LUISS

Dipartimento
di Giurisprudenza

Dottorato in Diritto e Impresa

Ciclo XXXVII

Il ruolo della responsabilità civile nella Governance dell'Intelligenza Artificiale

Raffaele Fabozzi

RELATORE

Francesco Di Ciommo

CORRELATORE

Camilla Scarpellino

CANDIDATO

Anno Accademico 2024/2025

Indice

Abstract

L'evoluzione tecnologica ha trovato nell'Intelligenza Artificiale (IA) la sua massima espressione, poiché consente l'automazione completa di molte attività umane. Oggi la società affida alla totale gestione della tecnologia, mansioni che richiedevano inderogabilmente l'attenzione e la logica umana, come guidare un'auto, diagnosticare un malore o stipulare un contratto. L'innovazione in questione è estremamente utile per incrementare la produttività e la competitività, ma deve essere regolata. Si osservi infatti come tutte queste attività non siano solo tecnicamente complesse, ma anche giuridicamente rilevanti.

Pertanto, il presente studio si propone di analizzare uno dei profili di frizione tra i nuovi software e l'attuale contesto normativo. In particolare, si analizza la divergenza tra l'attuale sistema della responsabilità civile e il cd. danno da algoritmo, nota in letteratura con il nome "liability gap". Il gap si registra a causa della crescente autonomia dei sistemi di IA che non consente l'applicazione dei tradizionali principi di responsabilità civile. La capacità di elaborare decisioni in modo autonomo e privo di controllo umano mal si adatta ai criteri di imputazione della colpa e del nesso causale. Pertanto, viene analizzato il quadro normativo attuale sulla responsabilità civile, che ormai contempla forme di tutela multilivello, dalla direttiva 85/374/CEE sulla responsabilità per danno da prodotti difettosi, alle fattispecie di responsabilità presunta previste dal codice civile. Quindi vengono valutate le proposte di regolazione della responsabilità civile dei sistemi di IA avanzate dalla Commissione UE, descrivendone struttura ed effetti. Infine, la tesi presenta soluzioni alternative ai canonici meccanismi di compensazione del danno. Scopo della ricerca è l'elaborazione di uno schema che suggerisca policy utili ad eliminare il gap di responsabilità e allochino i costi della tecnologia in modo efficiente e perequativo.

Abstract

Over the past century, technological advancements have culminated in the rise of Artificial Intelligence (AI) systems, enabling the automation of numerous tasks that once required human reasoning and attention. Today, sophisticated AI algorithms handle complex activities such as autonomous driving, medical diagnosis, contract drafting, and more. While these technologies greatly enhance productivity and competitiveness through rapid data analysis and decision-making, their growing influence, particularly in high-risk areas, necessitates proper regulation.

This thesis examines the tension between the rapid expansion of AI and the current regulatory frameworks, focusing on the gap between traditional tort liability systems and the challenges posed by the "algorithmic harm", i.e. the so-called "liability gap." Conventional civil liability principles struggle to address the increasing autonomy of AI, due to their ability to make independent decisions without human intervention, which complicates the assignment of fault and causality. The research explores the existing regulatory landscape governing civil liability, with particular focus on the multi-level legal protections in place. At the European level, it analyzes the Directive 85/374/EEC on liability for defective products, alongside national regulations regarding presumed liability in civil codes. The study also evaluates the European Commission's proposals for AI-specific civil liability regulations, discussing their framework and potential impact. Ultimately, the thesis presents alternative solutions to traditional compensation mechanisms, with the aim of developing a policy framework that closes the liability gap. The goal is to allocate the costs and risks of AI technology in a manner that is both efficient and equitable.

Introduzione

I sistemi di Intelligenza Artificiale (IA) hanno animato il dibattito pubblico europeo degli ultimi anni. L'Europa, con l'emanazione dell'Artificial Intelligence Act (AI Act) nell'agosto 2024[1], diviene la prima giurisdizione a fornire un quadro vincolante di governance per l'IA. L'intervento è apparso necessario a causa della diffusione massiva di questi software. Ormai piattaforme e motori di ricerca utilizzano algoritmi di deep learning e machine learning e, con loro, anche i servizi digitali e i prodotti IoT sono divenuti autonomi e intelligenti. L'autoapprendimento è la qualità che rende rivoluzionaria questa tecnologia, che ambisce a sostituire l'uomo nelle mansioni cognitive. Grazie a queste funzioni, i software oggi sono in grado di elaborare decisioni in poco tempo ed in assenza di supervisione. In base al loro livello di autonomia possono decidere come soddisfare ed eseguire un ordine, oppure suggerire all'utente una gamma di soluzioni tra le quali scegliere. In questo modo i software di IA oggi guidano auto, consigliano diagnosi e terapie, stilano la graduatoria in un concorso, stipulano un contratto etc. Come si può osservare, le attività appena elencate rappresentano tutte azioni e prestazioni giuridicamente rilevanti, contrassegnate da una certa complessità, e soprattutto, capaci di ledere diritti soggettivi di terze parti.

Gli incidenti causati da sistemi di intelligenza artificiale evidenziano sin da ora un vuoto normativo, dovuto all'inadeguatezza delle attuali norme sulla responsabilità, tradizionalmente fondate sui presupposti del controllo e della gestione del rischio. Tuttavia, l'autoapprendimento e l'autonomia del software riducono, o elidono completamente, il controllo umano sul sistema, creando così un cortocircuito nei tradizionali schemi di responsabilità. D'altronde è proprio l'autonomia, con la quale l'algoritmo svolge i propri compiti, ad accrescere la sua pericolosità, poiché limita le possibilità per l'uomo di intervenire, per evitare l'evento lesivo. Venuto meno il controllo sul processo dell'algoritmo, risultano di difficile applicazione anche i criteri di evitabilità dell'evento, negligenza e rimproverabilità; elementi fondamentali per la struttura della

[1] 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), disponibile al link: https://eur-lex.europa.eu/legal-content/MT/TXT/?uri=CELEX:32024R1689 ;

responsabilità civile. Ed è per questo che «autonomous systems present tort law with unique challenges to overcome»[2].

Queste considerazioni hanno mosso il Parlamento europeo, già nel 2016, ad interrogarsi sulla tenuta del quadro normativo europeo e nazionale, rispetto alle novità introdotte dall'IA, incaricando la Commissione di «esplorare, esaminare e valutare, nell'ambito della valutazione d'impatto del suo futuro strumento legislativo, le implicazioni di tutte le soluzioni giuridiche possibili»[3] per rispondere ai danni arrecati dai robot.

La Commissione europea in effetti interviene, il 28 settembre del 2022, pubblicando due proposte di direttiva sulla responsabilità da algoritmo. La prima, denominata Product Liability Directive (PLD), intende riformare la direttiva 85/374/CEE sulla responsabilità da prodotto difettoso; mentre la seconda, AI Liability Directive (AILD), introduce un quadro di strumenti legali intese ad agevolare le vittime pregiudicate dal risultato di un software. Tuttavia, entrambe le proposte confermano l'approccio antropocentrico della responsabilità civile, perpetuando la concezione secondo cui, in ultima analisi, solo gli esseri umani possono essere ritenuti responsabili di una condotta illecita. Il presente studio si propone così di analizzare la struttura e le caratteristiche del cd. "pacchetto IA", per valutarne l'adeguatezza, così come la tenuta del sistema di responsabilità proposto dalla Commissione UE. Pertanto, la ricerca descrive il quadro di governance predisposto dall'AI Act, per interrogarsi sulla più efficiente allocazione dei costi risarcitori tra tutti gli operatori coinvolti nella catena del valore dei sistemi di IA, esemplificativamente individuati nel fornitore, distributore, importatore e utilizzatore del software: il tutto al fine di stabilire quale regime di responsabilità civile possa garantire al meglio le funzioni compensativa, redistributiva, deterrente e di incentivo ad essa connesse. Dunque, per delineare le soluzioni di policy più adatte al caso di specie urge preliminarmente rispondere ai seguenti quesiti: quali soggetti sono nella posizione migliore per prevenire

[2] M. Phillip, *Tort Liability and Autonomous Systems Accidents - Challenges and Future Developments*, in Tort Liability and Autonomous Systems Accidents, 2023, pp.1-26 disponibile al link: https://www.researchgate.net/publication/374987278_Tort_Liability_and_Autonomous_Systems_Accidents_-_Challenges_and_Future_Developments

[3] Cit. Parlamento EU, Norme di diritto civile sulla robotica - Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=IT ;

l'evento lesivo o evitarne la ripetizione? Come agevolare l'onere probatorio che ricade sulle vittime lese da un software dotato di IA? Quale sistema di compensazione assicura la migliore copertura dei danni individuali e sociali arrecati da un sistema di IA?

Le risposte a tali interrogativi e le relative implicazioni di policy saranno esposte nelle conclusioni, dove verranno contestualizzati i risultati e le considerazioni raggiunte in ciascun capitolo, a completamento delle riflessioni condotte. Pertanto, la struttura della ricerca si articola in quattro capitoli. Il primo introduce l'argomento descrivendo lo sviluppo della tecnologia di IA, partendo dal funzionamento dei moderni algoritmi, dotati di rete neurale e capacità di autoapprendimento, fino alle applicazioni robotiche avanzate. La ricerca esamina criticamente le reali capacità intellettive dei software e l'idoneità del test di Turing nel valutarle. In particolare, si illustrano i diversi gradi di autonomia con cui un algoritmo svolge una prestazione e l'impenetrabilità del suo funzionamento. Il capitolo descrive poi i rischi connessi alla logica inferenziale che governa i sistemi di IA e gli effetti potenzialmente discriminatori; mettendo in luce come tali tecnologie possano acquisire un livello di autonomia decisionale tale da sfidare le tradizionali norme etiche e giuridiche. Pertanto, si analizzano gli interventi di policy sino ad oggi avviati per garantire uno sviluppo ed utilizzo sicuro, equo e trasparente dell'IA, bilanciando i progressi tecnologici con le implicazioni etiche che ne derivano.

Il secondo capitolo analizza la regolamentazione adottata dall'Unione europea sull'IA, partendo dal General Data Protection Regulation (GDPR)[4], riconosciuto come il primo intervento normativo sull'IA, poiché volto a disciplinare il trattamento dei dati personali, attività indispensabile per lo sviluppo e l'addestramento di questi software. Lo studio procede con l'analisi dell'AI Act, descrivendo il percorso legislativo e l'architettura normativa del Regolamento. Verrà illustrata la classificazione piramidale dei sistemi di IA, che li distingue per livello di rischio, con la recente aggiunta di disposizioni specifiche sull'IA generativa; per rispondere ai particolari rischi destati dai Foundation Models. Il capitolo pone in risalto la necessità di un approccio regolatorio armonizzato e coerente, in grado di bilanciare i rischi e i benefici derivanti dall'uso dell'IA, garantendo nel contempo la tutela dei diritti fondamentali dei cittadini.

[4] Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio, 27 Aprile 2016, disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679 ;

Il terzo capitolo entra nel cuore della questione, valuta l'adeguatezza dell'attuale sistema di responsabilità civile nell'affrontare i danni da algoritmo. L'analisi, in particolare, evidenzia una lacuna nella tutela giuridica prestata a determinate fattispecie, laddove il pregiudizio patito a causa della interrelazione tra uomo e macchina non corrisponda ai tradizionali criteri della responsabilità civile. Pertanto, il vuoto di tutela comporta l'ingiusta conseguenza di lasciare il danno lì dove cade, in ragione della pratica impossibilità di riscontrare tutti i presupposti richiesti dalle norme del codice o dalle leggi speciali sulla responsabilità civile. Il capitolo esamina la *ratio* della direttiva 85/374/CEE e l'equilibrio normativo da essa raggiunto tra sicurezza dei prodotti e promozione dell'innovazione. L'analisi rileva come essa non sia in grado di rispondere alle nuove esigenze e squilibri di potere, che si registrano nei rapporti tra gli attori della catena del valore dell'IA. L'asimmetria informativa che connota il funzionamento del software di IA è ancora più pregnante, come emerge dalle difficoltà che la vittima incontra nell'identificazione dei soggetti responsabili e nel soddisfare l'onere della prova previsto dalla normativa. *Quindim* la ricerca analizza il quadro normativo proposto dalla Commissione UE con la pubblicazione della PLD e AILD, per valutarne la completezza e l'efficacia rispetto alle problematiche evidenziate. Infine, il capitolo approfondisce l'opportunità di applicare analogicamente le principali fattispecie di responsabilità extracontrattuale nell'ordinamento italiano, per valutare vantaggi e svantaggi di ciascuna soluzione. Il capitolo conclude sottolineando l'importanza di continuare a sviluppare un regime di responsabilità che sia equo e che stimoli l'innovazione, senza soffocare il progresso tecnologico o imporre oneri sproporzionati ai produttori e agli utenti di sistemi di IA.

