17, par. 1, riconosce all'interessato il «diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo», stabilendo altresì che il titolare abbia l'obbligo di procedere alla cancellazione qualora ricorra una delle condizioni ivi previste.

[28] Par. 3.1

[29] Cfr. E. Adamo-E. Maio-S. Scalzini, *L'utilizzo della blockchain e degli smart contract nel settore industriale dell'afri-food*, ESI editore, Napoli, 2025; Russo, *Blockchain e smart contracts nei contratti della filiera agroalimentare*, a cura di P. BorghiI. Canfora-A. Di Lauro-L. Russo, in *Trattato di diritto alimentare italiano e dell'Unione europea*, cit., 361; E. Troisi, *Blockchain-based Food Supply Chains: the role of Smart Contracts*, in *Europea Journal of privacy law & tecnologies*, special iussue 2023, 139; Sisto, *Blockchain in agrifood supply chain. Achieving traceability and sustainability under the UN 2030 agenda*, cit., 220; M. Di Cillo, *L'applicazione delle tecnologie smart contract*

Alla luce delle considerazioni svolte, emerge come l'implementazione di sistemi avanzati di gestione e tracciabilità dei dati agroalimentari – fondati sull'impiego di tecnologie blockchain e, potenzialmente, di strumenti automatizzati quali gli *smart contract* – presenti indubbie potenzialità in termini di rafforzamento degli obblighi di sicurezza, trasparenza e rintracciabilità lungo la filiera, ma al contempo sollevi criticità giuridiche che l'attuale quadro normativo europeo affronta in modo ancora piuttosto frammentario. Proprio tali tensioni, accentuate dalla crescente integrazione di sistemi di intelligenza artificiale nella raccolta, elaborazione e valorizzazione dei dati agricoli, rendono necessario interrogarsi sul ruolo che il legislatore dell'Unione ha attribuito all'IA quale tecnologia trasversale e ad alto impatto regolatorio: profili che saranno analizzati nei paragrafi successivi attraverso l'esame del Regolamento (UE) 2024/1689 (AI Act) [30] e del suo coordinamento con la disciplina in materia di protezione dei dati personali di cui al GDPR, al fine di valutare se e in che misura tali fonti possano offrire una base giuridica coerente e sostenibile per lo sviluppo di sistemi di tracciabilità agroalimentare digitali, intelligenti e conformi ai diritti fondamentali.

3. – Come già più volte rilevato, tanto i modelli applicativi riconducibili alla c.d. *Agricoltura 4.0* quanto le forme di gestione algoritmica dei rapporti lungo la filiera agroalimentare presuppongono l'impiego di sistemi di intelligenza artificiale, il cui funzionamento risulta intrinsecamente connesso alla raccolta, al trattamento e alla conservazione di ingenti volumi di dati. Si tratta, in larga misura, di dati privati frequentemente conservati in infrastrutture centralizzate e sottoposti alla disciplina in materia di protezione dei dati, nonché di dati provenienti dai settori pubblico, industriale e della ricerca, che costituiscono la base informativa essenziale per i processi di addestramento, apprendimento e decisione automatizzata degli algoritmi.

Tali flussi informativi assumono, pertanto, una funzione basilare nell'architettura dei sistemi di IA, ponendosi quali elementi determinanti

e blockchain al settore agrifood: profili innovativi e criticità, in *Riv. Cammino Diritto*, 11, 2021.

[30] 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) n. 2018/858, (UE) n. 2018/1139 e (UE) n. 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

non soltanto per l'efficienza delle applicazioni tecnologiche nel comparto agricolo, ma anche per la conformità delle stesse ai principi di liceità, trasparenza, proporzionalità e responsabilizzazione che governano il trattamento dei dati e l'uso delle tecnologie digitali nel settore agroalimentare [31].

Il Regolamento (UE) 2024/1689, noto come *Artificial Intelligence Act* [32], rappresenta il primo intervento organico dell'Unione europea volto a disciplinare l'impiego dei sistemi di intelligenza artificiale, seguendo un approccio tendenzialmente unitario per tutti i settori di applicazione e, come vedremo, sostanzialmente incentrato sulla nozione di *rischio* [33].

Come può immaginarsi, il regolamento si è inserito in un contesto giuridico complesso. Esso incide direttamente sulla sfera etica e sociale del diritto unionale [34], in quanto, come abbiamo già detto prima, l'applicazione di sistemi IA ha

[31] Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM(2018) 237 final, Bruxelles.

[32] Cfr. nota 30.

[33] Cfr. tra gli altri U. Ruffolo, *AI Act. La regolamentazione europea dell'intelligenza artificiale*, Le regole dell'informazione, LUISS, 2025; G. Finocchiaro, *Riflessioni sull'AI Act e sul metodo legislativo europeo*, a cura di S. Mannelli, in *L'Europa di fronte alle sfide di un mondo diviso*, Rubbettino Editore, 2025, 87; G. Rugani, *La legge sull'intelligenza artificiale dell'UE come punto di arrivo e di partenza dei processi di co-regolazione*, in *Osservatorio sulle fonti*, 1,2024, 509; C. Casonato-B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal* 2021, 415; M. Kop, *EU Artificial Intelligence Act: The European Approach to AI*, in *Transatlantic Antitrust and IPR Developments*, 2021; B. Towsend, *Decoding the Proposed European Union Artificial Intelligence Act*, in *American Society of International Law (ASIL) Insights*, 2021; M. Veale-F.Z. Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, in *Computer Law Review International*, 2021, 97; W.G. Voss, *AI Act: the European Union's Proposed Framework Regulation for Artificial Intelligence Governance*, in *Journal of Internet Law*, 2021, 7.

[34] Proprio per la delicatezza del tema oggetto di disciplina positiva, con i documenti Commissione europea COM(2018) 237 final, cit., e Comunicazione della Commissione al Parlamento europeo, al Consigli, al Comitato economico sociale europeo e al Comitato delle regioni – Piano coordinato sull'intelligenza artificiale, COM(2018) 795 final, che precedono l'emanazione del AI Act di ben sei anni, la Commissione europea aveva già avviato una profonda riflessione sugli interrogativi giuridici ed etici in materia. Cfr. in argomento Leone, Big data e intelligenza artificiale nell'agricoltura europea 4.0: una lettura etico-giuridica, cit., 527, in cui l'A. sottolinea come già nel 2018 un gruppo di esperti ad alto livello AI, partendo proprio da un approccio basato sui diritti fondamentali, aveva già fissato una serie di principi atti a garantire l'eticità e la robustezza nel settore in termini di sorveglianza, governance dei dati, equità, benessere sociale e accountability. Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, Orientamenti etici per un'IA affidabile, Commissione europea, Bruxelles, 2018. Sulla base degli orientamenti, nel

rivoluzionato il mondo della produzione industriale in generale (industria 4.0) [35] e, conseguentemente, di quella agricola (agricoltura 4.0) [36].

Sono sorti non pochi contrasti dottrinali già con riguardo all'individuazione della definizione univoca di *sistema di IA*, oggi contenuta all'articolo 3, punto 1, dell'*AI Act*, che testualmente recita *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* [37].

In termini generali, il regolamento persegue l'obiettivo di migliorare il funzionamento del mercato interno e di promuovere la diffusione di un'IA *antropocentrica* e *affidabile*, garantendo al contempo la tutela della salute, dei diritti fondamentali, della sicurezza e dell'ambiente (articolo 1). Tale impostazione risulta piuttosto coerente con le prerogative del settore agroalimentare – pur non menzionato espressamente nel testo normativo, se non nel quarto considerando in cui sono individuate le potenzialità competitive dell'utilizzo di IA nelle realtà produttive industrializzate –, settore nel quale, come abbiamo visto, l'IA è sempre più utilizzata per il monitoraggio delle colture, la gestione dei processi produttivi, la previsione dei rischi climatici e sanitari, nonché per

2020 il gruppo di esperti ha pubblicato un'assessment list quale strumento di autovalutazione. Sulle implicazioni giuridiche derivanti dall'applicazione di sistemi algoritmi AI sulla tutela dei diritti umani cfr. Council of Europe, Algorithms and Human Rights – Study on the human right dimensions of automated data processing techniques and possible regulatory implications, Council of Europe study DGI(2017)12 Prepared by the Commettee of experts on Internet intermediaries (MSI-NET), Strasbourg, 2020.

[35] Sulle principali problematiche connesse all'AI cfr. G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Il Mulino, Bologna, 2024; V.V. Cuocci-E.P. Lopis-C. Motti, *La governance nell'era digitale (Atti della summer school 2022)*, Cacucci editore, Bari, 2023; C. Casonato-M. Fasan-S. Penasa, *Diritto e intelligenza artificiale. Sezione monografica*, in *DPCE Online*, 1, 2022; A. D'Aloia, *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2021.

[36] Cfr. P. Gailhofer, *et. al., The role of Artificial Intelligence in the Europea Green Deal*, Study requested by the AIDA Committee, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, European Parliament, Luxemburg, 2021.

[37] Per una ricostruzione del dibattito scientifico sul tema della individuazione di un'adeguata definizione di *Artificial Intelligence* cfr. C. Trincado Castán, *The legal Concept of Artificial Intelligence: the Debate Surrounding The Definition of AI System in the AI act*, in *BioLaw Journal*, 1, 2024, 305; S. Samoili, *et. al.*, *AI Watch. Defining Artificial Intelligence 2.0*, JRC126426, Luxembourg, 2021.

l'ottimizzazione delle filiere e dei sistemi di tracciabilità [38].