Il quarto capitolo, infine, esplora le ricadute economiche del sistema di responsabilità civile, applicato ai sistemi di IA, e del cd "liability gap", avendo particolare riguardo per i sistemi di IA ad alto rischio. Viene sottoposto a scrutinio critico l'approccio avallato dalla Commissione UE, il quale, attraverso una combinazione di regimi di responsabilità oggettiva e per colpa, sembra più focalizzato a colmare le lacune del sistema precedente che a stabilire una nuova struttura normativa con scelte politiche precise. Lo schema ottimale non può limitarsi alla sola funzione compensativa del danno, bensì deve distribuire tutte le esternalità negative che residuano nell'esercizio di una attività o nel commercio di un prodotto ritenuti pericolosi. Pertanto, la ricerca si apre all'indagine di

soluzioni legali alternative, come la polizza assicurativa, utilizzata per ridurre i rischi e alleggerire l'impatto economico sulle aziende tech. Si evidenziano, inoltre, i limiti strutturali del sistema di responsabilità civile, nonché gli elevati costi legali e le difficoltà di individuazione dei responsabili che ne riducono l'efficacia deterrente. A tal fine, l'analisi si allarga allo studio di sistemi redistributivi meno tradizionali, per suggerire un meccanismo di socializzazione dei costi legati ai danni da algoritmo. Questo risultato potrebbe essere raggiunto tramite l'istituzione di un sistema di no-fault e di un fondo di garanzia, per risarcire tutti gli incidenti le cui dinamiche non permettono il tradizionale accertamento dell'illecito o della colpa.

Capitolo I
Opportunità e rischi dell'Intelligenza Artificiale: etica, tecnoetica e diritto

1) Dagli algoritmi alla robotica: i dilemmi etici dei nuovi Agenti

Il concetto di Intelligenza Artificiale (IA) è discusso in letteratura dal 1950, data in cui Alan Turing elaborò l'omonimo test proponendo di sottomettere una serie di domande ad una macchina e ad un essere umano affidando ad un terzo il compito di individuare le risposte formulate dall'individuo. Qualora la macchina fosse stata in grado di replicare alle domande emulando quelle dell'essere umano, avrebbe dimostrato capacita' cognitive, e dunque secondo l'assunto cartesiano "Cogito ergo sum" avrebbe dimostrato la sua natura di soggetto razionale. La metodologia con la quale viene condotto il test rivela che l'oggetto di confronto tra essere umano e software non è il processo logico-cognitivo affrontato dalla macchina bensì il suo risultato. Da allora, il progresso scientifico ha portato alla realizzazione di software sempre più evoluti, capaci di sostituire l'uomo in attività sempre più avanzate; attività non solo meccaniche ma anche e soprattutto cognitive, come guidare un'auto, diagnosticare malattie, condurre colloqui di lavoro, stipulare contratti e polizze, assistere clienti in difficoltà. Ergo i software attualmente elaborati dalla tecnica che «mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»[5] potrebbero facilmente superare il test di Turing e apparire come macchine effettivamente intelligenti.

Tuttavia, ad oggi non esiste una definizione condivisa di Intelligenza Artificiale, ma d'altro canto è ancora assente una definizione ufficiale del concetto stesso di Intelligenza. È inoltre ontologicamente errato parlare di una sola intelligenza artificiale, data la molteplicità di software elaborati con distinte capacità e funzionalità, come i natural

[5]Commissione UE, *L'intelligenza artificiale per l'Europa*, Bruxelles, 25 ottobre 2018, [COM (2018) 237 final], in eur-lex.europa.eu, comunicazione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni.

language systems, machine learning, simulation of senses, neural networks, computer games, expert systems e robotics[6]. È attraverso questi sistemi, o la combinazione di essi, che l'IA imita le facoltà umane, dalla più semplice scrittura di testi e traduzioni o simulazione di esperienze sensoriali, sino alle più complesse capacità di apprendere informazioni ed elaborare decisioni.

Grazie a queste funzionalità la macchina avrebbe raggiunto un certo grado di autonomia nell'adempimento dei compiti assegnatigli. Proprio il grado di autonomia raggiunto dai software ha portato la letteratura a distinguere due macrocategorie di IA, la prima costituisce la forma "debole" ed identifica algoritmi di apprendimento automatico in grado di elaborare soluzioni per problemi relativi a specifici settori[7], attenendosi strettamente alle istruzioni fornite dal programmatore. A questa si contrapporrebbe l'IA forte che supera la funzione di analisi dei dati, presentando capacità adattive in grado di andare oltre le direttive del programmatore, per individuare correlazioni tra dati non precedentemente evidenziate. L'algoritmo in questo caso sarebbe in grado di apprendere dalla propria esperienza (cd. self-learning), tanto da riuscire a rapportarsi con informazioni fino ad allora sconosciute. La capacità di autoapprendimento permette al software di perfezionare una propria discrezionalità nella modalità di adempimento del compito assegnato, il che tuttavia comporta due principali conseguenze: il medesimo software risponderà in modo diverso ad una stessa domanda posta in momenti diversi della sua fase di apprendimento e due software, identici alla nascita, daranno risposte diverse alle stesse domande, a causa delle diverse esperienze registrate durante il funzionamento.

I software dovrebbero quindi essere in grado di migliorare il proprio operato grazie all'arricchimento di dati e feedback raccolti sia dalle interazioni con gli esseri umani che con altri dispositivi. Infatti, la nascita e lo sviluppo dell'IA si rintraccia in un insieme di fattori quali il potere computazionale, la capacità di memorizzazione e il volume di dati. Questi elementi hanno permesso lo sviluppo di una macchina che imita il ragionamento

[6] Cit. P. Cerka, J. Grigiene, G. Sirbikyt, *Liability for damages caused by artificial intelligence*, in Computer Law & Security Review, 2015, p. 378; per maggiori informazioni sulla distinzione di questi sistemi e le loro funzioni vedi John McCarthy, *What is artificial intelligence?*, Stanford University, Computer Science Department, 2007, in https://www-formal.stanford.edu/jmc/whatisai.pdf;

[7] G. Pasceri, *Intelligenza artificiale e algoritmo e machine learning – la responsabilità del medico e dell'amministrazione sanitaria*, in *Temi di diritto privato e di diritto pubblico* (collana diretta da G. Alpa), Milano, Giuffrè, 2021;

umano ma che, ben lungi dal pensare, opera un'analisi statistica svolta su milioni di dati[8]. Infatti, la risposta generata dall'IA a un determinato prompt consiste nella sequenza di parole, immagini o azioni ritenute più probabili dall'algoritmo sulla base del dataset fornito, un'elaborazione prettamente matematica senza alcun apporto critico. Proprio il sistema di apprendimento appena descritto, parallelamente agli sviluppi nel settore della robotica, ha consentito l'integrazione dei sistemi embodied, ovvero componenti hardware dotati della capacità di relazionarsi ed interagire con la realtà esterna ma privi di capacità induttive e deduttive, con i sistemi no-embodied. Questi ultimi, al contrario, sono software intelligenti responsabili del processo di apprendimento e computazionale appena descritto[9]. Dall'integrazione dei software no-embodied con devices hardware sempre più evoluti sono nate nuove forme di Agenti, ossia di enti che determinano autonomamente le proprie azioni nel mondo reale, ma che non comprendono stati mentali ed intenzionalità tipicamente associati all'agire umano. La loro struttura è caratterizzata da tre requisiti: l'assimilazione, la determinazione, il miglioramento[10].

L'"anima"[11] di un sistema di intelligenza artificiale (IA) è rappresentata dagli algoritmi, ossia una serie di istruzioni create dagli sviluppatori per risolvere specifici problemi. Questi algoritmi non risolvono direttamente il problema, ma lo suddividono in sottoproblemi[12], cercando diverse soluzioni possibili per ciascuno di essi. Per giungere alla soluzione di ogni sottoproblema gli algoritmi, che sono alla base dell'IA, procedono delineando «un insieme di possibili soluzioni parziali a un problema, che possono essere

[8] L. Floridi, *The emergence of AI*, in The Ethics of Artificial Intelligence, Principles, Challenges, and Opportunities, Oxford University Press, 2023, p. 5;
[9] Cfr. N. F. Frattari, *Robotica e responsabilità da algoritmo. il processo di produzione dell'intelligenza artificiale*, in Contratto e Impresa – Saggi, 2020, p. 463;
[10] Sulla teoria dei nuovi agenti e le loro tre caratteristiche vedi L. Floridi, *The emergence of AI*, Op. Cit. p.10;
[11] Sull'analogia tra anima e codice vedi N. F. Frattari, Robotica e responsabilità da algoritmo. il processo di produzione dell'intelligenza artificiale, p. 470; Di due a anime, una meccanica ed una cognitiva parla anche L. Floridi in, *Present- AI as a New Form of Agency, Not Intelligence*, in The Ethics of Artificial Intelligence, Principles, Challenges, and Opportunities, Oxford University Press, 2023, p. 20;
[12] M. Liverani, *Algoritmi di Ordinamento*, 2005, l'autore riporta in merito al funzionamento dell'algoritmo Quicksort il sistema «È basato su una strategia di tipo divide et impera, ossia sull'idea di poter suddividere il 8 problema in sottoproblemi di uguale natura, ma via via sempre più semplici da risolvere; ovviamente tale strategia è vantaggiosa solo se lo sforzo necessario successivamente per ricomporre le soluzioni dei sottoproblemi ed ottenere la soluzione del problema iniziale, è inferiore all'impegno necessario per risolvere il problema nel suo complesso con un algoritmo diretto»
disponibile al link: https://www.researchgate.net/publication/265349837_Algoritmi_di_ordinamento

verificate per vedere se sono realmente soluzioni o se potrebbero portare a soluzioni»[13]. Questo sistema determina la rete neurale dell'IA, dove i rami rappresentano le soluzioni parziali, mentre i nodi costituiscono i punti di verifica e l'ultimo stadio riporta tutte le possibili soluzioni[14].

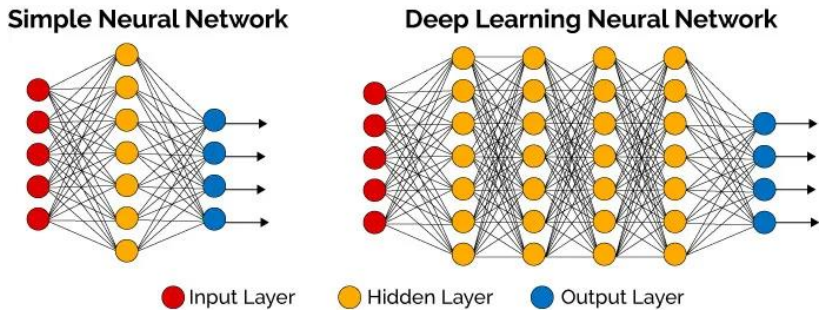

Figura 1. Schema di una rete neurale per Deep Learning.

In questa prospettiva l'algoritmo detta al software la condotta da tenere, durante il traning migliora e affina le prestazioni del network ed inoltre può intervenire nella correzione dei bias presenti sul sistema. In base a questa descrizione sarebbe opportuno impostare sistemi di verifica che orientino verso il risultato eticamente più corretto, ad esempio limitando le conseguenze dannose e pericolose tra gli scenari ritenuti più probabili.

D'altra parte, se l'azione di una macchina si basa sulla soluzione scelta da un algoritmo, è possibile che essa si trovi di fronte a dilemmi etici; un esempio è il caso di un'auto a guida autonoma che, trovandosi di fronte a un ostacolo, deve scegliere tra due scenari possibili: investire un passante o frenare causando un incidente. Un essere umano potrebbe facilmente ritenere la seconda alternativa la meno pericolosa e si ritiene prioritaria la tutela dell'individuo. Tuttavia, il software di controllo della macchina prenderà in considerazione altri elementi nella determinazione della condotta, come la velocità dell'auto, il numero di auto in coda, la distanza con esse, il numero di passeggeri che potrebbero essere coinvolti. Per cui è possibile che l'algoritmo non opti per la scelta ritenuta più etica secondo la morale comune. Il Massachusetts Institute of Technology

[13] Cit. D. Poole, A. Mackworth, *Artificial Intelligence: Foundations of Computational Agents*, Cambridge University Press, 2010;
[14] P. Cerka, J. Grigiene, G. Sirbikyt, *Liability for damages caused by artificial intelligence*, Op. cit. p. 379;

(MIT), a tal proposito ha elaborato una piattaforma online dal nome "Moral Machine"[15] la quale pone all'utente una serie di casistiche sempre più surreali invitandolo a riflettere sulla quantità di dati ed evenienze che una macchina dovrebbe tenere in conto prima di prendere una decisione. I quesiti posti dalla piattaforma interrogano gli utenti sulla migliore scelta da operare in un ipotetico scenario in cui non è possibile terminare la corsa della vettura e si prospettano due possibili dinamiche dell'incidente nelle quali vengono colpite rovinosamente gruppi di persone che differiscono per numero età, sesso, classe sociale.

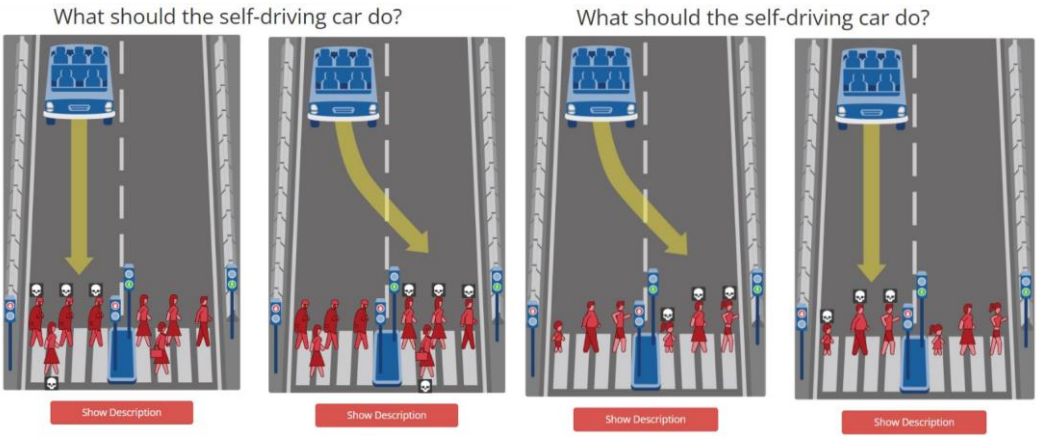

Figura 2. Il quesito della Moral Machine che propone due differenti dinamiche dell'incidente tra cui scegliere.

Questo caso evidenzia l'importanza di dare corrette istruzioni ai dispositivi che, se non correttamente trainati, potrebbero degenerare ritenendo più accettabili le soluzioni in cui perdono la vita donne, senzatetto, persone in sovrappeso, criminali o persone di diversa etnia. Un algoritmo addestrato con dati di scarsa qualità, come quelli provenienti dal pubblico di utenti su internet, potrebbe portare a comportamenti immorali o fortemente discriminatori. Per questo motivo si dovrebbe ritenere estremamente pericoloso affidare ad un computer decisioni sulla salute e sulla vita delle persone, come nel caso di sistemi balistici dotati di puntamento automatico con il compito di identificare i nemici da colpire in una folla di civili[16].

[15] Vedi in https://www.moralmachine.net/ ;
[16] S. Chesterman, *Artificial Intelligence and the Problem of Autonomy*, in Notre Dame Journal on Emerging Technologies (JET) 1, 2020, p. 227; e Cfr. P. U. Lima e A. Paiva, *Autonomous and Intelligent Robots:*

La facoltà dei sistemi di IA di arrecare danni sia al patrimonio che all'integrità psicofisica degli individui solleva numerose questioni di rilevanza legale, in particolare appare necessario stabilire quali sono i soggetti responsabili delle azioni o decisioni pregiudizievoli dell'IA o i criteri per accertare l'errore o il bias dell'algoritmo. Ne consegue che il principio del *neminem laedere* oggi deve includere anche il danno algoritmico, chiamando in causa tutti i soggetti coinvolti nella catena produttiva e distributiva dell'IA e che possono essere ricondotti in modo generale ai «fabbricanti, gli operatori, i proprietari o gli utilizzatori»[17] del robot. Infatti, come ha chiarito il Parlamento europeo, nella risoluzione del 2017, "Norme di diritto civile sulla robotica", l'attuale regime giuridico non permette di considerare robot soggetti giuridicamente responsabili; pertanto, il loro operato deve essere ricondotto ai soggetti artifici della sua fabbricazione e sviluppo. Benché ora sia possibile affidare alle macchine valutazioni un tempo lasciate alla scienza e alla discrezionalità umana, ciò non costituisce un sufficiente elemento di paragone tra l'uomo e la macchina. Infatti, una delle critiche mosse al test di Turing ha proprio ad oggetto il termine di confronto utilizzato per identificare le macchine dotate di intelligenza. La risposta elaborata dalla macchina è il risultato di calcoli probabilistici, che non implicano tutte le considerazioni etiche, storiche, professionali, educative, personali che invece caratterizzano il ragionamento umano. Tutte le macchine sono costruite per sostituire il lavoro dell'individuo, ma non per questo le antropomorfizziamo. La lavastoviglie, ad esempio, è in grado di lavare i piatti in modo più accurato e con un minor dispendio di acqua di un essere umano, ma non per questo viene paragonato all'individuo. Pertanto, «Turing aveva metaforicamente ragione e sostanzialmente torto»[18] in quanto cade nell'errore metodologico di valutare l'intelletto sulla base della risposta e non del processo che ha portato all'asserzione.

Il funzionamento degli attuali software sopra descritto non è il risultato di un processo cognitivo bensì di una potenzialità computazionale elevata ed allenata su un notevole volume di dati. In conclusione, non è possibile per ora parlare di vera e propria

Social, Legal and Ethical Issues, in Multidisciplinary Perspectives on Artificial Intelligence and the Law, edited by Antunes, Henrique Sousa, et al., Springer International Publishing AG, 2024, p. 134;

[17] Cit. Parlamento europeo, Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL);

[18] Sulla critica al test di Turing e l'esempio della lavastoviglie vedi L. Floridi in, *Present- AI as a New Form of Agency, Not Intelligence*, Op. cit. da cui anche la citazione riportata a pag. 20;

Intelligenza Artificiale, quanto più di potenti calcolatrici istruite per individuare la soluzione più efficiente dato un certo numero di variabili in gioco e scenari ipotizzabili.

2) I pericoli di un'IA autonoma e discriminatoria

La capacità dell'algoritmo di apprendere dalla propria esperienza gli permette di raggiungere output più accurati, deducendo nuovi criteri per selezionare le risposte migliori grazie ai dati ed i feedback raccolti durante il suo funzionamento. Questa facoltà è stata sviluppata grazie all'interconnessione tra componenti embodied e no-embodied che consente al software un collegamento con il mondo esterno grazie a sensori ed interfacce. L'autoapprendimento, unitamente alla capacità di adempiere ai compiti senza la necessità di un intervento umano, costituisce l'elemento sul quale si sviluppa l'autonomia dei sistemi[19]. Sebbene ad oggi non esista una nozione di autonomia dell'IA universalmente accettata, letteratura accademica, ricercatori, aziende e istituzioni hanno sottolineato la centralità dell'autonomia dell'IA in tutti i report riguardanti i rischi associati e i tentativi di regolamentazione. Già il Parlamento europeo nella citata risoluzione definiva l'autonomia delle macchine come «la capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna»[20] . Anche la letteratura ha contribuito alla definizione dell'autonomia propria dell'IA quando, andando ad analizzarne gli aspetti più tecnici ha definito il robot autonomo come "un sistema "embodied", dotato di sensori per percepire e comprendere il mondo circostante, attuatori che gli permettono di agire su quel mondo (eventualmente includendo l'interazione con altri robot, animali e/o esseri umani), e capacità decisionale completamente indi controllo esterno, ovvero da parte dell'uomo»[21]. Alla molteplicità di definizioni si aggiungono i diversi gradi e forme in cui l'autonomia si riscontra nelle macchine. Infatti, nella tecnica si possono distinguere prodotti caratterizzati da diversi

[19] N. F. Frattari, *Robotica e responsabilità da algoritmo. il processo di produzione dell'intelligenza artificiale*, op. cit. p. 466;
[20] Cit. Parlamento europeo, Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL), capo sulla "Responsabilità", lett. AA;
[21] Cit. P. U. Lima e A. Paiva, *Autonomous and Intelligent Robots: Social, Legal and Ethical Issues*, Op. cit. p. 128;

gradi e tipi di autonomia, ad esempio fisica e/o cognitiva, parziale o totale. Alcuni sistemi presentano un'autonomia parziale se capaci di interpretare soltanto determinati tipi di dati a disposizione e selezionano le soluzioni limitatamente all'obiettivo per i quali sono stati programmati. Ciò che invece possono modificare in autonomia sono le istruzioni che guidano la selezione della risposta[22]. Infine, si distinguono diversi tipi di autonomia, da quella fisica e cognitiva, a quella morale, sino a raggiungere la piena consapevolezza di sé con la capacità di elaborare un'intenzione propria. Sotto questo profilo è possibile distinguere, ad esempio, le auto driveless e self-driving, infatti in base ad una classificazione condotta da SAE, Society of Automotive Engineers International che prende ad oggetto il rapporto tra l'automa e il conducente, si identificano cinque livelli di automazione:

1) il primo livello corrisponde ai sistemi di driver assistance presenti in quasi tutti recenti modelli di automobile in commercio, sono in grado di adattare la velocità, mantenere il veicolo nella corsia, o di frenare in caso di emergenza, previo consenso dell'autista;
2) il secondo livello consente la gestione automatizzata di accelerazione, decelerazione, ed il cambio di direzione;
3) il terzo livello permette al sistema di controllare tutte le funzioni della vettura, ma residua il potere del conducente di intervenire tempestivamente in caso di necessità;
4) il quarto livello prevede un intervento dell'uomo limitato all'inserimento di parametri come la destinazione e la velocità massima;
5) il quinto livello è costituito dalla totale automazione del veicolo[23].

Pertanto, una macchina completamente autonoma potrebbe essere qualificata come robot, incontrando il primo rilevante contrasto con il vigente regime di responsabilità civile. Infatti, quest'ultimo si fonda sul controllo esercitato dal proprietario o dal detentore sulla cosa che ha prodotto il danno, una condizione tuttavia incompatibile con l'autonomia del software. L'evoluzione del robot da strumento ad agente, dovuta alla sua capacità di modificare i criteri di selezione per elaborare risposte e azioni, potrebbe

[22] D. M. Terramundi, *Le sfide della discriminazione algoritmica*, in GenIus, 2022, p. 26;
[23] M. Tampieri, L'intelligenza artificiale: una nuova sfida anche per le automobili, Contratto e impresa, 2020, p. 747;

scagionare conducenti e produttori dall'imputazione della responsabilità per i danni causati dall'automa. Tuttavia, con tale asserzione, non si vuole sostenere un'equivalenza tra autonomia ed intelligenza, piuttosto la prima è considerata requisito necessario, ma non sufficiente, della seconda[24]. Pertanto, l'IA non ragiona, ma agisce. La separazione tra intelletto e azione[25], anche per lo svolgimento di tutti quei compiti che richiedono uno sforzo cognitivo, è permessa grazie alla più che sufficiente conoscenza raccolta e analizzata dall'IA sulle soluzioni applicabili al dato problema. Se si pone ad esempio la redazione di un parere legale, si possono distinguere molteplici attività richieste al cervello umano: la conoscenza di casi simili precedenti, l'estrapolazione della *ratio* che caratterizza la soluzione assunta per ciascun di essi, nonchè l'esperienza del professionista sulla materia, sull'istituto o sulla giurisprudenza adottata dal tribunale competente e, in qualche caso, fantasia o inventiva. La scienza ha quindi elaborato software che sostituiscono il giurista in attività tecniche meno complesse, come la selezione di documenti utili per una causa, ma anche algoritmi per il suggerimento di precedenti e norme utili alla redazione di atti e pareri[26]. In tal caso la macchina non comprende a fondo le caratteristiche del caso concreto ma risponde facendo appello ad un'immensa massa di dati sui precedenti legali, che le permettono quindi il raggiungimento di una cognizione approfondita della materia. Tuttavia, almeno per ora, l'intelletto gioca un importante ruolo in queste come in altre professioni, infatti il tool non promette di ottenere atti giudiziari perfetti pronti per l'utilizzo, bensì assiste gli avvocati nella redazione di atti o pareri.