La portata trasversale del Regolamento emerge dalla lettera dell'articolo 2, che ne estende l'applicazione non solo ai fornitori e agli utilizzatori di sistemi di IA stabiliti nell'Unione, ma anche ai soggetti extra-UE i cui sistemi producano effetti nel territorio europeo, circostanza frequente nelle catene agroalimentari globalizzate [39].

Particolarmente rilevante è la classificazione dei sistemi di IA in funzione del livello di rischio, prevista agli articoli 5 e 6 del Regolamento. Se da un lato l'articolo 5 vieta le pratiche di IA che comportano un rischio inaccettabile per i diritti fondamentali (*pratiche di IA vietate*), dall'altro, l'articolo 6 individua i c.d. *sistemi di IA ad alto rischio*, rinviando all'Allegato III per l'elencazione dei settori e delle applicazioni interessate. Ed invero, sebbene il comparto agricolo non sia espressamente menzionato quale settore autonomo, numerose applicazioni tipiche dell'agroalimentare – quali i sistemi di valutazione automatizzata della conformità dei prodotti, di gestione delle risorse, di accesso a finanziamenti o assicurazioni agricole – potrebbero rientrare tra i

[38] Il regolamento (UE) 2024/1689, sin dai primi considerando, individua le potenzialità competitive che l'utilizzo di sistemi di IA può apportare alle imprese che ne fanno uso, sui piani economico, sociale, ambientale, etc. In particolare, il considerando (4) sancisce che *l'IA consiste in una famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'IA, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, istruzione e formazione, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi.*

[39] In particolare, ai sensi dell'articolo 2, par. 1 del regolamento (UE) 2024/1689, questo si applica: *a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo; b) ai deployer dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione; c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione; d) agli importatori e ai distributori di sistemi di IA; e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio; f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione; g) alle persone interessate che si trovano nell'Unione.*

sistemi categorizzati *ad alto rischio*, poiché incidono sui diritti economici e sociali degli operatori.

L'articolo 6, paragrafo 1, dell'*AI Act* fissa due condizioni che, se congiuntamente soddisfatte, consentono di considerare il sistema di IA *ad alto rischio*: la prima (lett. *a*) prevede che il sistema di IA sia destinato a essere utilizzato *come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto* [40]*;* la seconda (lett. *b*) che il prodotto, il cui componente di sicurezza a norma della letteta *a*) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia *soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I* [41]. È inoltre sancito al paragrafo 2 del medesimo articolo che, salvo le eccezioni di cui al paragrafo 3 [42], *sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III* [43].

In tali ipotesi, il fornitore è tenuto al rispetto di una serie di ulteriori cautele disciplinate agli articoli 8-27, tra le quali l'adozione di un sistema di gestione dei rischi (inteso come processo interattivo pianificato ed eseguito nel corso dell'intero ciclo vita di un sistema ad alto rischio, che richiede riesami e aggiornamenti costanti) [44], stringenti requisiti relativi alla redazione

[40] *Disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'Allegato I* (par. 1, lett. *a*).

[41] Inoltre, salvo le eccezioni di cui al par. 3, il par. 2 prevede che *oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.*

[42] *In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale.* (…)*Un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.*

[43] I settori indicati nell'Allegato III che, l'articolo 6, par. 2, considera anche *ad alto rischio* sono: *biometria, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso; infrastrutture critiche; istruzione e formazione professionale; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; accesso ai servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; attività di contrasto, nella misura in cui il pertinente diritto dell'Unione o nazionale nel permette l'uso; mitigazione, asilo e gestione del controllo delle frontiere, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso; amministrazione della giustizia e processi democratici.*

[44] In particolare, l'art. 9, par. 2, prevede che il sistema di gestione dei rischi comprende le se-

della *documentazione tecnica* [45], alla *conservazione delle registrazioni* [46], alla *trasparenza e fornitura di informazioni ai deployer* [47], nonché l'introduzione di un sistema di gestione della *qualità* che garantisca il rispetto delle norme del regolamento [48].

Tra le accortezze necessarie per l'utilizzo dei sistemi di IA ad alto rischio, l'articolo 14 prevede inoltre che i fornitori di questi modelli progettino e sviluppino degli strumenti di supervisione umana durante tutto il periodo di utilizzo. La possibile interfaccia uomo-macchina – nell'ottica di una maggio-

guenti fasi: *a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali quando il sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista; b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72; d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi individuati ai sensi della lettera a).*

[45] Al riguardo, l'art. 11 prevede che la documentazione tecnica di un sistema di AI ad alto rischio sia redatta prima della immissione sul mercato della messa in commercio del sistema e che sia tenuta aggiornata nel tempo. *La documentazione tecnica è redatta in modo da dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti di cui alla presente sezione e da fornire alle autorità nazionali competenti e agli organismi notificati, in forma chiara e comprensibile, le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti. Essa contiene almeno gli elementi di cui all'allegato IV. Le PMI, comprese le start-up, possono fornire in modo semplificato gli elementi della documentazione tecnica specificati nell'allegato IV. A tal fine la Commissione definisce un modulo di documentazione tecnica semplificata che risponda alle esigenze delle piccole imprese e delle microimprese. Qualora una PMI, compresa una start-up, decida di fornire in modo semplificato le informazioni richieste nell'allegato IV, utilizza il modulo di cui al presente paragrafo. Gli organismi notificati accettano il modulo ai fini della valutazione della conformità* (par. 2).

[46] I sistemi di IA ad alto rischio consentono dal punto di vista tecnico la registrazione automatica degli eventi per tutta la durata del ciclo vita del sistema. La relativa disciplina è contenuta all'art. 13 del regolamento (UE) 2024/1689.

[47] I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso, in un formato appropriato digitale o non digitale, che comprendono informazioni concise, complete, corrette e chiare, che siano pertinenti, accessibili e comprensibili per i *deployer*. L'art. 13, par. 3, elenca le informazioni che devono essere obbligatoriamente comunicate nelle istruzioni per l'uso: *a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato; b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio [tra cui: i) la finalità prevista; ii) il livello di accuratezza che ci si può attendere, comprese le metriche, di robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza; iii) qualsiasi circostanza nota o prevedibile connessa*

re certezza a tutela della salute, della sicurezza e dei diritti fondamentali che potrebbero essere lesi da un utilizzo e ragionevolmente prevedibile della tecnologia IA – può consistere, ove tecnicamente possibile, in una misura individuata e integrata nel sistema IA dal fornitore prima della sua immissione sul mercato o messa in servizio, ovvero in misure individuate previamente dal fornitore del sistema di IA ad alto rischio e adatte ad essere attuate in una fase successiva (esecutiva) dal *deployer* (articolo 14, paragrafo 3, lett. *a*) e

all'uso del sistema di IA ad alto rischio in conformità della sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali di cui all'articolo 9, paragrafo 2; iv) se del caso, le capacità e caratteristiche tecniche del sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output; v) ove opportuno, le sue prestazioni per quanto riguarda le persone o i gruppi di persone specifici sui quali il sistema è destinato a essere utilizzato; vi) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA ad alto rischio; vii) se del caso, informazioni che consentano ai deployer di interpretare l'output del sistema di IA ad alto rischio e di usarlo in modo opportuno]; c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità; d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA ad alto rischio da parte dei deployer; e) le risorse computazionali e di hardware necessarie, la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura, compresa la relativa frequenza, necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software; f) se del caso, una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio che consente ai deployer di raccogliere, conservare e interpretare correttamente i log in conformità dell'articolo 12.

[48] Il regolamento (UE) 2024/1689 prevede all'art. 17 che il sistema di gestione della qualità sia documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprende almeno gli aspetti seguenti: *a) una strategia per la conformità normativa, compresa la conformità alle procedure di valutazione della conformità e alle procedure per la gestione delle modifiche dei sistemi di IA ad alto rischio; b) le tecniche, le procedure e gli interventi sistematici da utilizzare per la progettazione, il controllo della progettazione e la verifica della progettazione del sistema di IA ad alto rischio; c) le tecniche, le procedure e gli interventi sistematici da utilizzare per lo sviluppo e per il controllo e la garanzia della qualità del sistema di IA ad alto rischio; d) le procedure di esame, prova e convalida da effettuare prima, durante e dopo lo sviluppo del sistema di IA ad alto rischio e la frequenza con cui devono essere effettuate; e) le specifiche tecniche, comprese le norme, da applicare e, qualora le pertinenti norme armonizzate non siano applicate integralmente, o non includano tutti i requisiti pertinenti di cui alla sezione 2, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme a tali requisiti; f) i sistemi e le procedure per la gestione dei dati, compresa l'acquisizione, la raccolta, l'analisi, l'etichettatura, l'archiviazione, la filtrazione, l'estrazione, l'aggregazione, la conservazione dei dati e qualsiasi altra operazione riguardante i dati effettuata prima e ai*

b)) [49].

In contesti come quello agroalimentare, caratterizzati da una forte asimmetria informativa tra gli operatori della filiera poco *informatizzati* (spesso composta da piccoli imprenditori agricoli e da imprese familiari) e i soggetti tecnologicamente più evoluti, la possibilità di comprendere il funzionamento dei sistemi di IA e di intervenire sulle decisioni automatizzate costituisce una garanzia di non poco conto. L'obbligo di assicurare una supervisione umana effettiva mira, infatti, a prevenire decisioni automatizzate opache o discriminatorie da parte dei sistemi di IA, che per loro natura – *high risk* – tendono a incidere sulla sfera individuale e collettiva degli utilizzatori e dei consumatori della relativa filiera.