A causa della correlazione tra autonomia e dataset usati dall'IA possiamo desumere che, per un suo corretto sfruttamento, è necessario un ambiente AI-friendly, che consenta la raccolta di dati grazie alle interazioni tra l'uomo e la realtà digitale. Secondo Floridi,

---

[24] P. U. Lima e A. Paiva, *Autonomous and Intelligent Robots: Social, Legal and Ethical Issues*, Op. cit. p. 128;

[25] Sulla metafora del divorzio tra azione e intelletto vedi L. Floridi, *Present - AI as a New Form of Agency, Not Intelligence*, Op. cit. p. 24;

[26] Questo software AI è disponibile al link: https://www.paxton.ai/drafting?utm_term=legal%20document%20automation&utm_campaign=Contract+Review&utm_source=adwords&utm_medium=ppc&hsa_acc=2628735617&hsa_cam=21149240576&hsa_grp=160110283109&hsa_ad=695349301351&hsa_src=g&hsa_tgt=kwd-512864940367&hsa_kw=legal%20document%20automation&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKCAjwps-zBhAiEiwALwsVYUwZJzJ3zOEFap5wdA83J77gCJXJE1wQB3VwmdgN988qkQbup0gjahoCu8IQAvD_BwE ;

la ormai costante sovrapposizione tra le realtà offline e online avrebbe integrato un terzo livello di esistenza chiamato "infosfera"[27]. Infatti, un set di dati esaustivo, vario e aggiornato è il presupposto per un AI di qualità che elabori soluzioni accurate e che riflettano il più fedelmente possibile le specificità del caso concreto. L'algoritmo, come qualsiasi processo matematico, basa la propria risposta sui numeri; pertanto, qualora la soluzione suggerita dall'AI non corrisponda alla fattispecie, l'errore deve essere ricercato nelle operazioni matematiche o nei numeri stessi[28]. I dati costituiscono la descrizione matematica della realtà, qualora siano incompleti anche la concezione della realtà dell'IA sarà parziale e corrotta. L'inesattezza del set di dati e l'incapacità dell'algoritmo di ridimensionare i dati in determinati contesti può degenerare in conclusioni inesatte che, se poste a base di azioni o decisioni, avrebbero un grave potenziale discriminatorio. Questo difetto dell'IA preoccupa soprattutto in particolari settori di grande rilevanza economico-sociale come quello della salute, dell'istruzione, dell'occupazione, dell'accesso al credito e dei servizi finanziari. Un caso di studio è stato presentato da Peter Embi, il quale ha commentato un'analisi dell'IBM sul funzionamento di un software progettato per analizzare l'incidenza della depressione post-partum nelle donne. L'algoritmo era stato sviluppato per prevedere la richiesta di servizi sanitari relativi a questa patologia, al fine di allocare adeguatamente le risorse necessarie. Per questo motivo, erano stati inseriti nel sistema di intelligenza artificiale i dati relativi alle diagnosi e alle richieste di sostegno psicologico pervenute a Medicaid da parte delle puerpere.

In base ai dati analizzati, il software segnalava una maggiore probabilità di riscontrare la depressione post-partum nelle donne bianche rispetto alle donne di colore. Questo risultato contrastava con le evidenze empiriche, che mostravano una più alta incidenza della malattia tra le donne di basso status socio-economico, aventi diritto al sostegno pubblico per la salute. La ragione di tale discrepanza risiedeva nella parzialità della ricerca, che non aveva coinvolto un numero sufficiente di donne di colore. Di conseguenza, l'algoritmo aveva interpretato la carenza di dati sulle diagnosi di depressione nelle donne di colore come una loro minore predisposizione alla malattia, piuttosto che come il risultato di un mancato coinvolgimento di quella categoria di donne

[27] L. Floridi, vedi nota 21;
[28] D. M. Taramundi, *Le sfide della discriminazione algoritmica*, in GenIus, 2022, p. 26;

nello studio.[29] Questo dimostra che le preoccupazioni generate dall'implementazione di sistemi dotati di IA in settori sempre più ampi della società e dell'industria non sono del tutto prive di fondamento.

Due assunti possono essere ricavati da questo esempio: un set di dati incompleto può portare ad un risultato non corretto; e i dati riflettono discriminazioni già presenti nel modo reale. Nell'esempio citato l'algoritmo ha dedotto semplicemente che il numero di pazienti rispecchiasse l'esatto numero delle donne affette. Non contestualizzava il dato alla luce delle disparità economiche che non permettono a tutti di raggiungere i medesimi servizi, anche sanitari. Il pericolo è aggravato nei casi di discriminazione indiretta, ossia i casi in cui i criteri o trattamenti dati apparentemente neutri determinino situazioni di svantaggio per ragioni di sesso, razza, etnia, orientamento sessuale, lingua, religione, opinione politica, disabilità o età[30].

La corretta interpretazione dei dati e la ragionevolezza delle conclusioni sono elementi imprescindibili per valutare una scelta o di un responso. Ad esempio, un software utilizzato per la selezione del personale in determinati settori potrebbe erroneamente considerare le persone che portano gli occhiali più competenti, basandosi sulla loro percentuale nell'attuale posto di lavoro. Questo tipo di bias può portare a decisioni non obiettive e discriminatorie. Altri algoritmi potrebbero subire lo stesso bias in relazione al numero di donne presenti nella determinata azienda o ufficio[31]. Il medesimo errore ricorre nei software programmati per valutare la solvibilità dei clienti che richiedono un prestito o un credito[32]. Inoltre, come verrà approfondito nei capitoli

---

[29] P. J. Embi, *Algorithmovigilance—Advancing Methods to Analyze and Monitor Artificial Intelligence–Driven Health Care for Effectiveness and Equity*, in *Jama Network Open*, 2021. Un altro caso in cui l'utilizzo costante di dati provenienti da una determinata razza può portare ad un trattamento sanitario diverso è il caso di strumenti medici e.g. « in the area of skin cancer, are programmed to identify images of light skin and not dark skin, even if black population has a higher mortality rate from melanoma cancer. Also in the area of negative discrimination by race, there are algorithms in the area of hospital costs that induce to determine that black patients are healthier than white patients and for this reason, these receive a better treatment» in M. S. Fernandes and J. R. Goldim, *Artificial Intelligence and Decision Making in Health: Risks and Opportunities*, Artificial Intelligence and Normative Challenges International and Comparative Legal Perspectives, in Law, Governance and Technology Series, Springer Nature Switzerland AG 2023, p. 198;

[30] D. M. Taramundi, *Le sfide della discriminazione algoritmica*, Op. cit. p. 28;

[31] J. Goncalves-sa e F. Pinheiro, *Societal implications of Reccomandation Systems: A Technical Perspective,* in Multidisciplinary Perspectives on Artificial Intelligence and the Law, edited by Antunes, Henrique Sousa, et al., Springer International Publishing AG, 2024, p. 55;

[32] Cfr. V. Papadouli, *Artificial Intelligence's Black Box: Posing New Ethical and Legal Challenges on Modern Societies*, nel numero Artificial Intelligence and Normative Challenges International and Comparative Legal Perspectives, in Law, Governance and Technology Series, Springer Nature Switzerland

successivi, il danno potrebbe estendersi ben oltre il pregiudizio individuale qualora la dinamica discriminatoria investa non più determinati individui, bensì un'intera collettività. In questo caso il pregiudizio verrebbe subito non soltanto dagli utenti/clienti che entrano in contratto con il software, ma dall'intera categoria di persone. Ne sono un esempio i trial clinici, precedentemente menzionati, i cui set di dati per ragioni storiche e sociali vedono una maggiore rappresentazione di alcune etnie e/o di un genere. Queste inferenze ledono contemporaneamente sia l'individuo che la collettività di riferimento.

Tuttavia, per una corretta comprensione del fenomeno è necessario separare il concetto di bias da quello di discriminazione. Infatti, mentre i bias riguardano strettamente i difetti del modello alla base dell'algoritmo, e possono essere causati da dati di cattiva qualità e processi inferenziali corrotti; la discriminazione invece ha un significato socio normativo ben specifico e concerne tutte le ingiustificate disuguaglianze che potrebbero originare dalla decisione dell'algoritmo[33]. Il principio di non discriminazione, condiviso da tutte le dichiarazioni sui diritti fondamentali[34], deve trovare applicazione anche presso i giudizi generati dai sistemi di AI. A sostegno di questo principio la Dichiarazione di Montrèal sullo sviluppo responsabile dell'Intelligenza Artificiale impone agli operatori del settore di produrre «sistemi IA (…) progettati e addestrati in modo da non creare, rafforzare o produrre discriminazioni in base, tra l'altro, a differenze sociali, sessuali, etniche, culturali o religiose»[35]. Sul punto è bene specificare che non tutti i trattamenti differenziati hanno carattere discriminatorio, al contrario in alcuni casi condizioni diverse hanno lo scopo di colmare le disuguaglianze sociali ed economiche; ad esempio, alcune università prevedono importi delle tasse d'iscrizione diversificate in base al reddito degli studenti. Il principio, in breve, rispecchia la differenza tra eguaglianza ed equità, dove la prima garantisce a tutti lo stesso trattamento, mentre la seconda elargisce a tutti solo ciò che meritano o di cui hanno bisogno. Pertanto, un

---

AG 2023, p. 47, l'autore riporta il caso di un algoritmo utilizzato per valutare la solvibilità dei client: «This has already been noticed in case of a credit card launched some years ago by the prominent American bank Goldman Sachs in cooperation with the famous tech-giant company Apple: their "employed" AI system was blamed for discriminating against women and the most prevalent reason was found to be the 'intrusion' of inherent biases in its training datasets.»

[33] D. M. Taramundi, *Le sfide della discriminazione algoritmica*, Op. cit. p. 27;

[34] Il principio di non discriminazione è protetto dalle seguenti disposizioni a titolo esemplificativo: art.14 CEDU, art. 21 Carta di Nizza, art. 7 della Dichiarazione Universale dei Diritti Umani, art. 26 del Patto Internazionale sui Diritti Civili e Politici, non ultimo, l'articolo 3 della Costituzione italiana;

[35] Reperibile al link https://declarationmontreal-iaresponsable.com/wp-content/uploads/2023/01/VF_UdeM_Decl_IA_Resp_LA_Declaration_Ital_26oct2021.pdf ;

trattamento risulterà discriminatorio qualora i criteri adottati per distinguere le fattispecie siano irragionevoli o errati.

Alla luce dei rilievi esposti sull'autonomia dei sistemi di IA, nella determinazione dei criteri per l'elaborazione dell'outcome, e sulle potenziali conseguenze discriminatorie degli stessi o delle istruzioni impartite all'AI, risulta chiaro che deve essere operato un bilanciamento tra rischi e benefici legati all'utilizzo del software. Se da un lato, nello svolgere le medesime mansioni caratterizzate da una certa ripetitività, la sostituzione di impiegato con un sistema automatizzato può consentire di beneficiare di maggiori efficienza e velocità nello svolgimento, dipendente dalla capacità dell'IA di identificare pattern da cui elaborare schemi su cui fondare le proprie previsioni; dall'altro, ove le decisioni e le valutazioni da operare nello svolgimento di una determinata attività impingendo nella sfera intima o morale della vita delle persone, come ad esempio la sfera sanitaria o politica, queste non possono essere lasciate all'analisi di una macchina calcolatrice. L'arbitrarietà dell'uomo, sia nella scelta dei parametri da valutare, che nel decidere di emettere un giudizio potrebbe costituire un'immensa differenza nelle operazioni militari, dove è necessario distinguere nemici dai civili oppure stabilire una diagnosi di cancro con il solo utilizzo di un'immagine[36]. Dovrà pertanto essere valutata caso per caso l'opportunità di demandare le decisioni ad un software, rispetto al suo utilizzo come semplice strumento a sostegno dell'ingegno e della discrezionalità umana. In questa prospettiva, il regime di responsabilità che verrà adottato per compensare i danni arrecati dagli algoritmi potrebbe orientare l'ago della bilancia tra decisore umano e automatizzato in base al livello di rischio implicato del device e i potenziali costi risarcitori.