È pur vero, però, che il regolamento non disciplina in concreto le modalità attraverso le quali il controllo umano debba essere eseguito, ma, in ogni caso, la previsione di una necessaria interazione uomo-macchina testimonia l'intenzione del legislatore di non volere automatizzare *tout court* i processi

fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio; g) il sistema di gestione dei rischi di cui all'articolo 9; h) la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato a norma dell'articolo 72; i) le procedure relative alla segnalazione di un incidente grave a norma dell'articolo 73; j) la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, comprese quelle che forniscono o sostengono l'accesso ai dati, gli organismi notificati, altri operatori, clienti o altre parti interessate; k) i sistemi e le procedure per la conservazione delle registrazioni e di tutte le informazioni e la documentazione pertinenti; l) la gestione delle risorse, comprese le misure relative alla sicurezza dell'approvvigionamento; m) un quadro di responsabilità che definisca le responsabilità della dirigenza e di altro personale per quanto riguarda tutti gli aspetti elencati nel presente paragrafo.

[49] L'art. 14, par. 4, in ogni caso prevede che il sistema di IA ad alto rischio sia fornito al *deployer* in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di: *a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili; d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.*

che si servono di strumenti IA.

Ma detto questo, oltre ai sistemi AI *vietati* e a quelli *ad alto rischio*, *l'AI Act* offre anche ulteriori classificazioni normative per modelli di IA a rischio meno elevato, per le quali prevede la tendenziale libertà di circolazione nel mercato, salvo il rispetto di una serie di obblighi informativi a tutela degli utilizzatori. Si fa riferimento alle previsioni di cui al Capo V del regolamento in parola, che disciplina il funzionamento dei c.d. *modelli di IA per finalità generali* e, nel caso questi presentino capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, ovvero siano ritenuti tali sulla base di una decisione della Commissione (*ex officio* o dietro segnalazione qualificata) [50], il regolamento prevede obblighi rafforzati per i fornitori che utilizzano *modelli di IA per finalità generali* c.d. *con rischio sistemico.*

Quanto ai *modelli di IA per finalità generali* (non affetti da rischi apparentemente eccessivi), l'articolo 53, paragrafo 1, prevede una serie di obblighi informativi in capo ai fornitori di questi modelli, tra i quali: la redazione e il costante aggiornamento della documentazione tecnica del modello [51]; l'elaborazione, l'aggiornamento e la pubblicità delle informazioni e della documentazione per i fornitori di sistemi di IA che intendono integrare il modello di IA per finalità generali nei loro sistemi di IA [52]; l'attuazione di una politica volta ad adempiere al diritto dell'Unione in materia di diritto d'autore e di diritti ad esso collegati [53]; e la redazione e la messa a disposizione del pubblico di una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di IA per finalità generali [54].

[50] Art. 51, par. 1, lett. *a)* e *b)*, regolamento (UE) 2024/1689.

[51] *Compresi il processo di addestramento e prova e i risultati della sua valutazione, che contiene almeno le informazioni di cui all'allegato XI affinché possa essere trasmessa, su richiesta, all'ufficio per l'IA e alle autorità nazionali competenti* (par. 1, lett. *a*).

[52] *Fatta salva la necessità di rispettare e proteggere i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali conformemente al diritto dell'Unione e nazionale, le informazioni e la documentazione:* i fornitori di modelli di IA per finalità generali *i. consentono ai fornitori di sistemi di IA di avere una buona comprensione delle capacità e dei limiti del modello di IA per finalità generali e di adempiere ai loro obblighi a norma del presente regolamento; nonché ii. contengono almeno gli elementi di cui all'allegato XII* (par. 1, lett. *b*).

[53] *E, in particolare, a individuare e rispettare, anche attraverso tecnologie all'avanguardia, una riserva di diritti espressa a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790* (par. 1, lett. *c*).

[54] *secondo un modello fornito dall'ufficio per l'IA* (par. 1, lett. *d*).

Con riguardo, invece, ai c.d. *modelli di IA con rischio sistemico*, dopo aver sancito all'articolo 52, paragrafi 1, 2, 3 e 4, le modalità di segnalazione da parte dei fornitori e di individuazione di queste categorie di modelli da parte della Commissione [55], il legislatore ha previsto al successivo paragrafo 6, in conformità con gli obiettivi di sicurezza e trasparenza del regolamento, che *la Commissione garantisce che sia pubblicato un elenco di modelli di IA per finalità generali con rischio sistemico e lo mantiene aggiornato, fatta salva la necessità di rispettare e proteggere i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali conformemente al diritto dell'Unione e nazionale*.

Inoltre, come già anticipato, l'articolo 55 fissa una serie di ulteriori obblighi cumulativi di informazione da parte dei fornitori, rispetto a quelli precedentemente descritti per i *modelli di IA per finalità generali*, tra i quali: l'effettuazione di una valutazione dei modelli in conformità di protocolli e strumenti standardizzati che rispecchino lo stato dell'arte [56]; la valutazione e l'attenuazione dei possibili rischi a livello unionale, comprese le loro fonti, che possono derivare dallo sviluppo, dall'immissione sul mercato o dall'uso di modelli di IA con rischio sistemico; la tracciabilità e la segnalazione senza

[55] In particolare, l'articolo 52 del regolamento (UE) 2024/1689 prevede al par. 1 che *se un modello di IA per finalità generali soddisfa la condizione di cui all'articolo 51, paragrafo 1, lettera a)* (e cioè che presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento)*, il fornitore pertinente informa la Commissione senza ritardo e in ogni caso entro due settimane dal soddisfacimento di tale requisito o dal momento in cui viene a conoscenza che tale requisito sarà soddisfatto. Tale notifica comprende le informazioni necessarie a dimostrare che il requisito in questione è stato soddisfatto. Se la Commissione viene a conoscenza di un modello di IA per finalità generali che presenta rischi sistemici di cui non è stata informata, può decidere di designarlo come modello con rischio sistemico.* Inoltre, il medesimo fornitore *può presentare, unitamente alla sua notifica, argomentazioni sufficientemente fondate per dimostrare che, in via eccezionale, sebbene soddisfi tale requisito, il modello di IA per finalità generali non presenta, a causa delle sue caratteristiche specifiche, rischi sistemici e non dovrebbe essere pertanto classificato come modello di IA per finalità generali con rischio sistemico* (par. 2). A questo punto *se la Commissione conclude che le argomentazioni presentate a norma del paragrafo 2 non sono sufficientemente fondate e il fornitore in questione non è stato in grado di dimostrare che il modello di IA per finalità generali non presenta, per le sue caratteristiche specifiche, rischi sistemici, essa respinge tali argomentazioni e il modello di IA per finalità generali è considerato un modello di IA per finalità generali con rischio sistemico.*

[56] *Anche svolgendo e documentando il test contraddittorio (adverarial testing) del modello al fine di individuare e attenuare i rischi sistemici* (lett. *a)*.

ritardo indebito all'ufficio per l'IA e, se del caso, alle autorità competenti nazionali delle informazioni pertinenti su incidenti gravi ed eventuali misure correttive per porvi rimedio; garantire un livello adeguato di protezione della cybersicurezza [57].

Un ultimo profilo da analizzare è quello alla ripartizione di responsabilità lungo la catena del valore dell'IA, nel caso in cui dei soggetti terzi rispetto al fornitore iniziale del sistema dovessero apportare delle modifiche strutturali al sistema di IA stesso.

Al riguardo l'articolo 25 prevede che qualsiasi distributore, importatore, *deployer* o altro terzo è considerato fornitore di un sistema di IA ad alto rischio *nelle circostanze seguenti: a) se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo; b) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6; c) se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6.*

Qualora si verificasse una di queste circostanze, il fornitore originario del sistema di IA sarebbe esentato dalla responsabilità *ex* articolo 25, comma 2, per gli avvenimenti successivi, perdendo automaticamente la qualifica di *fornitore* del sistema, purtuttavia permarrebbero obblighi relativi alla stretta cooperazione con i nuovi fornitori e alla messa a disposizione delle informazioni necessarie, nonché a qualsiasi altra forma di assistenza richiesta per l'adempimento degli obblighi di cui all'AI Act.

Anche questi ultimi obblighi possono essere superati da parte del fornito-

[57] L'articolo 55 dell'*AI act* prevede inoltre, al par. 2, che *i fornitori di modelli di IA per finalità generali con rischio sistemico possono basarsi su codici di buone pratiche ai sensi dell'articolo 56 per dimostrare la conformità agli obblighi di cui al paragrafo 1 del presente articolo, fino alla pubblicazione di una norma armonizzata. La conformità alle norme armonizzate europee garantisce ai fornitori la presunzione di conformità nella misura in cui tali norme contemplano tali obblighi. I fornitori di modelli di IA per finalità generali con rischi sistemici che non aderiscono a un codice di buone pratiche approvato o che non si conformano alle norme armonizzate europee devono dimostrare mezzi alternativi adeguati di conformità ai fini della valutazione da parte della Commissione.*

re iniziale tramite una dichiarazione, anteriore alla messa in circolazione del sistema di IA in questione, in cui viene espressamente specificato che quel determinato modello non debba (in ogni caso) essere trasformato in un sistema di IA *ad alto rischio* e, pertanto, il fornitore non sarebbe soggetto *ab origine* all'obbligo di consegnare la documentazione (paragrafo 2).

Sui profili di responsabilità torneremo in seguito, occorre però precisare in questa sede che i rapporti tra il fornitore del sistema di IA e l'utilizzatore dello stesso hanno senza dubbio natura negoziale. È a tutti noto che il contratto costituisce la massima espressione della libertà economico/individuale delle parti, ed invero, salvo casi eccezionali come quello della violazione di norme imperative, il fornitore e l'utilizzatore potrebbero in ogni caso prevedere delle clausole escludenti della responsabilità del fornitore (o viceversa), senza violare la disciplina generale del contratto. Peraltro, un contratto di fornitura di un sistema di IA con un utilizzatore professionista che a sua volta è un imprenditore agricolo, può tranquillamente essere inquadrato quale contratto *business to business* non accedendo, neppure, alla disciplina speciale prevista a tutela dei consumatori nei contratti *business to consumer*.

Da questa brevissima disamina dell'*AI Act* emerge, come detto, una normativa *risk oriented*, incentrata sostanzialmente sulla prevenzione, il monitoraggio e la valutazione dei singoli rischi da parte degli stessi operatori (progettatori, fornitori, *deployer*, etc.). È indubbio, però, che il quadro in esame sia connotato da un certo grado di indeterminatezza, in quanto i sistemi di IA si applicano a un numero indistinto di settori che hanno tutti sbocco sul mercato e, indubbiamente, questa sorta di incertezza giuridica si trasforma in timore da parte degli utilizzatori nel fare pieno affidamento sui sistemi stessi.

La situazione sembra aggravarsi in ambito agroalimentare, poiché, come abbiamo visto, il processo di digitalizzazione del comparto agricolo europeo non riguarda esclusivamente l'evoluzione tecnologica intesa in termini di gestione intelligente delle colture, o dei macchinari per il monitoraggio e la gestione degli allevamenti o dei fondi agricoli, ma riguarda altresì la *digitalizzazione/automatizzazione* dei rapporti di filiera attraverso l'integrazione dei sistemi di IA e delle tecnologie di gestione dei *big data* come la *blockchain*. Digitalizzare (nel senso di *automatizzare*) tutti i rapporti che intercorrono dal campo alla tavola significherebbe affidare ai modelli di IA anche la gestione del flusso di informazioni obbligatorie che viaggiano lungo la catena alimen-

tare fino ai consumatori, e quindi di tutte quelle garanzie giuridiche, etiche e sociali che fondendosi generano il valore di un prodotto alimentare.

Questa operazione, che oggi sembrerebbe costituire una valida prospettiva per il futuro, non risulta ancora in concreto attuabile senza un adeguato aggiornamento normativo settoriale e specifico, idoneo non soltanto a integrare adeguatamene le normative sul riparto di responsabilità nei sistemi di IA che operano unitamente a piattaforme *blockchain* c.d. *pure* (aperte), ma anche a individuare e risolvere le problematiche specifiche del settore alimentare, i cui prodotti sono destinati a essere ingeriti dall'uomo per il proprio sostentamento e che pertanto coinvolge i valori più profondi delle Costituzioni moderne, dalle CDFUE e della CEDU. Come già detto in precedenza, la trasmissione dei dati lungo la catena produttiva agroalimentare dal pre-produttore al consumatore finale assume una valenza giuridica, etica e sociale che va ampiamente oltre la dimensione tecnica tipica dell'informazione.

3.1. – Pur nella consapevolezza che tutt'oggi non esiste una normativa specifica che disciplini nel dettaglio l'uso integrato di sistemi di IA generativa che si servono di piattaforme esterne di gestione dei *big data* come la *blockchain*, è indubbio che l'impiego su larga scala di dati per l'addestramento dei sistemi di intelligenza artificiale generativa solleva rilevanti interrogativi in ordine alla possibile lesione dei diritti esclusivi di riproduzione ed elaborazione delle opere originarie, alla *qualità* e alla attendibilità dei dati sui quali i sistemi intelligenti eseguono le operazioni di *training*, nonché in ordine al discusso riparto delle relative responsabilità.

Con riguardo al primo punto, la disciplina tradizionale del diritto d'autore non era stata concepita per regolare fenomeni di *data mining* massivo di contenuti protetti a fini di addestramento algoritmico, con la conseguenza che tali attività possono astrattamente integrare un illecito in assenza del consenso dei titolari dei diritti secondo la disciplina generale. Ne deriva la necessità di interrogarsi sul confine tra uso lecito e violazione, ossia sul punto oltre il quale l'impiego non autorizzato di dati generati e opere protette, pur funzionale a un processo tecnologicamente innovativo e trasformativo, ecceda i limiti della libera utilizzazione e sfoci nella compressione indebita del diritto di sfruttamento esclusivo. In altri termini, ci si domanda se e in che

modo l'utilizzo non autorizzato di opere protette per addestrare l'IA possa ritenersi lecito anche a seguito del processo di *trasformazione* delle stesse, una volta incamerate, da parte dei sistemi di IA generativi [58].

Sotto il profilo tecnico, la fase di acquisizione dei contenuti protetti avviene frequentemente mediante procedure automatizzate di raccolta e analisi dei dati, quali il *web scraping* e il *text and data mining*, con un'evidente esposizione al rischio di violazione del diritto di riproduzione. A ciò si aggiunge il rischio che il sistema di IA finisca per assimilare e restituire porzioni riconoscibili di opere tutelate o di dati protetti in quanto personali ai sensi del GDPR, generando forme di utilizzo derivato [59]. Tale dinamica impone di tenere distinti l'addestramento algoritmico dall'apprendimento umano: mentre quest'ultimo è mediato da un processo selettivo, soggettivo e interpretativo, il modello computazionale opera attraverso correlazioni statistiche e riproduzioni temporanee di grandi quantità di dati, prive di qualsiasi dimensione percettiva o valutativa. È in questo senso che la dottrina ha individuato il *discrimen* tra uso *espressivo*, tipico dell'essere umano, e uso *non espressivo*, riconducibile all'algoritmo, rendendo giuridicamente improprio il parallelismo tra apprendimento umano e *training* dell'IA generativa [60].

[58] L'attualità e la concretezza del problema conferma nel numero di azioni legali che alcuni colossi dell'informazione stanno promuovendo contro i principali fornitori di IA. Si prenda l'esempio di M.M. Grybaum-R. Mac, *The times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work*, in *The New York Times*, 2023; *Getty Imsges and others v. Stability AI* (2025) EWHC 38 (Ch). In quest'ultimo caso in cui è stata respinta la richiesta deli Attori di ottenere un risarcimento per l'utilizzo non autorizzato di dati protetti per l'addestramento di sistemi AI, in quanto il giudice ha ritenuto il *petitum* eccessivamente generico data l'assenza di una normativa che chiarisca formalmente come deve essere condotto il campionamento e l'estrapolazione delle opere coinvolte. Cfr. Pollicino-Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, cit., 393; G. Giannone Codiglione-M. Bassini, *From private enforcement to public enforcement. Copy- right enforcement in the digital age: a comparative overview*, in *Copyright and Fundamental Rights in the Digital Age*, London, 2020, 216; C. Geiger-V. Iaia, *Generative AI, Digital Constitutionalism and Copyright: Towards a Statutory Remuneration Right Grounded in Fundamental Rights*, in *MediaLaws.it*, 2023.

[59] Cfr. N. Lucchi, *ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems*, in *European Journal of Risk Regulation*, 15, 3, 2024, 602; M.A. Lemley-B. Casey, *Fair Learning*, in *Texas Law Review*, 99, 4, 2021, 743.

[60] Cfr. R. Brauneis, *Copyright and the Training of Human Authors and Generative Machines*, in *SSRN Scholarly Paper, Social Science Research Network*, 2024; G. G. Starr, *Aesthetic experience models human learning*, in *Frontiers in Human Neuroscience*, 17, 2023; M. Sag, *Copyright Safety for*

Una soluzione al problema prospettata a livello comunitario è quella delle c.d. eccezioni di *text and data mining* (TDM) di cui alla direttiva (UE) 2019/790 [61], che sembrano rappresentare il principale strumento di bilanciamento tra tutela dei diritti esclusivi e promozione dell'innovazione. La Direttiva in parola ha introdotto distinti regimi, tra cui uno, di carattere speciale, riservato a enti di ricerca e istituzioni culturali (articolo 3), e uno di portata generale (articolo 4), esteso anche agli operatori commerciali [62]. Se la prima eccezione mira a favorire la ricerca scientifica, essa tuttavia esclude gran parte degli attori privati, limitando le potenzialità di sviluppo tecnologico. L'articolo 4, pur ampliando la platea dei beneficiari, subordina l'operatività dell'eccezione alla facoltà di *opt-out* dei titolari dei diritti, da esercitarsi mediante strumenti leggibili da macchina. In assenza di standard tecnici armonizzati e a fronte di implementazioni nazionali disomogenee, tale meccanismo è stato da alcuni criticato in quanto rischia di generare incertezza sia per i titolari dei diritti sia per gli sviluppatori di sistemi di IA [63]. Infine, come già evidenziato nel precedente paragrafo, l'*AI Act* rafforza gli obblighi di trasparenza e tracciabilità in capo agli sviluppatori, imponendo la documentazione delle fonti dei dati e delle politiche di conformità al diritto d'autore.