[36] Su un'analisi approfondita relativa alle questioni etiche relative alle armi automatiche che utilizzano sistemi di AI vedi S. Chesterman, *Artificial Intelligence and the Problem of Autonomy*, p. 241;

3) Programmare l'algoritmo secondo principi etici

Le criticità illustrate nel precedente paragrafo sono state portate all'attenzione pubblica da esperti e operatori del settore (come Elon Musk e Steve Wozoniak), che nel marzo 2023 hanno pubblicato una lettera aperta per chiedere una pausa immediata di sei mesi nello sviluppo e training di sistemi più potenti di Chat Gpt-4 per focalizzarsi, invece, sul perfezionamento dei sistemi di IA generativi già presenti sotto il profilo della sicurezza, accuratezza, trasparenza, resistenza e affidabilità[37]. I dubbi sulla compatibilità dei sistemi di IA con l'attuale struttura etica, sociale ed economica sono stati sollevati anche dalle istituzioni europee e statunitensi. Nel 2016 l'OSTP (White House Office of Science and Technology Policy (OSTP), la Commissione per Gli Affari Giuridici del Parlamento europeo e il Comitato Ristretto per la Scienza, l'Innovazione e la Tecnologia hanno pubblicato tre distinti report sulle strategie per affrontare lo sviluppo dell'IA. I documenti, pur con separati approcci, condividono l'obiettivo di costruire una "good AI society", attraverso la collaborazione dei governi, del settore privato e della comunità accademica. Il Parlamento europeo in particolare ha evidenziato la necessità di regole comuni nel territorio europeo per condurre test sui sistemi intelligenti in un contesto reale, per identificare in modo uniforme gli esperimenti autorizzati e quelli eccessivamente rischiosi[38]. Il report rilasciato dal Parlamento suggerisce di elaborare un quadro di principi etici comuni per lo sviluppo della robotica "Guidelines on Regulating Robotics" e che dovrebbe guidare sia la programmazione che l'utilizzo di sistemi di AI. Si parla infatti di principi roboetici, i quali non devono essere concepiti come un codice etico per le macchine, in quanto non ancora dotate di intenzionalità, bensì dovrebbero orientare i programmatori nello sviluppo dell'IA e nel bilanciamento tra i vantaggi e i potenziali rischi della nuova tecnologia. Nello specifico questi precetti impongono: la protezione dell'essere umano dai danni arrecati dai robot, il diritto di rifiutare l'assistenza di un robot, il rispetto della libertà dell'uomo, la tutela della privacy, il contrasto alle tecniche manipolatorie dell'IA soprattutto nei confronti della popolazione più fragile, la tutela dei

[37] Future of Life Institute, Pause Giant AI Experiments: An Open Letter, in https://futureoflife.org/open-letter/pause-giant-ai-experiments/ ;

[38] Per uno studio che analizza il contenuto e compari le strategie dei tre report vedi. Cath, C. and Wachter, S. and Mittelstadt, B. and Taddeo, M. and F., Luciano, *Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach*, 2016. Available at SSRN: https://ssrn.com/abstract=2906249 or http://dx.doi.org/10.2139/ssrn.2906249;

legami sociali, la garanzia ad un equo accesso alla tecnologia per limitare il divario digitale[39]. L'OSTP, invece, evidenzia la necessità di garantire la trasparenza e la comprensibilità delle logiche dei sistemi per poter implementare i principi etici di equità, responsabilità e giustizia sociale, tuttavia non indica gli strumenti legali per raggiungere questi obiettivi. Il report suggeriva, inoltre, di impartire lezioni di etica a ad ingegneri e sviluppatori del settore AI per istruirli a riconoscere bias e risultati corrotti, nonché porvi rimedio[40]. Infine, anche il Comitato inglese prevede collaborazioni tra diversi esperti, anche a livello istituzionale, all'interno di una Commissione sull'Intelligenza Artificiale per lo studio di implicazioni etiche, legali e sociali dell'utilizzo di sistemi AI.

La collaborazione tra esperti umanisti e tecnici è necessaria per stabilire i principi etici da seguire e per tradurli in linguaggi informatico. La scelta della condotta più corretta da seguire può risultare difficile da definire in astratto, ovvero senza i dettagli del caso concreto; tuttavia, dovranno essere individuate delle best practice che, in ciascun settore, istruiscano l'algoritmo nella selezione del risultato più corretto possibile. Peraltro, anche la valutazione morale della condotta umana comporterebbe i medesimi dubbi; ad esempio in un processo giudiziario, benchè esistano regole precise per giudicare la colpevolezza dell'imputato, l'azione non viene giudicata in astratto, ma alla luce delle circostanze del caso concreto[41]. Le difficoltà crescono se si considera che non tutti gli uomini condividono gli stessi dettami morali, né la medesima scala di priorità. Vi sono infatti diversi approcci che potrebbero modificare i parametri decisionali dell'IA; infatti ipotizzando un software che applichi la prospettiva utilitarista questo si concentrerebbe solo sugli esiti concreti della decisione/azione, invece se si attenesse alla filosofia kantiana indagherebbe l'intenzione dell'automa, diversamente se considerasse l'etica

[39] European Parliament Committee on Legal Affairs. (2016). Civil law rules on robotics (2015/2103 (INL)). Brussels, Belgium: European Parliament, 4° paragrafo "Analysis of the ethical principles to develop in robotics", in https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf ;
[40] Executive Office of the President National Science and Technology Council Committee on Technology. (2016). Preparing for the future of artificial intelligence. Washington, DC, USA, p. 32; in https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_ for_the_future_of_ai.pdf.
[41] M. S. Fernandes and J. R. Goldim, *Artificial Intelligence and Decision Making in Health: Risks and Opportunities*, in Multidisciplinary Perspectives on Artificial Intelligence and the Law, edited by Antunes, Henrique Sousa, et al., p. 199;

delle virtù l'azione dovrebbe essere qualificata in base alle qualità che promuovono o dimostrano[42].

Una volta stabilita la scala di valori con la quale analizzare le azioni e giudizi emessi dalla macchina è necessario trasmetterli all'algoritmo: è possibile intervenire sugli scopi per i quali la macchina è predisposta, oppure sulle singole istruzioni che guidano il software stesso nella selezione delle risposte. Gli sviluppatori, considerando le caratteristiche e i rischi associati all'IA, possono prevenire l'attuazione di determinate azioni o risultati, minimizzando così il rischio di danni e, nel caso questi si verifichino, attenuarne le conseguenze. L'obiettivo non è costruire una "macchina morale", ossia un sistema capace di seguire l'imperativo categorico di Kant, bensì impartire istruzioni e codici informatici che indirizzino la scelta dell'algoritmo verso il risultato ritenuto più corretto ed equo dalla collettività di riferimento. Tuttavia, la traduzione di dettami etici in linguaggio informatico non è così diretta. Gli algoritmi, infatti, «non tollerano l'ambiguità o l'incertezza, che sono sempre presenti nel mondo reale»[43], pertanto dovranno essere elaborati comandi certi, come il divieto di determinate pratiche o l'utilizzo di criteri discriminatori[44].

Quindi valori come l'altruismo, la solidarietà o la perequazione sono troppo generici e indeterminati per essere insegnati ad una macchina, per ora, inoltre ciascun ambito di applicazione implicherà dilemmi etici diversi e in base allo scopo perseguito. In medicina, ad esempio, i principi di bioetica impongono il rispetto del consenso, della dignità umana, della salute psicofisica, dei diritti umani e della responsabilità, nonché della libertà di autodeterminazione e del diritto di rifiutare le cure predisposte tramite AI[45]. Infatti, la disponibilità del pubblico di affidare la propria diagnosi ad un algoritmo non è così scontata; ma lo stesso potrebbe anche dirsi di altri servizi in grado di incidere sulla situazione sostanziale di un soggetto come la stipulazione di una polizza o di un contratto. Sebbene le valutazioni automatizzate siano ritenute più imparziali di quelle umane,

[42] U. Pagallo, *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in Sistemi intelligenti, Il Mulino - Rivisteweb, p. 618;
[43] Cit. M. S. Fernandes and J. R. Goldim, *Artificial Intelligence and Decision Making in Health: Risks and Opportunities*, Op. cit.;
[44] V. Papadouli, *Artificial Intelligence's Black Box: Posing New Ethical and Legal Challenges on Modern Societies*, Op. cit. p. 57;
[45] M. S. Fernandes and J. R. Goldim, *Artificial Intelligence and Decision Making in Health: Risks and Opportunities*, Op. cit. p. 200;

perché non corrotte da imprecisioni dovute a errore umano, pigrizia, antipatia o incompetenza, non hanno guadagnato del tutto il favore di consumatori e utenti.

Sussiste ancora una generale mancanza di fiducia nei confronti dell'AI, non tutti apprezzano la voce preregistrata nei centralini e neppure le chat-bot, utilizzate come prima interfaccia nell'assistenza al cliente. Pertanto, ci si attende la medesima reticenza del pubblico anche nell'utilizzo di sistemi di AI per gestire rapporti più complessi nel campo dei diritti civili, della cosa pubblica o sulla strada alla guida di un'auto.

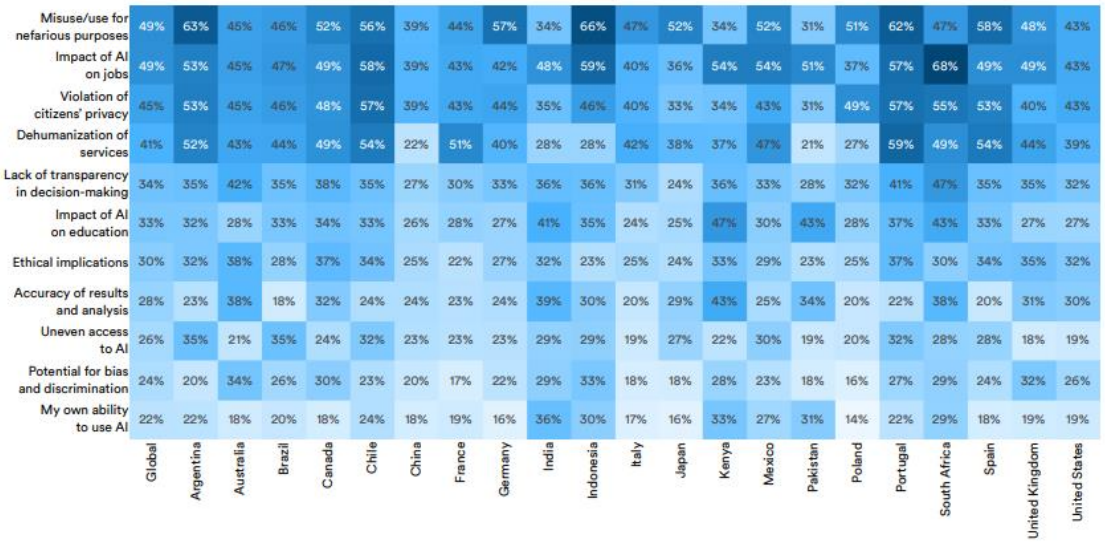

Figura 3. Preoccupazioni relative all'IA nel mondo secondo il "Report sugli indici IA" 2024 dell'OCSE.

In particolare, a spaventare il comune utente è la mancanza di controllo sul funzionamento del device e l'impossibilità di conoscere le ragioni che hanno condotto ad un determinato risultato. I sistemi di deep-learning non sono in grado di argomentare le proprie decisioni, inoltre non sono capaci di distinguere la causalità tra fatti dalla mera correlazione tra dati. Quindi esteriormente è difficile, se non impossibile, capire se la decisione sia fondata su assunti discriminatori e parziari. Infatti, l'algoritmo elabora le proprie decisioni senza divulgare i dati e i criteri che ne costituiscono il fondamento. L'opacità, per ora irrisolta, dei software non consente di aggirare agilmente il pericolo di discriminazioni, in quanto ostacola l'identificazione dell'errore. Come in un sillogismo, non è possibile individuare una conclusione errata senza conoscere la premessa minore e

l'assunto principale[46], perché è dall'inferenza tra i due che si valuta la ragionevolezza della prima. La poca trasparenza comporta anche l'imprevedibilità della condotta dell'AI, in quanto la funzione di autoapprendimento arricchirà la rete neurale di nuovi e inaccessibili patterns. Il difetto è aggravato dalla abilità dell'algoritmo di individuare nuovi modelli per selezionare le sue conclusioni ma senza identificare nuove relazioni causali tra i dati; Tuttavia, se non riesce ad individuare le relazioni causali sottostanti tra questi dati, il suo ragionamento rimane limitato, in quanto l'algoritmo continuerà a basarsi sui dati originali senza essere in grado di adattarsi o comprendere la reale dinamica dei fenomeni.

In altre parole, anche se l'algoritmo trova nuovi modi per analizzare i dati, non sarà in grado di capire[47]. L'opinione pubblica globale ha quindi richiesto una maggiore attenzione di governi, istituzioni ed enti di ricerca nello sviluppo della tecnologia, a cui ha fatto seguito una codificazione plurale e variegata di principi etici ai quali operatori del settore e utilizzatori dovranno attenersi. Infatti, accanto alla dichiarazione di Montreàl possiamo menzionarne ulteriori che hanno proposto linee guida o elenchi di principi sul corretto utilizzo dell'IA.

Asilomar AI Principles	Sviluppati durante una conferenza nel 2017 dall'Future of Life Institute, questi principi si concentrano su ricerca, etica e valori, e problemi a lungo termine legati allo sviluppo dell'IA[48].
IEEE Ethically Aligned Design	Identifica tre Principi Generali che dovrebbero guidare lo sviluppo etico dell'IA: garantire i diritti umani, perseguire il benessere umano e ambientale, e mitigare i rischi[49].

[46] C. Cutrecasas, *Legal challenges of Artificial Intelligence (AI)*, in *Global Privacy Law review*, 2020, p. 6;
[47] M. V. Butz, *Towards Strong AI*, in KI - Künstliche Intelligenz, 2021, p. 3 https://doi.org/10.1007/s13218-021-00705-x ;
[48] Disponibile al link https://futureoflife.org/open-letter/ai-principles/ ;
[49] Disponibile al link https://standards.ieee.org/industry-connections/ec/ead-v1/ ;

Linee guida etiche dell'UE per un'IA affidabile	La Commissione Europea ha nominato un gruppo di esperti ad alto livello sull'IA i quali hanno presentato un elenco di 7 requisiti fondamentali che i sistemi di IA dovrebbero soddisfare per essere considerati affidabili[50].
L'etica dell'IA: modellare il futuro delle nostre società	L'UNESCO ha pubblicato una raccomandazione nel quale evidenzia le 5 aree politiche nei quali attivare interventi concreti affinché le politiche raggiungano uno sviluppo e un uso etico dell'intelligenza artificiale[51].
Dichiarazione di Toronto	La dichiarazione adottata da Amnesty International nel 2018 tutela il diritto di eguaglianza e di non discriminazione rispetto all'utilizzo di sistemi di machine learning[52].
Hiroshima AI Process	lanciato sotto la presidenza del G7 del Giappone nel maggio 2023, mira a creare una governance inclusiva e sicura per l'intelligenza artificiale avanzata, come l'AI generativa. L'iniziativa ha portato la pubblicazione dei "Principi guida internazionali" e il "Codice internazionale di condotta per le organizzazioni che sviluppano sistemi di ia avanzati"[53]

Tabella 1. Principali iniziative promosse da attori pubblici e privati nella regolazione dell'IA.

Le iniziative nell'ambito della governance dell'IA avrebbero un impatto maggiore e una diffusione più ampia se fossero promosse da organizzazioni internazionali altamente rappresentative o da gruppi di lavoro che riuniscono esperti di diverse nazionalità e competenze. Soltanto una lista di principi globalmente condivisi potrebbe costituire un set di standard minimi ai quali gli operatori di AI, che spesso operano su un mercato

[50] Disponibile al link: https://digital-strategy.ec.europa.eu/it/library/ethics-guidelines-trustworthy-ai ;
[51] Disponibile al link: https://www.unesco.it/wp-content/uploads/2023/11/Brochure-su-Raccomandazione-UNESCO-sullIntelligenza-Artificiale-1.pdf ;
[52] Disponibile al link: https://www.torontodeclaration.org/declaration-text/english/ ;
[53] Disponibile al link: https://www.japan.go.jp/kizuna/2024/02/hiroshima_ai_process.html ;

internazionale, devono uniformarsi nello sviluppo dei loro prodotti. Con questo presupposto la Commissione europea nel 2020 pubblicava un Libro Bianco sull'approccio europeo all'IA volto a «favorire i progressi scientifici, a preservare la leadership tecnologica dell'UE e a garantire che le nuove tecnologie siano al servizio di tutti gli europei e ne migliorino la vita rispettandone i diritti»[54]. Il documento suggerisce un confronto internazionale su un nucleo di principi condivisi e proponeva l'Europa quale sede ideale per la composizione e mediazione dei diversi interessi e valori sensibili.

Le organizzazioni internazionali hanno promosso iniziative anche nell'elaborazione dei principi IA individuati dal Policy Observatory dell'OCSE, successivamente approvati dal G20. I principi rivolti agli operatori di IA chiedono: uno sviluppo inclusivo e sostenibilità, rispetto dei diritti umani e dei valori democratici assicurando una società equa e giusta, trasparenza ed esplicabilità, resistenza e sicurezza, responsabilità. Parallelamente ai governi si indirizzano le seguenti raccomandazioni nell'implementazione di AI policies: investire nella ricerca, costruire un ambiente economico e politico favorevole allo sviluppo dell'IA, reperire competenze e formare la nuova forza lavoro per la transizione digitale, promuovere la cooperazione internazionale per elaborare una strategia unitaria allo sviluppo responsabile dell'IA[55]. Il trend ha portato all'emissione di circa 200 codici di condotta e linee guida per i sistemi di intelligenza artificiale. L'alta produzione di iniziative di soft law è il risultato di iniziative di policy isolate avviate singolarmente da ciascuna organizzazione internazionale o associazione di stakeholder; invece di limitarsi a recepire i principi già esistenti, queste entità hanno preferito affermare una propria politica, generando così una pioggia di direttive etico-normative.

Dall'analisi comparata dei documenti è possibile individuare un nucleo di principi comuni che possono essere individuati in: benessere, inoffensività, giustizia, autonomia e trasparenza. L'interpretazione di questi principi può divergere leggermente, tuttavia è possibile individuare nozioni condivise di ciascun principio, il benessere ad esempio dev'essere inteso quale miglioramento delle condizioni di salute dell'uomo e di salubrità dell'ambiente. Invece, l'inoffensività dell'IA si riferisce alla sua inattitudine a causare

[54]Cit. Commissione UE, Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, Bruxelles, 19.2.2020, COM (2020) 65 p. 1;
[55] Cit. "OECD AI Principles overview" sito disponibile al link: https://oecd.ai/en/ai-principles ;

danni a persone e/o cose. Il termine giustizia può essere anche tradotto con il concetto di equità e non discriminazione. Il principio di autonomia riguarda sia individui che robot, infatti si riferisce all'abilità della macchina di agire allontanandosi dalle istruzioni del programmatore e del controllo che l'uomo dovrebbe mantenere sul suo processo. In particolare, sarà sempre l'essere umano ad avere il potere di "decidere di decidere," ossia di stabilire in quali circostanze e casi specifici delegare l'analisi al dispositivo e quando, invece, è più opportuno l'intervento diretto dell'uomo e della sua discrezionalità. Infine, la trasparenza investe due profili del funzionamento dell'IA: la sua intelligibilità[56], ossia la capacità di comprendere la logica e i fatti posti alla base di una decisione, nonchè la possibilità di identificare la causa del malfunzionamento e ripartire correttamente le responsabilità per i danni arrecati dai sistemi di IA[57].

Il recepimento dei principi etici in linguaggio di programmazione può comportare diversi errori ed abusi. Floridi ha infatti individuato cinque principali categorie di rischi osservati nel tentativo delle aziende di introdurre le direttive etiche nel processo di produzione e training dell'IA. Il primo, nominato Ethic Shopping, consiste nella tendenza degli operatori di scegliere i singoli dettami da adottare in base al loro preesistente condotta al fine di legittimarla. L'Ethic Bluewashing (termine analogicamente ispirato dal greenwashing) consiste in una particolare forma di misinformazione che utilizza messaggi pubblicitari o dichiarazioni pubbliche non fondate per accrescere la reputazione "morale" dell'azienda e fuorviare consumatori e finanziatori. Un abuso istituzionale dell'etica dell'IA si è verificato anche nelle discussioni parlamentari e governative per l'adozione di atti legislativi e di soft law sull'IA al fine di ritardarne l'emanazione o renderli meno efficaci configurando il cd. Ethics Lobbying. Ulteriore conseguenza della molteplicità di codici di condotta e della loro frammentaria applicazione è la possibile esportazione di software sviluppati applicando standard etici minori in mercati arretrati e meno tutelati, fenomeno denominato Ethic Dumping. Inoltre, le divergenze aumentano considerando che continenti diversi spesso promuovono valori differenti. Ad esempio, le priorità legislative di Cina, UE e Stati Uniti divergono significativamente sui beni da

[56] S. Wachter, B. Mittelstadt, L. Floridi, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in International Data Privacy Law, Volume 7, 2017, 76;

[57] Per un'analisi comparata dei principali codici etici per l'IA vedi L. Floridi, *A Unified Framework of Ethical Principles for AI*, in Op. cit.

tutelare nei confronti dell'IA generativa. Parallelamente, l'ulteriore conseguenza dell'applicazione regionale e non condivisa dei principi consiste nello sviluppo di sistemi di IA meno accurati e sicuri e la loro vendita in aree geografiche meno avanzate dal punto di vista tecnologico, che quindi saranno maggiormente predisposte ad accettare tecnologie meno avanzate per un minor costo. Infine, si paventa il rischio di Ethics Shirking ossia l'elaborazione di standard meno gravosi per la valutazione etica di algoritmi operanti in settori dove la loro applicazione si prospetta particolarmente conveniente[58].

In definitiva la stesura di codici di condotta per gli operatori di IA costituisce il primo passo verso una regolazione del fenomeno, infatti la riflessione etica sottende sempre i precetti legali, contribuisce alla selezione dei valori da tutelare e consente di ottenere maggior consenso dei cittadini. In altri casi giocano un ruolo meramente direttivo/interpretativo, come l'elenco dei sette principi etici[59] non vincolanti menzionato dall'Artificial Intelligence Act dell'Unione Europea che dovrebbero contribuire «all'elaborazione di un'IA coerente, affidabile e antropocentrica». In generale è possibile osservare che la condivisione limitata e l'incoercibilità dei suddetti codici etici potrebbero determinare un basso tasso di efficacia, soprattutto in un mercato globalizzato dove processo produttivo, training, vendita e successivo monitoraggio dei sistemi di IA vengono svolti in regioni con standard e legislazioni diverse.

[58] L. Floridi, *From Principles to Practices-The Risks of Being Unethical*, Op. cit.;
[59] Il Considerando n. 27 del del 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) recepisce i sette principi elaborati dall'HLEG: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità;

Capitolo II
Il quadro normativo europeo sull'Intelligenza Artificiale

1) Il GDPR, primo tentativo di regolazione dell'IA

I sistemi di IA hanno rivoluzionato il di trattamento dei dati personali attraverso un ulteriore e superiore livello di automazione. Il deep learning permette all'IA di performare autonomamente tutte le fasi del trattamento dati: scelta delle informazioni, criteri di elaborazione, svolgimento del processo, elaborazione dell'outcome[60]. Queste caratteristiche hanno sollevato numerose preoccupazioni legate all'IA e all'impenetrabilità del processo di selezione dei dati e dei criteri logici utilizzati per elaborare il singolo responso, tanto da definirla una vera e propria black-box. D'altronde, come evidenziato nel paragrafo precedente, organizzazioni governative e non hanno elaborato linee guida per uno sviluppo etico dell'IA nelle quali enunciano tra i principali obiettivi la trasparenza e l'intellegibilità dei software. In verità l'Unione Europea aveva già cercato di raggiungere questi obiettivi nella governance delle nuove tecnologie attraverso il General Data Protection Regulation, che regola le modalità di trattamento dei dati personali. I Big Data e l'IA sono, infatti, indissolubilmente legati, i primi perché abbisognano di un algoritmo per essere analizzati, in quanto l'uomo impiegherebbe troppo tempo per studiare quel volume di dati, la seconda perché deve ai dati la sua stessa esistenza. Ciò che ha permesso lo sviluppo dell'IA accanto all'avanzamento tecnologico in diversi campi dell'informatica e dell'ingegneria è la disponibilità di set di dati su cui allenare gli algoritmi. È dunque oggi possibile apprezzare maggiormente la lungimiranza del legislatore europeo nell'emanare il GDPR, inquadrandolo come il primo tentativo di regolazione dell'IA, essendo questa interamente basata sul trattamento dei dati.[61].

---

[60] S. Wrigley, *Taming Artificial Intelligence: "Bots," the GDPR and Regulatory Approaches*, in M. Corrales et al. (eds.), Robotics, AI and the Future of Law, Perspectives in Law, Business and Innovation, p. 183;

[61] A. J. Wulf e O. Seizov, *Artificial Intelligence and Transparency: a blueprint for improving the Regulation of Ai application in EU*, in *EBLR*, 2020, 612;

Scopo del regolamento è quello di agevolare lo sviluppo di un mercato dei dati, necessario per lo sviluppo di un'economia digitale europea, attraverso un quadro normativo certo e uniforme. Questo scopo prettamente economico deve tuttavia essere realizzato tutelando il diritto dei cittadini europei alla tutela dei propri dati personali, così imponendo un bilanciamento che deve sempre presupporre che «il trattamento dei dati personali [debba] essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»[62]. La lettura in combinato disposto dei due recitals evidenzia il bilanciamento che sottende l'attività di trattamento dei dati personali: da un lato riconosce l'implicazione di diversi valori morali e sociali, mentre dall'altro emerge l'interesse economico di quest'attività di business. La contraddizione, infatti, è solo apparente in quanto il riconoscimento del diritto non impedisce ai diretti interessati di disporne, al contrario, il clima di fiducia creato dal regolamento consentirà lo sviluppo dell'economia digitale[63] nel mercato europeo. La fiducia del pubblico è ottenuta proprio grazie al maggior controllo sui dati garantito dal GDPR, durante tutte le fasi di trattamento dei dati.