Generative AI, in *Houston Law Review*, 61, 2, 2023, 295.

[61] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (*Copyright in the Digital Single Market Directive*, CD- SMD), GUUE L 130, 17.5.2019.

[62] In particolare, l'art. 3, par. 1, della direttiva (UE) 2019/790 sancisce che *gli Stati membri dispongono un'eccezione ai diritti di cui all'articolo 5, lettera a), e all'articolo 7, paragrafo 1, della direttiva 96/9/CE, all'articolo 2 della direttiva 2001/29/CE, e all'articolo 15, paragrafo 1, della presente direttiva per le riproduzioni e le estrazioni effettuate da organismi di ricerca e istituti di tutela del patrimonio culturale ai fini dell'estrazione, per scopi di ricerca scientifica, di testo e di dati da opere o altri materiali cui essi hanno legalmente accesso.* L'art. 4, par. 1, prevede invece che *gli Stati membri dispongono un'eccezione o una limitazione ai diritti di cui all'articolo 5, lettera a), e all'articolo 7, paragrafo 1, della direttiva 96/9/CE, all'articolo 2 della direttiva 2001/29/CE, all'articolo 4, paragrafo 1, lettere a) e b), della direttiva 2009/24/CE e all'articolo 15, paragrafo 1, della presente direttiva per le riproduzioni e le estrazioni effettuate da opere o altri materiali cui si abbia legalmente accesso ai fini dell'estrazione di testo e di dati.*

[63] Cfr. su questo J.P. Quintais, *Generative AI, copyright and the AI Act*, in *Computer Law & Security Review*, 56, 2025; C. Geiger, *et al., Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/EU*, in *SSRN Scholarly Paper, Social Science Research Network*, 2019; T. Margoni-M. Kretschmer, *A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology*, in *GRUR International*, 71, 8, 2022, 685.

Purtuttavia, esso non sembra colmare le lacune strutturali sul piano tecnico e della *governance*, lasciando irrisolte molte delle difficoltà applicative connesse all'effettiva attuazione delle eccezioni di *text and data mining* [64].

Il secondo elemento di problematicità cui si accennava in apertura di questo paragrafo riguarda i rapporti tra la disciplina relativa ai sistemi di IA generativi e la assoluta necessità di assicurare la qualità dei dati e un'opportuna *governance* degli stessi, nelle fasi di apprendimento e di utilizzo dei sistemi di IA (con il supporto di tecnologie di gestione distribuita dei dati). L'obiettivo di garantire un'adeguata qualità dei dati, presupposto essenziale per assicurare l'affidabilità dei sistemi di IA, emerge sin dai considerando dell'*AI Act*, in cui è disposto che sia *gli spazi comuni di dati istituiti dalla Commissione europea*, sia l'agevolazione della *condivisione dei dati tra imprese e con i governi, nell'interesse pubblico*, *saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio ai dati di elevata qualità ai fini di addestramento, convalida e prova dei sistemi di IA* (considerando 68).

L'adeguata gestione dei dati presuppone non solo che essi siano accurati, completi, coerenti e privi di distorsioni, ma anche la consapevolezza che l'analisi di ampie e eterogenee masse informative, pur necessaria per l'addestramento dei sistemi di intelligenza artificiale, accresce il rischio di impiego di dati errati, parziali o non rappresentativi nelle fasi di *training* [65]. In tale prospettiva, il noto principio del *garbage in, garbage out*, ampiamente indagato in dottrina, evidenzia come l'utilizzo di dati di scarsa qualità o caratterizzati da fenomeni di sottorappresentazione possa tradursi in *output* distorti o discriminatori, con ricadute negative tanto sui singoli quanto sulla collettività [66].

Ne discende che né i dati, né gli algoritmi, possono ritenersi *neutrali*, poiché le scelte operate nelle fasi di raccolta, selezione e trattamento incorporano inevitabilmente valori, priorità e asimmetrie informative, con il rischio di generare *filter bubble* e di accentuare dinamiche di esclusione o discriminazione. Da qui la centralità, anche alla luce delle prescrizioni dell'*AI Act*, di

[64] Cfr. per un'analisi sul punto P. Quintais, *Generative AI, copyright and the AI Act*, in *Computer Law & Security Review*, 56, 2025.

[65] Cfr. M.G. Peluso, *Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato*, in *Riv. di diritto dei media*, 2, 2022, 322.

[66] Cfr. per tutti Gallese, *La standardizzazione nell'AI Act*, in *La disciplina dell'intelligenza artificiale*, cit., 305.

procedure strutturate di valutazione dei *bias* [67], audit e documentazione, quali strumenti imprescindibili di *governance* della qualità dei dati.

Al riguardo, in dottrina non si è mancato di sottolineare come l'individuazione e il mantenimento di alti ed efficaci standard relativi al governo dei dati sui quali si basano i sistemi di IA generativi, in linea con le ambizioni dell'*AI Act*, dipenda in larga misura dal ruolo e dai poteri riconosciuti alle Istituzioni nazionali, che saranno chiamate (come si vedrà nel successivo paragrafo, con specifico riferimento all'ordinamento italiano) ad applicare la nuova disciplina europea (si pensi agli organismi interni di certificazione dei sistemi di IA ad alto rischio, le autorità di notifica e le altre autorità che saranno designate a livello nazionale per agevolare l'attuazione dell'*AI Act* nel nostro ordinamento) [68].

Con specifico riferimento alla disciplina contenuta nel GDPR e alla relativa applicazione in ambito di sistemi IA, e in particolare con riguardo al già menzionato principio della *minimizzazione dei dati* di cui all'articolo 5, paragrafo 1, lett *c*) – secondo cui i dati personali devono essere *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati* – risulta di tutta evidenza una incongruenza di fondo con le previsioni dell'*AI Act*. In altri termini, sebbene il GDPR in linea di principio non osti allo sviluppo di applicazioni di intelligenza artificiale e di tecnologie di gestione dei *big data*, pur subordinandole a un bilanciamento tra la tutela dei dati personali e il perseguimento di altri interessi di rilievo sociale ed economico, è indubbio che la disciplina europea in materia di protezione dei dati propenda per il contingentamento dell'utilizzo dei dati personali al fine di massimizzare gli obiettivi di tutela della riservatezza che connotano il GDPR; invece, al contrario, le tecnologie di *machine learning* saranno in grado

[67] Nel contesto dell'IA un *bias* può essere definito come una deviazione non casuale che altera la rappresentazione della realtà all'interno di un *dataset* o di un modello algoritmico, compromettendo l'equità, l'accuratezza e la neutralità delle decisioni automatizzate. Cfr. su K. Mavrogiorgos-A. Kiourtis-A. Mavrogiorgou-A. Menychtas-D. Kyriazis, *Bias in Machine Learning: A Literature Review*, in *Applied Sciences*, 2024; 14, 8860; A. Sinha-D. Sapra-D. Sinwar-V. Singh-G. Raghuwanshi, *Assessing and Mitigating Bias in Artificial Intelligence: A Review*, in *Bentham Science*, vol. 17, 1, 2024; P.S. Varsha, *How can we manage biases in artificial intelligence systems – A systematic literature review*, in *International Journal of Information Management Data Insights*, vol. 3, 1, 2023.

[68] Cfr. in tal senso Leone, *Big data e intelligenza artificiale nell'agricoltura europea 4.0: una lettura etico-giuridica*, cit., 532.

di massimizzare i risultati e altresì di funzionare in maniera più affidabile soltanto attraverso l'analisi di dati in grosse quantità e, come detto, di alta qualità (intesa in termini di veridicità e di indipendenza da altri fattori che ne influenzano l'attendibilità) [69].

Si pensi al valore affidato ai dati nel settore della produzione agro-alimentare che, oltre a quelli relativi alle persone fisiche che entrano in contatto con la catena produttiva (i quali saranno indubbiamente considerati dai *personali* ai sensi del GDPR), anche informazioni proprietarie come formule specifiche per mangimi o fertilizzanti, metodi di coltivazione innovativi, elenchi di clienti o dettagli sui contratti possono essere protetti come segreti commerciali, a condizione che l'azienda adotti misure ragionevoli per mantenerli confidenziali.

È indubbio che questi dati rientrerebbero a pieno nelle categorie dei dati protetti dal GDPR e risponderebbero, pertanto, alle suddette logiche *conservative* non del tutto rispondenti all'impianto del nuovo *AI Act.*

3.2. – A seguito dell'evoluzione giuridica che a sua volta accompagna la c.d. transizione digitale europea, uno degli elementi di maggiore complessità giuridica riguarda storicamente le modalità di riconoscimento e di attribuzione delle responsabilità per i danni generati dell'applicazione di strumenti di IA nei processi produttivi.

La Direttiva (UE) 2024/2853 [70] del Parlamento europeo e del Consiglio, adottata il 23 ottobre 2024 e pubblicata nella Gazzetta ufficiale dell'Unione europea il 18 novembre 2024, inaugura una significativa modernizzazione del regime europeo di responsabilità per danno da prodotti difettosi, ponendo le basi per una disciplina che tenga finalmente conto della digitalizzazione dei prodotti, dell'economia circolare e degli sviluppi tecnologici legati all'intelligenza artificiale (IA) e al software complesso [71].