Il trattamento è legittimo qualora autorizzato dall'interessato o previsto dalla legge, in entrambi i casi l'interessato ha il diritto di ricevere informazioni chiare sul titolare del trattamento e sulle principali caratteristiche dell'analisi dati (finalità del trattamento, delle modalità e della durata della conservazione dei dati). Oltre ai diritti informativi il controllo sui dati prevede il diritto dell'interessato di revocare il consenso ed interrompere il trattamento, il diritto di rettificare i dati non aggiornati ed il diritto al risarcimento dei danni materiali ed immateriali per violazione di tali prescrizioni. Accanto ai diritti dell'interessato riconosciuti dal GDPR, questo inaugura il principio di accountability che impone al titolare del trattamento l'obbligo di valutare i rischi dell'attività di analisi dei dati e predisporre preventivamente misure per prevenirli, ridurli e permettere il ripristino del corretto funzionamento. Il sistema di tutela introdotto dal GDPR contempla strumenti preventivi e reattivi che sostanziano il principio di accountability ed il principio di privacy "by design and by default" che impone al titolare del trattamento di strutturare l'attività

[62] Cit. Considerando n. 4 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
[63] Considerando n. 7 Regolamento (UE) 2016/679;

di trattamento «mette[ndo] in atto misure tecniche e organizzative adeguate (…) al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati»[64]. Pertanto, alla luce della breve analisi del regolamento, si possono distinguere due principali approcci normativi il primo, di carattere generale in quanto applicabile a tutti i tipi di trattamento, è costituito dalle prescrizioni sui diritti degli interessati e basi giuridiche del trattamento, mentre il secondo prevede una forma di co-regolazione[65]. Infatti, come sopra anticipato, il regolamento non esplicita quali misure dovranno essere adottate da ciascun titolare ma lascia a quest'ultimo la scelta dei protocolli e misure di sicurezza più adatti al caso concreto, secondo la logica della responsabilizzazione propria dell'accountability. Infine, una terza opzione per la regolamentazione dell'IA propone un modello giuridico basato su disposizioni specifiche per disciplinare ciascun tipo di trattamento. La sezione quarta del regolamento costituisce un esempio di questo approccio, in quanto regola specificatamente i processi decisionali automatizzati, ossia trattamenti dai quali scaturiscano decisioni basate unicamente sul trattamento automatizzato. Il trattamento è completamente automatizzato qualora venga svolto in totale assenza di intervento umano o dove tale contributo «risulti artefatto e sia irrilevante ai fini della decisione»[66]. La tutela prevede «il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[67]. I rimedi previsti dal dispositivo consentono all'interessato «di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[68]. Dal citato dispositivo è possibile rilevare la lungimiranza del legislatore europeo, attento ad impedire che decisioni di rilevante portata sulla vita degli individui vengano elaborate su una base conoscitiva limitata e senza alcun tipo di controllo umano[69]. La disposizione, in principio preposta a tutelare gli utenti rispetto alla pratica della profilazione, oggi costituisce l'unico

[64] Cit. Art 25, 1° comma Regolamento 679/2016;
[65] S. Wrigley, *Taming Artificial Intelligence: "Bots," the GDPR and Regulatory Approaches*, Op. cit. p.185;
[66]Cit. A. Moretti, *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679*, in *Dir. Inform.*, 2018, p. 808;
[67] Cit. par 1 art. 22 del Regolamento 679/2016;
[68] Vedi Supra;
[69] Cfr. A. Ricci, *I diritti dell'interessato*, in Aa. Vv. G. Finocchiaro (a cura di), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, Zannichelli, 2017, p. 243;

strumento normativo che permetterebbe l'apertura della black-box: infatti gli artt. 13 e 15 del regolamento prevedono, per i trattamenti automatizzati la possibilità di chiedere informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste. Infatti, proprio invocando le citate disposizioni la letteratura ha ipotizzato l'esistenza di un right to explanation, ossia «the right to obtain human assessment and an explanation of the decision reached after such assessment»[70]. Tuttavia, gli artt. 13 e 15 del GDPR garantiscono solo le «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato», pertanto non comprendono anche i criteri e le ragioni che hanno motivato il singolo responso, consentendo all'interessato di accedere solo alla logica di funzionamento generale del software. Soltanto il Considerando 71 menziona effettivamente il diritto ad ottenere «una spiegazione della decisione conseguita dopo tale valutazione», tuttavia il dettato non ha valore vincolante, ma è meramente indicativo della soluzione interpretativa adottabile; pertanto, non può garantire un effettivo righ to explanation.

Il GDPR pone quindi gli strumenti per poter potenzialmente rivendicare un controllo dei propri dati rispetto all'utilizzo dell'IA e alla possibilità di essere sottoposti a decisioni discriminatorie o non pertinenti; tuttavia, la sua efficacia è dibattuta. In particolare, è possibile rilevare un'inconciliabilità tra il trattamento svolto dall'IA ed alcuni requisiti di liceità del trattamento previsti dal GDPR, tra i quali: il libero consenso al trattamento, la determinazione ex ante delle finalità perseguite e il principio di minimizzazione dei dati. La libertà del consenso può dirsi compromessa in presenza di tutti i prodotti o servizi che operano tramite e/o integrano il proprio funzionamento con software di IA, e che obbligano il consumatore ad aderire al trattamento per goderne. Il consenso al trattamento deve essere espresso in relazione a finalità predeterminate, tuttavia il sistema di autoapprendimento soggetto a continue modifiche determinate da impulsi esterni non consente di predeterminarle in modo specifico. Le inferenze raggiunte tramite sistemi di deep learning sfuggono al controllo umano e alla sua previsione, pertanto non è possibile

[70] Cfr. S. Wachter B. Mittelstadt, L. Floridi , *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation* , in *International Data Privacy Law*, Volume 7, 2017, 76. L'autore, analizzando le disposizioni del GDPR, ha prospettato diverse ricostruzioni di un diritto alla spiegazione delle decisioni ottenute tramite l'analisi automatizzata di dati. La conclusione alla quale perviene è che non sussiste un vero e proprio obbligo del titolare a dover fornire una giustificazione sui risultati del proprio trattamento, sebbene queste incidano in modo rilevante sulla persona. Ritiene quindi che la tutela fornita dal Regolamento EU 679/2016 nasca "monca".

comunicare in modo puntuale come i singoli dati verranno trattati ed impiegati. Per la stessa ragione non è rispettato anche il principio di minimizzazione dei dati, in quanto il sistema di IA utilizza i dati forniti non solo per avviare un procedimento ma anche e soprattutto per accrescere la propria banca dati e le proprie inferenze logico-statistiche[71].

Il principio di minimizzazione dei dati impone al titolare del trattamento l'utilizzo di dati personali strettamente necessari per raggiungere la finalità predeterminata. Di fatto, la debolezza della norma dipende dall'aver affidato alle parti il compito di garantirne l'effettività, *in primis* al titolare che predispone il design del trattamento e, poi, degli interessati che dovranno agire in caso di violazione[72]. Sebbene il Garante per la protezione dei dati personali abbia il compito di interpretare e accertare il rispetto delle disposizioni sulla privacy, l'ente non ha le risorse necessarie per garantire l'accertamento capillare delle violazioni; non vanta collegamenti con gli esperti e consulenti del settore che potrebbero, invece, essere validi aiuti nell'indagare possibili illeciti ed elaborare metodi alternativi di compliance[73].

Ebbene, ai sensi del GDPR, possiamo considerare responsabili del trattamento dati, e dell'intero funzionamento dei sistemi di IA, sia gli operatori di front-end, che decidono di avvalersi dell'IA e ne traggono beneficio, sia operatori di back-end, che hanno programmato e definito il software; entrambi trattano dati, ma per una finalità diversa: il primo per ottenere il risultato per il quale il programma è stato creato, il secondo per sviluppare il software. La responsabilità, ed il compito di chiarire la logica utilizzata dall'algoritmo, potrebbe quindi essere addebitati sia al produttore/programmatore che all'acquirente, che impiega il software per l'esercizio della propria impresa[74].

Condizione per azionare i diritti *ex* GDPR nei confronti del titolare è il trattamento di dati personali, ossia tutte le informazioni riferibili ad un individuo; pertanto, l'utilizzo da parte dell'IA di dati anonimizzati non darebbe titolo per agire in quanto non riferibili al soggetto. Sul punto, però, si deve rilevare che i dati anonimizzati sono sempre soggetti al

[71] Sui difetti dell'istituto del consenso ex GDPR in relazione all'utilizzo di sistemi di IA vedi A. Astone, *Autodeterminazione nei dati e sistemi A.I.,* in Contratto e Impresa, 2022, p. 434;
[72] A. J. Wulf , O. Seizov, *op. cit.*
[73] S. Degli Esposti e E. Mocholi Ferrandiz, *After the GDPR: Cybersecurity is the Elephant in the Artificial Intelligence Room*, in *EBLR*, 2021, p. 21;
[74] A. Neri, *Uso di un algoritmo discriminatorio nella contrattazione privata*, in *Nuova Giur. Civ. Comm.*, 2021, p. 983;

pericolo di re-identificazione, che potrebbe sopravvenire a causa dell'inserimento di maggiori informazioni sul medesimo soggetto all'interno del data set; se tale pericolo si dovesse verificare l'interessato avrebbe nuovamente diritto a tutte le informazioni relative al trattamento. Non solo, come anticipato, l'IA è preposta ad elaborare previsioni tramite processi inferenziali, le nuove informazioni così ottenute saranno anch'esse considerate dati personali, qualora riferibili ad un singolo soggetto. Tuttavia, si ricorda che il diritto di opporsi o contestare il trattamento è comunque limitato ai soli casi in cui la decisione automatizzata comporti effetti giuridici, o comunque un impatto significativo sulla persona, come ad esempio nel caso in cui l'algoritmo sia preposto ad elaborare diagnosi[75], profili di clienti sui quali basare una proposta contrattuale[76] oppure provvedimenti amministrativi[77].

Insomma, il GDPR rappresenta il primo passo verso una regolazione delle nuove tecnologie che basano il loro funzionamento sull'elaborazione dei dati. Sebbene la norma sia stata ritenuta un ostacolo per la competitività dell'Unione Europea nel mercato delle nuove tecnologie, potrebbe invece rappresentare un passo in avanti rispetto a Stati che non hanno ancora regolato il settore e che si troveranno a dover fronteggiare le prime class actions. Infatti, una delle caratteristiche del GDPR è la genericità con cui sono state definite le misure e gli standard, che per essere attuati richiedono un bilanciamento tra l'interesse del titolare a trattare i dati e la volontà degli interessati a non essere soggetti al trattamento. In questa prospettiva sarebbe più utile aiutare i titolari, nella scelta delle misure da attuare e potenziare l'apparato amministrativo di settore, per aumentare i controlli ed emanare linee guida che riducano *ex ante* la discrezionalità dei titolari. Il trattamento svolto dall'intelligenza artificiale implica invece un bilanciamento tra interessi individuali e collettivi, come quello generale allo sviluppo di nuove tecnologie. Infatti, lo scopo dell'algoritmo non sono più i dati dei singoli individui, bensì le previsioni da questi deducibili. Pertanto, i dati anonimizzati costituiscono il mezzo per giungere ad un fine scientifico più ampio, il quale non incide direttamente sulla persona[78]. Il limite del regolamento risiede nell'aver disciplinato i dati esclusivamente da una prospettiva non

[75] G. Pasceri op. cit.;
[76] A. Neri, Op. cit. p. 4;
[77] A. Masucci, *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Giappichelli Editore, Torino, 2011;
[78] G. Proietti, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in *Contr. impr.*, 2022, 895;

patrimoniale, ignorando che il modello di business predominante nell'economia digitale si basi sull'utilizzo dei dati come corrispettivo per l'accesso a beni e servizi offerti su internet. Le piattaforme ed i motori di ricerca sfruttano i dati per molteplici finalità; ad esempio, trattano dati dell'utente per l'esecuzione del contratto, per finalità di marketing e profilazione, per svolgere analisi predittive utili per anticipare trend di mercato consentendo di elaborare strategie di business più efficaci. I propositi economici della norma sono stati in parte riconosciuti dalla la giurisprudenza che, nonostante abbia definito il dato quale *res extra commercium*, ha preso atto della progressiva «patrimonializzazione del dato» nei contratti che autorizzano il trattamento dei propri dati personali per finalità di marketing in cambio di servizi o prodotti[79]. Se il singolo dato riveste un valore infinitesimale, la raccolta e il trattamento dei Big Data costituisce la ricchezza e il petrolio dell'economia digitale[80].