[69] Cfr. G. Resta, *Cosa c'è di europeo nella proposta di regolamento UE sull'intelligenza artificiale?*, in *Il diritto dell'informazione e dell'informatica*, 2, 2022, 335.

[70] Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio.

[71] Cfr. in argomento A. Fusaro, *Intelligenza artificiale e responsabilità da prodotti difettosi: la direttiva 2024/2853*, in *Nuova giur. comm.*, 2, 2025, 48; T. De Mari Casareto Dal Verme, *La nuova direttiva sulla responsabilità da prodotto difettoso: riflessioni sulla distribuzione del rischio nella*

La nuova disciplina abroga la Direttiva 85/374/CEE [72] e stabilisce un quadro comune che gli Stati membri dovranno recepire entro il 9 dicembre 2026, applicabile ai prodotti immessi sul mercato o messi in servizio successivamente a tale data [73].

Una delle novità più rilevanti riguarda l'estensione della nozione di *prodotto*, che nel nuovo testo è definita quale *ogni bene mobile, anche se integrato in un altro bene mobile o in un bene immobile o interconnesso con questi…*, includendovi pacificamente anche software, file per fabbricazione digitale e componenti digitali, così come qualsiasi elemento integrato o interconnesso con beni materiali che consenta un loro funzionamento o controllo automatizzato (articolo 4).

In tale ambito rientrano senza dubbio i sistemi di IA generativi, anche quando operano attraverso tecnologie decentralizzate come la *blockchain*, ove il software e gli algoritmi costituiscono la componente essenziale del *prodotto* offerto al consumatore o all'utilizzatore finale. Tale inclusione, consente di superare il problema legato alla distinzione, per fini probatori, tra beni fisici che incorporano o che sono interconnessi con software e il software stesso e, inoltre, che gli *stakeholder* della filiera siano soggetti al regime di responsabilità stabilità dalla nuova Direttiva, anche nei casi in cui la responsabilità sorga a causa della manipolazione o della falsificazione dei dati [74].

Il paradigma della responsabilità oggettiva del produttore, già previsto nella precedente disciplina per i danni causati da prodotti difettosi, viene traslato nella nuova Direttiva con riguardo, anche, ai beni digitali e ai sistemi intelligenti, prescindendo dalla prova della colpa e facendo leva, piuttosto, sulla dimostrazione del difetto, del danno e del nesso causale. In caso di prodotti tecnologicamente complessi come quelli basati su IA, la direttiva introduce anche meccanismi di presunzione del difetto o della causalità quando il

filiera digitale, in *Accademia-Elettronico*, 9, 2025, 933; N. Cevolani, *La nuova disciplina europea della responsabilità per danno da prodotti difettosi (dir. 2024/2853/UE)*, in *Nuove leggi civ. comm.*, 2, 2025, 439.

[72] Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi.

[73] Consiglio dell'UE, *L'UE adegua le norme sulla responsabilità per danno da prodotti difettosi all'era digitale e all'economia circolare*, comunicato stampa 746/24, 10 ottobre 2024.

[74] Cfr. in tal senso Sisto, *Blockchain in agrifood supply chain. Achieving traceability and sustainability under the UN 2030 agenda*, cit., 220.

danneggiato si trova ad affrontare difficoltà tecniche e scientifiche eccessive per ottenere prove in proprio possesso (articolo 10). In tali eventualità, il giudice potrebbe presumere il difetto e il nesso causale qualora sia dimostrato che il prodotto non soddisfi gli obblighi di sicurezza previsti o che il danneggiato abbia incontrato *difficoltà eccessive* nel reperire le prove per ragioni tecniche. Tali presunzioni si rivelano cruciali nei contenziosi che coinvolgono sistemi IA di difficile spiegabilità (il cosiddetto *black box effect*), dove la trasparenza degli algoritmi è intrinsecamente limitata.

Un ulteriore elemento di rilievo consiste nell'espansione delle ipotesi di responsabilità post-vendita: la direttiva contempla che i produttori possano essere ritenuti responsabili non soltanto per i difetti originari, ma anche per quelli derivanti da aggiornamenti software, funzionalità di apprendimento automatico (*machine learning*) o vulnerabilità di cybersicurezza emersi dopo l'immissione sul mercato, nonché per modifiche sostanziali apportate al prodotto – circostanze queste di particolare rilievo nel contesto dell'IA generativa e delle sue continue evoluzioni [75].

Dal punto di vista pratico, seppure anche in questo caso non menziona le responsabilità per la gestione di sistemi di AI nelle produzioni agricole, la nuova direttiva assume rilievo in ogni caso: l'adozione crescente di sistemi di IA generativa per l'analisi predittiva delle colture, la gestione di filiere complesse, il monitoraggio della sicurezza alimentare o la tracciabilità digitale –

[75] In particolare, questo principio si evince dall'analisi congiunta del considerando 50 in cui il legislatore europeo riconosce che, nelle tecnologie digitali, il produttore può mantenere un livello di *controllo* sul prodotto anche dopo l'immissione sul mercato, in particolare quando si tratta di software, aggiornamenti, upgrade o algoritmi di *machine learning*; del considerando 51 in cui è stabilito che qualora un prodotto continui a evolvere attraverso aggiornamenti o upgrade software forniti sotto il controllo del produttore, questi elementi devono essere considerati parte integrante del prodotto stesso, ciò implica che qualsiasi difetto o malfunzionamento originatosi da tali aggiornamenti rientra nel regime di responsabilità previsto dalla direttiva, dal considerando 52 che affronta esplicitamente il caso in cui la mancata fornitura di aggiornamenti di sicurezza necessari per affrontare vulnerabilità di cybersicurezza sia di per sé causa di difettosità del prodotto; l'art. 7 che detta i criteri per la determinazione del difetto, richiamando il principio che un prodotto è difettoso se non fornisce il livello di sicurezza che ci si può legittimamente aspettare; e l'art. 11, par. 2, ove è testualmente disposto che *in deroga al paragrafo 1, lettera c), un operatore economico non è esentato dalla responsabilità se il carattere difettoso di un prodotto è dovuto a uno dei seguenti elementi, a condizione che il prodotto sia sotto il controllo del fabbricante: a) un servizio correlato; b) software, compresi aggiornamenti o migliorie; c) la mancanza degli aggiornamenti o delle migliorie del software necessari per mantenere la sicurezza; d) una modifica sostanziale del prodotto.*

spesso supportata da tecnologie *blockchain* per assicurare immutabilità e trasparenza dei dati – rende inevitabile l'emergere di situazioni in cui difetti informatici o algoritmici possano causare danni produttivi, contaminazioni, errori di classificazione o violazioni del diritto dei consumatori. In tali casi, come già osservato, l'orientamento della nuova normativa europea consente al danneggiato di far valere le proprie ragioni senza dover dimostrare la colpa soggettiva dell'operatore economico, ma facendo riferimento al difetto riconosciuto nella catena digitale del prodotto agroalimentare intelligente.

Occorre tuttavia segnalare che, da una parte, l'aggiornamento della materia della responsabilità per danno da prodotto difettoso costituisce un passo necessario per includere i sistemi digitali e l'IA nel novero dei beni coperti da protezione giuridica uniforme, ampliando il concetto di responsabilità oggettiva anche alle tecnologie emergenti, così da evitare vuoti di tutela. D'altra parte, esso mostra i limiti di un regime di responsabilità nato in un'epoca predigitale quando affronta i complessi meccanismi decisionali automatizzati dei modelli di IA generativi, che si evolvono nel tempo attraverso processi di apprendimento continuo e dipendono da catene logiche non sempre immediatamente decifrabili.

La questione di fondo riguarda, pertanto, l'interrogativo circa la compatibilità delle soluzioni civilistiche tradizionali (pur riadattate) con le esigenze di tutela delle vittime di malfunzionamenti di IA: se da un lato il regime oggettivo della direttiva consente una risposta efficace ai danni derivanti da prodotti difettosi, dall'altro esso può risultare insufficiente a coprire i danni consequenziali più sfumati e le specificità causali della IA generativa, come gli errori algoritmici derivanti da *training dataset* distorti, la propagazione di *bias* o le interconnessioni con infrastrutture distribuite di *blockchain,* che rendono difficile l'individuazione di un singolo *difetto* tecnico secondo i parametri tradizionali.

Pur riconoscendo l'importanza del nuovo regime europeo, una rivisitazione più profonda del diritto civile della responsabilità appare forse necessaria per assicurare una protezione piena ed efficace delle vittime di danni causati da sistemi di IA generativi. Tale rivisitazione potrebbe prevedere, ad esempio, un quadro più esplicito sulla responsabilità dei fornitori di modelli generativi AI, regole specifiche sulla causalità algoritmica, nonché l'introduzione di obblighi di trasparenza e *auditing* dei modelli come prerequisito di responsabi-

lità. In assenza di tali strumenti, infatti, l'attuale disciplina rischia di affidarsi a concetti tradizionali – come quello del *difetto tecnico* – che non sempre si conciliano con la natura pervasiva e auto-adattativa dei sistemi di AI avanzati.

In tal contesto, peraltro, si segnala che nel dibattito normativo europeo in materia di AI erano stati avviati i lavori preliminari per l'emanazione di una disciplina specifica della responsabilità civile per l'IA (nota come *AI Liability Directive* – proposta 2022/0303) [76] volta a integrare e armonizzare le regole di responsabilità per danni causati da sistemi di IA in generale, inclusi quelli non classificabili come *prodotti* nel senso tradizionale.

Tuttavia, mentre la Direttiva (UE) 2024/2853 è stata formalmente adottata e pubblicata, i lavori per la proposta di direttiva sulla specifica responsabilità civile per l'uso dell'IA sono stati abbandonati da parte delle Istituzioni europee, a seguito della impossibilità di raggiungere un accordo tra Parlamento e Consiglio che integrasse un compromesso negoziale soddisfacente tra gli Stati membri e i gruppi politici del Parlamento europeo, lasciando così sostanzialmente al diritto interno agli Stati le modalità di recepimento della nuova Direttiva del 2024, senza ulteriori indicazioni specifiche in materia di responsabilità per danno generato da AI.

4. – Volgendo lo sguardo all'ordinamento nazionale, il legislatore italiano ha recentemente adottato la legge 23 settembre 2025, n. 132, recante *Disposizioni e deleghe al Governo in materia di intelligenza artificiale* [77].

L'intervento normativo, entrato in vigore il 10 ottobre 2025, si propone di introdurre principi generali in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e modelli di intelligenza artificiale, promuovendo un utilizzo corretto, trasparente e responsabile dell'IA in una prospettiva antropocentrica, nonché di garantire un'adeguata vigilanza sui rischi economici e sociali e sugli impatti sui diritti fondamentali, in coerenza

[76] COM (2022) 496: Proposal for a Directive of the european Parliament and the Council adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). Procedure 2022/0303/COD.

[77] G.U. n. 223 del 25/09/2025.

con il regolamento (UE) 2024/1689 (*AI Act*) [78].

Dal punto di vista della tecnica legislativa, il legislatore nazionale introduce delle norme di principio per specifici settori in cui l'applicazione di sistemi di IA sembra avere maggiormente preso campo (Capo II) [79] – non sono previste norme *ad hoc* per il settore agroalimentare –, designa le Autorità nazionali per l'intelligenza artificiale [80], e delega, al contempo, al Governo l'emanazione di decreti legislativi (nella maggior parte dei casi entro dodici mesi dall'emanazione della legge) sia in specifiche materie già individuate negli articoli della legge 132/2025 (come quello relativo alle disposizioni in materia di trattamento di dati personali [81]) sia, in generale, in ambiti non espressamente disciplinati, in materia di *dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale* (articoli 16 e 24).

[78] Per un quadro generale sulle novità introdotte dalla legge 23 settembre 2025, n. 132, cfr. A. Contaldo-G. T. Elmi-C. Cavaceppi-S. Marchiafava, *Intelligenza Artificiale. Legge 23 settembre 2025, n. 132. Il nuovo scenario giuridico italiano*, in *Nuove Leggi nuovo Diritto*, diretta da G. Cassano-G. Spangher, Pacini Giuridica editore, Pisa, 2025; V. Franceschelli-A. Sirotti Gaudenzi, *La legge italiana sull'Intelligenza Artificiale. Commento alla Legge 23 settembre 2025, n. 132*, in *I prontuari giuridici*, diretta da A. Sirotti Gaudenzi, Maggioli editore, 2025; E. Innocenti-M. Lai, *Brevi note sulla legge n. 132/2025 in materia di intelligenza artificiale*, in Centro Studi formazione Cisl, Saggi e Articoli, 4 novembre 2025; B. Fragasso, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura*, in *Sistema Penale*, 10, 2025, 157.

[79] In particolare, la l. n. 132/2025 detta al Capo II disposizioni di settore relative all'uso dell'IA in ambito sanitario e di disabilità (artt. 7 e 8); di trattamento dei dati personali (art. 9); di fascicolo sanitario elettronico, sistemi di sorveglianza nel sistema sanitario e governo della sanità digitale (art. 10); di lavoro (artt. 11 e 12); di professioni intellettuali (art. 13); nella PA (art. 14); nell'attività giudiziaria (art. 15).

[80] In particolare, l'art. 20 della l. n. 132/2025 sancisce al par. 1 che *al fine di garantire l'applicazione e l'attuazione della normativa nazionale e dell'Unione europea in materia di intelligenza artificiale, l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) sono designate quali Autorita' nazionali per l'intelligenza artificiale, ferma restando l'attribuzione alla Banca d'Italia, alla CONSOB e all'IVASS del ruolo di autorita' di vigilanza del mercato ai sensi e secondo quanto previsto dall'articolo 74, paragrafo 6, del regolamento (UE) 2024/1689.*

[81] Il riferimento va all'art. 9 della l. n. 132/2025 ove è disposto che *il trattamento dei dati personali anche particolari come definiti dall'articolo 9 del regolamento (UE) 2016/679, con il massimo delle modalità semplificate consentite dal predetto regolamento per finalità di ricerca e sperimentazione anche tramite sistemi di intelligenza artificiale e machine learning, inclusi la costituzione e l'utilizzo di spazi speciali di sperimentazione a fini di ricerca, anche mediante l'uso secondario dei dati personali, è disciplinato con decreto del Ministro della salute da emanare entro centoventi giorni dalla data di entrata in vigore della presente legge, sentiti il Garante per la protezione dei dati personali, gli enti di ricerca, i presidi sanitari nonché le autorità e gli operatori del settore.*

Proprio quest'ultimo aspetto sembra costituire una prospettiva percorribile in futuro per l'introduzione di norme specifiche che riguardino l'applicazione di sistemi di IA nel settore agroalimentare, ma al contempo la norma è stata oggetto di analisi critiche in dottrina [82].

Innanzitutto, l'articolo 16, paragrafo 1, delega al governo l'emanazione di decreti legislativi *per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi* di IA. Soprattutto in una materia in corso di definizione come quella relativa all'IA, lo strumento della legislazione delegata assicura senz'altro un certo grado di flessibilità operativa ma, allo stesso tempo, si presta a utilizzi impropri e talvolta forzati, se visto sotto il profilo della organicità della materia oggetto di normazione [83].

In altri termini, il reiterato ricorso a decreti legislativi integrativi potrebbe generare effetti distorsivi, estendendo *de facto* l'ambito della delega e, pertanto, rischiando di dare vita a una legislazione stratificata (*per fasi*) che poco rispecchia l'idea del legislatore del 2025, oltre che fioriera di profili di incostituzionalità [84]. Al contrario, la nozione di *disciplina organica* di cui all'articolo 16, paragrafo 1, della legge 132/2025 impone la costruzione di un sistema normativo *coerente, strutturato e fondato su una visione unitaria della materia*, così come è già accaduto in ambito di regolazione della *privacy* [85].

[82] Cfr. Pollicino-Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, cit., 393.

[83] Sui problemi legati ai decreti legislativi integrativi e correttivi cfr. L. Gori, *Dalla «fonte» decreto legislativo integrativo e correttivo al «fine» di integrazione e correzione (tramite una pluralità di fonti)*, in *Osservatorio sulle fonti*, 2, 2019; M. Ruotolo, *I limiti della legislazione delegata integrativa e correttiva*, in *Aa.Vv., La delega legislativa*. Atti del seminario svoltosi in Roma Palazzo della Consulta, 24 ottobre 2008; M. Cartabia, *L'effettività come presupposto e vittima dei decreti legislativi "integrativi e correttivi*, a cura di A. Bardusco-F. Pizzetti, in *L'effettività tra sistema delle fonti e controlli. Alcuni casi emblematici*, Giuffrè editore, Milano, 1998; N. Lupo, *Deleghe e decreti legislativi correttivi: esperienze, problemi, prospettive*, Giuffrè editore, Milano, 1996.

[84] Cfr. G. Marchetti, *Riflessioni su alcuni aspetti problematici della delegazione legislativa. In particolare: la "sistemazione" normativa tramite delega, il ruolo del Parlamento nell'adozione dei decreti delegati e il ricorso ai decreti integrativi e correttivi*, in *Osservatorio sulle fonti*, 2, 2019, 1; M. Bassini, *Le tecnologie avanzano, le norme passano ma le costituzioni rimangono*, in *dirittocomparati.it*, 3 novembre 2014.

[85] Cfr. in questi termini Pollicino-Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parla-*

Ancora il paragrafo 1 dell'articolo 16 impone al legislatore delegato il vincolo di non introdurre *obblighi ulteriori* rispetto a quelli stabiliti nell'AI Act [86]. Questa limitazione va letta unitamente alla previsione di cui al paragrafo 3, lett. *a*, secondo la quale, come anticipato, il Governo, nell'esercizio della delega legislativa di cui al paragrafo 1, individua *ipotesi per le quali appare necessario dettare il regime giuridico dell'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale, nonché i diritti e gli obblighi gravanti sulla parte che intenda procedere al suddetto utilizzo*. Inoltre, la lett. *b* del paragrafo 3 impone che il Governo preveda *strumenti di tutela, di carattere risarcitorio o inibitorio, e* individui *un apparato sanzionatorio per il caso di violazione delle disposizioni introdotte ai sensi della lettera a.*

mentare e vincoli europei, cit., 395, in cui gli AA. evidenziano che l'esperienza normativa in ambito di *privacy*, culminata nel d.lgs. 166/2003 è emblematica di una *transizione da un approccio frammentario a uno sistemico*. Invero, l'iniziale pluralità di fonti (l. n. 675/1996 e l. n. 675/1996, normative settoriali, disposizioni regolamentari) generava incertezza e disomogeneità nella relativa disciplina, che restava priva di un centro di coordinamento concettuale e normativo. Soltanto a seguito della delega contenuta nella l. n. 127/2001, il Governo fu incaricato di predisporre una disciplina organica, che razionalizzasse le fonti e, altresì, rafforzasse le autonomie istituzionali e adeguasse la normativa interna a quella europea, anticipando di fatto l'armonizzazione successiva ad opera del GDPR. Cfr. anche G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Giuffrè editore, Milano, 1997; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, vol. 2, Giappichelli editore, Torino, 2016.

[86] In tal senso si pone anche il considerando (3) del regolamento (UE) 2024/1689 che testualmente prevede *i sistemi di IA possono essere facilmente impiegati in un'ampia gamma di settori dell'economia e in molte parti della società, anche a livello transfrontaliero, e possono facilmente circolare in tutta l'Unione. Alcuni Stati membri hanno già preso in esame l'adozione di regole nazionali per garantire che l'IA sia affidabile e sicura e sia sviluppata e utilizzata nel rispetto degli obblighi in materia di diritti fondamentali. Normative nazionali divergenti possono determinare una frammentazione del mercato interno e diminuire la certezza del diritto per gli operatori che sviluppano, importano o utilizzano sistemi di IA. È pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione al fine di conseguire un'IA affidabile, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione, l'innovazione, la diffusione e l'adozione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno, stabilendo obblighi uniformi per gli operatori e garantendo la tutela uniforme dei motivi imperativi di interesse pubblico e dei diritti delle persone in tutto il mercato interno, sulla base dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE)*. Cfr. sul punto M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in *Quaderni AISDUE - Rivista quadrimestrale*, 2, 2024, numero speciale *La nuova disciplina UE sull'intelligenza artificiale*.

Tale impostazione risulta di difficile interpretazione in una fase ancora prodromica all'emanazione delle relative norme settoriali.

Occorre altresì considerare che, seppur non espressamente richiamato, certamente l'Allegato III dell'*AI Act* (che elenca le categorie di sistemi di IA maggiormente pericolose per la salute, la sicurezza e i diritti fondamentali) potrebbe costituire un punto di partenza per il legislatore delegato italiano. A tal riguardo, è interessante considerare che la Commissione europea, come già evidenziato in precedenza, si è normativamente impegnata ad aggiornare periodicamente le pratiche *ad alto rischio* contenute nell'Allegato III [87], invece, con riguardo alla legislazione delegata di cui si discute, oltre al problema legato ampiezza delle relative deleghe, non risultano chiare le modalità di aggiornamento della disciplina sulla base della evoluzione delle necessità di regolazione dei sistemi di IA [88].

È indubbio che l'impianto *risk oriented* che connota l'IA, costituisca un limite all'agire del legislatore delegato, in quanto non potrà prescindere dalle classificazioni dei sistemi IA sulla base della loro pericolosità nella relativa utilizzazione anche nella individuazione dei settori da disciplinare in forma prioritaria rispetto agli altri.

A tal riguardo, l'impostazione dell'*AI Act* differisce ampiamente rispetto a quella prevista dal GDPR. Invero, l'approccio *bottom-up* che connota il regolamento sulla protezione dei dati personali rinvia sostanzialmente al titolare del trattamento la responsabilità di valutare l'impatto delle operazioni di trattamento sui diritti alla riservatezza e alla protezione dei dati personali dell'interessato, al contrario – come più volte detto – l'*AI Act* adotta una logica *top-down*, basata cioè sulla classificazione preventiva e centralizzata dei

[87] L'art. 7, par.1, dell'*Ai Act* prevede che *alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato III aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati nell'allegato III; b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali, e tale rischio è equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III.*

[88] Cfr. in tal senso . Pollicino-Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, cit., 393; O. Pollicino, *Regolazione e innovazione tecnologica nell'ordinamento della rete*, in *Riv. AIC*, 2, 2025, 129.

sistemi di IA in base ai livelli di rischio individuati dal legislatore europeo [89]. Il legislatore nazionale, nell'applicazione della delega contenuta nella legge n. 132/2025 non potrà tralasciare la struttura *risk oriented* del nuovo impianto normativo.

Infine, l'articolo 24 della legge n. 132/2025, in coerenza con quanto previsto all'articolo 16, fissa i principi sui quali l'attività del legislatore delegato dovrà attenersi e, in particolare, con riguardo ai profili legati alla responsabilità civile, il paragrafo 5, lett. *d*, dispone che il Governo nell'esercizio della delega preveda, *nei casi di responsabilità civile, strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal regolamento (UE) 2024/1689.*

5. – Alla luce dell'analisi condotta sulle fonti europee e nazionali in materia di Intelligenza artificiale e sulle problematiche connesse all'impiego di sistemi di IA nelle sue applicazioni, può ritenersi che l'attuale quadro normativo non osti, seppure entro limiti ben definiti, alla progettazione e alla implementazione di sistemi avanzati di tracciabilità dei prodotti agroalimentari, fondati sull'integrazione tra intelligenza artificiale, tecnologie di gestione distribuita dei dati e strumenti di automazione contrattuale.

Come evidenziato infatti, dal punto di vista tecnico, la combinazione tra sistemi di IA (anche di tipo generativo) e infrastrutture *blockchain* appare uno strumento più che adatto a sostenere modelli avanzati di tracciamento lungo l'intera filiera produttiva, idonei a identificare con estrema precisione e velocità non soltanto i singoli lotti, ma perfino i singoli prodotti (o i relativi ingredienti), al fine di ripercorrerne accuratamente le fasi della produzione, rafforzando la trasparenza, l'affidabilità e l'immutabilità delle informazioni relative ai prodotti agroalimentari, e integrando in maniera più incisiva che mai gli obiettivi generali del regolamento n. 178/2002.

[89] Cfr. su questo O. Pollicino-F. Paolucci, *Regolare l'intelligenza artificiale: la lunga via dei diritti fondamentali"*, in *La disciplina dell'intelligenza artificiale*, a cura di O. Pollicino - F. Donati - G. Finocchiaro - F. Paolucci, Giuffrè editore, Milano, 2025, 26; G. De Gregorio, P. Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 59, 2, 2022, 473 s.; G. Finocchiaro, *Intelligenza artificiale. Quali Regole*, Il Mulino editore, Bologna, 2024.

Il Regolamento (UE) 2024/1689 (*AI Act*), pur non disciplinando espressamente la tracciabilità di filiera, fornisce un insieme di principi e requisiti – in termini di gestione del rischio, qualità dei dati, trasparenza e supervisione umana – che risultano compatibili con l'impiego di sistemi di IA a supporto della raccolta, dell'elaborazione e dell'interpretazione dei dati agroalimentari. Tali requisiti, letti in combinazione con il GDPR, impongono una progettazione dei sistemi di tracciabilità orientata al rispetto dei principi di liceità, minimizzazione e sicurezza dei dati, soprattutto laddove vengano trattate informazioni riferibili ad operatori economici o a persone fisiche coinvolte nella filiera.

In questo contesto, la *blockchain* si configura non tanto come uno strumento alternativo, quanto come un elemento complementare all'IA, in grado di garantire l'integrità e la non modificabilità delle informazioni registrate, mentre i sistemi di IA possono svolgere funzioni di analisi predittiva, rilevazione di anomalie, supporto alle decisioni e generazione automatizzata di documentazione di filiera. L'eventuale utilizzo di *smart contract* può ulteriormente rafforzare il sistema, consentendo l'automazione di obblighi informativi, controlli di conformità e meccanismi di allerta in caso di deviazioni dagli standard normativi o qualitativi.

Pertanto, l'integrazione tra sistemi di IA e tecnologie *blockchain* al fine di costituire dei modelli integrati e centralizzati di tracciabilità alimentare sembra costituire un valido strumento informatico per raggiungere gli obiettivi di sicurezza propri del regolamento n. 178/2002 in una prospettiva di innovazione tecnologica responsabile. Tuttavia, si rende assolutamente necessario un intervento normativo che prenda in considerazione, nello specifico, gli aspetti legati alla tracciabilità dei prodotti, che chiarisca i profili di responsabilità, di interoperabilità e standardizzazione, affinché la tracciabilità digitale possa divenire uno strumento effettivo, prioritario e diffuso al servizio della filiera agroalimentare e della tutela dei consumatori.

Abstract

Il lavoro analizza i principali profili giuridici connessi all'impiego dell'intelligenza artificiale nei sistemi di tracciabilità digitale dei prodotti agroalimentari, con particolare attenzione all'integrazione tra tecnologie di IA e strumenti di gestione distribuita dei dati, quali la blockchain. Muovendo dall'esame del quadro normativo europeo e nazionale, il contributo mette in luce le criticità relative alla governance dei dati, alla qualificazione dei sistemi di IA, ai profili di responsabilità civile e alla compatibilità di tali tecnologie con i principi di sicurezza e tracciabilità alimentare trasparenza e tutela dei diritti fondamentali..

The paper examines the main legal issues related to the use of artificial intelligence in digital traceability systems for agri-food products, with particular attention to the integration of AI technologies and distributed data management tools such as blockchain. Building on an analysis of the European and national regulatory frameworks, the contribution highlights the critical aspects concerning data governance, the classification of AI systems, civil liability issues, and the compatibility of these technologies with the principles of food safety and traceability, transparency, and the protection of fundamental rights.