2) Artificial Intelligence Act: processo legislativo, principi definitori e struttura normativa

Il Regolamento EU sull'Intelligenza Artificiale (AI Act) costituisce un primo esempio di bilanciamento tra i rischi e i benefici implicati dai nuovi sistemi di IA. Lo scopo del Regolamento è quello di promuovere lo sviluppo e il commercio di tecnologie intelligenti nel mercato unico, ed al contempo assicurare ai cittadini dell'UE software affidabili e sicuri ed un alto livello di protezione dei diritti fondamentali[81]. Il processo legislativo che ha portato all'adozione dell'AI Act è iniziato nell'aprile 2021 con la proposta della Commissione europea di un atto che uniformasse le norme nel mercato unico europeo sui prodotti e servizi resi tramite IA. In particolare, la Commissione proponeva una propria definizione di sistema di IA e un sistema di governance basato su quattro classi di rischio: inaccettabile, alto, limitato e minimo. Il Consiglio europeo è intervenuto nel dicembre del 2022 inserendo disposizioni specifiche per l'IA per finalità generali, o meglio conosciuta

[79] A. Astone, Autodeterminazione nei dati e sistemi A.I., Op. cit. p. 435 che commenta la sentenza del Cons. Stato, 29 marzo 2021 n. 2631;
[80] The Economist, *The world's most valuable resource is no longer oil, but data*,6 maggio 2017;
[81] F. Di Ciommo, C. Scarpellino, Le priorità della Presidenza italiana del G7 sull'Intelligenza Artificiale, p. 8, disponibile al link: https://sog.luiss.it/it/node/4253 ;

come IA generativa, ed escludendo dall'ambito di applicazione del regolamento determinati settori come quello della sicurezza nazionale, difesa, forze dell'ordine e scopi militari. Infine, Parlamento e Consiglio europeo hanno raggiunto un accordo provvisorio sul testo di legge da adottare nel dicembre 2023 includendo le categorie di IA generativa ad alto rischio e distinguendo i sistemi di IA a rischio limitato, che presentano criticità in punto di trasparenza, dai sistemi che invece comportano un rischio minimo ai quali verrà imposto soltanto il rispetto della normativa europea previgente, come il GDPR. Dopo l'approvazione separata di Parlamento europeo e Consiglio l'AI Act è stato firmato il 13 giugno 2024 ed entrato in vigore il 1° agosto 2024[82].

L'ambito di applicazione del regolamento comprende tutti i sistemi di IA prodotti e commerciati nel mercato europeo. La nozione di sistema di IA adottata dal legislatore europeo si basa sulle principali caratteristiche della tecnologia intelligente e che la distingue dai software tradizionali con limitate capacità di automatizzazione. Infatti, per IA il regolamento intende «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»[83]. Questa formulazione, suggerita dal Parlamento, si allinea con la nozione di IA adottata dall'OCSE con il dichiarato scopo di «di garantire la certezza del diritto [ed] agevolare la convergenza internazionale e un'ampia accettazione»[84]. La formulazione volutamente ampia della fattispecie è stata avvallata con l'intento di includere tutte le possibili manifestazioni del fenomeno concentrandosi sugli elementi di rischio di questa tecnologia, ossia: la capacità di autoapprendimento, la molteplicità di obiettivi perseguiti e l'autonomia[85]. Questa capacità può manifestarsi con livelli di

[82] Parlamento europeo, Legislative Train for a Europe fit for a Digital Age, giugno 2024, disponibile al link: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence ;
[83] Cit. art. 3, 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), disponibile al link: https://eur-lex.europa.eu/legal-content/MT/TXT/?uri=CELEX:32024R1689;
[84] Cit. Considerando n. 12 del 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);
[85] L'elenco è stato utilizzato dal Considerando n. 12 del 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);

autonomia variabili, non è quindi necessaria la completa automatizzazione del processo perché il sistema venga considerato intelligente. Infine, il regolamento sottolinea la distinzione tra gli obiettivi impliciti ed espliciti perseguiti dai sistemi di IA, in quanto le finalità attribuite al software nel contesto di riferimento e gli obiettivi per il quale l'algoritmo è stato programmato possono differire. Un esempio che chiarisce questa circostanza può essere rinvenuto nel funzionamento di un software di raccomandazione dei contenuti di una piattaforma di streaming, volta a massimizzare il loro tempo di visualizzazione, indirizzando verso altri contenuti che li trattengano in più a lungo possibile sulla piattaforma.

L'ambito di applicazione così definito risulta molto ampio, andando ad includere una vastissima gamma di sistemi, al netto del fatto che va ad incidere sia sulla vendita di dispositivi, sia all'offerta di servizi eseguiti tramite software di IA, indipendentemente dalla loro ubicazione[86]. Tuttavia, è bene precisare che sebbene i sistemi di IA possano essere distribuiti sia sotto forma di servizio (come le applicazioni deputate allo svolgimento di determinate prestazioni) sia nella forma di prodotto, quale semplice software o software supportato da una componente hardware, il legislatore europeo ha ritenuto la qualificazione di prodotto più adatta alla natura di questi sistemi. Questa scelta poggia su tre ordini di motivi: l'equivalenza funzionale di tutti i sistemi di IA avrebbe garantito un'uniformità applicativa del regolamento, precedenti disposizioni europee[87] avevano già qualificato device dotati di IA quali prodotti, infine tale qualificazione avrebbe permesso di adottare il consolidato schema normativo europeo sulla sicurezza dei prodotti[88].

In tale contesto, l'ampia formulazione della fattispecie è stata inevitabile, data la scelta dell'AI Act di adottare un approccio normativo orizzontale applicabile a qualsiasi

[86] Il Considerando n° 22 prevede la circostanza in cui «è opportuno che determinati sistemi di IA rientrino nell'ambito di applicazione del presente regolamento anche quando non sono immessi sul mercato, né messi in servizio, né utilizzati nell'Unione. È il caso, ad esempio, di un operatore stabilito nell'Unione che appalta alcuni servizi a un operatore stabilito in un paese terzo in relazione a un'attività che deve essere svolta da un sistema di IA che sarebbe classificato ad alto rischio.»;

[87] Qualificano l'IA quale prodotto i seguenti atti normativi in materia di dispositivi medici: Direttiva 93/42/CEE del Consiglio, del 14 giugno 1993, concernente i dispositivi medici e i nuovi regolamenti 2017/745 e 2017/746 sui dispositivi medico-diagnostici in vitro;

[88] G. Mazzini, S. Scalzo, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts,* in Camardi (a cura di), *La via europea per l'Intelligenza artificiale,* 2023, p.3 Disponibile al link SSRN: https://ssrn.com/abstract=4098809 or http://dx.doi.org/10.2139/ssrn.4098809;

sistema di IA, indipendentemente dal tipo di prestazione o dalla finalità perseguita. L'elemento distintivo delle fattispecie adottato dal regolamento è il rischio potenziale generato dal sistema di IA. In base a ciascun livello di rischio, il regolamento stabilisce regole di diversa intensità e portata. Il sistema di governance può essere idealmente rappresentato da uno schema piramidale, in cui il livello più alto è occupato dai sistemi che implicano pratiche di IA vietate (art. 5), seguiti dai sistemi ad alto rischio (art. 6), dai modelli di IA a scopo generale con rischio sistemico (art. 51), dai GPAI senza rischio sistemico (art. 53) e infine dai sistemi con rischio trascurabile (art. 50).

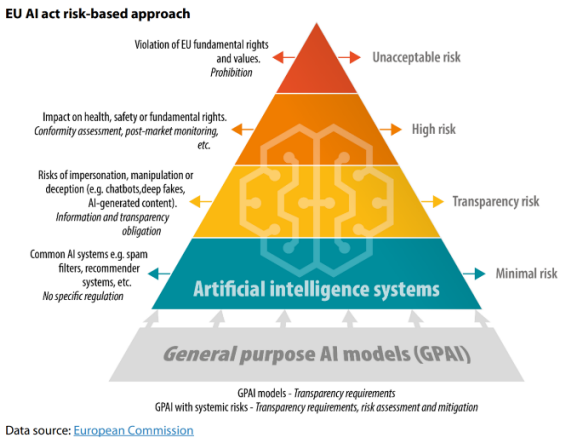

Figura 4. Schema piramidale che illustra i livelli di rischio previsti dall'AI Act.

In primis il regolamento evidenzia tutte le pratiche che comportano pericoli "inaccettabili" per la dignità umana, la libertà, la democrazia, lo Stato di diritto e i diritti fondamentali. Quindi sono proibiti nel mercato unico tutti i sistemi di IA che utilizzino tecniche subliminali, sfruttino le vulnerabilità delle persone più fragili, assegnino un punteggio sociale agli individui, valutino la propensione a commettere reati, utilizzino dati biometrici per profilare la popolazione o permettano l'identificazione biometrica remota "in tempo reale" nei luoghi pubblici[89]. Sono qualificati, invece, ad alto rischio i device che possono comportare un «impatto nocivo significativo» alla salute, alla sicurezza e ai diritti fondamentali. Il regolamento li identifica nei sistemi per i quali sono

[89] Art. 5 del 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);

già stati imposti standard di sicurezza da leggi speciali di cui all'allegato I[90] e in quelli operanti nei settori indicati dall'Allegato III.

Sistemi destinati alla gestione di infrastrutture critiche	I sistemi di IA destinati a essere utilizzati come componenti di sicurezza ai fini della gestione e del funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità
Sistemi biometrici	I sistemi di identificazione biometrica remota, i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti e i sistemi di IA destinati a essere utilizzati per il riconoscimento delle emozioni.
Sistemi destinati alla gestione del merito creditizio	I sistemi di IA utilizzati per valutare il merito di credito o l'affidabilità creditizia delle persone fisiche
Sistemi di IA per la giustizia	I sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o per suo conto per assistere le autorità giudiziarie nelle attività di ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti
Sistemi di IA utilizzati nelle elezioni	I sistemi di IA destinati a essere utilizzati per influenzare l'esito di elezioni o referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum

Tabella 2. Elenco di alcuni sistemi di IA ad alto rischio secondo l'AI Act.

[90] Secondo l'art. 6 il sistema è ad alto rischio se già «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.»;

I modelli di IA per finalità generali, o IA generativa, sono sviluppati attraverso un addestramento «con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti»[91]. La distinzione tra IA semplice e IA generativa è evidenziata dalle caratteristiche funzionali di quest'ultima. La definizione di IA generativa fa riferimento alla vasta gamma di dati o parametri utilizzati e alla capacità di svolgere un elevato numero di compiti distinti. Un'altra particolare caratteristica riguarda, invece, la varietà di outcome in grado di generare contenuti di testo, audio, immagini o video.

La categoria dell'IA per finalità generali si caratterizza per le capacità particolarmente elevate di questi sistemi, in considerazioni delle quali è stata predisposta una sottocategoria: l'IA per finalità generali con rischio sistemico. Il rischio sistemico si riscontra in tutti quei sistemi che registrano «un impatto significativo sul mercato interno a causa della loro portata»[92]. La presenza di rischio sistemico viene accertata valutando le caratteristiche del sistema alla luce di tutte le fasi di produzione dell'IA generativa. In particolare, si osservano: il processo di training dell'IA svolto prima della sua diffusione sul mercato (come il pre-addestramento, la generazione di dati sintetici ed il perfezionamento). Nonché le prestazioni del sistema valutate sulla base della velocità di calcolo (numero di operazioni in virgola mobile[93] che possono essere compiute in un secondo) e della «qualità o dele dimensioni del set di dati di addestramento, il numero di utenti commerciali e finali, le sue modalità di input e output, il suo livello di autonomia e scalabilità o gli strumenti a cui ha accesso»[94]. Sulla base delle metriche sopra menzionate, una volta identificata la fattispecie di rischio, vengono applicati requisiti e obblighi di carattere generale per ciascuna di esse; ad esempio, i requisiti imposti dall'AI Act ai sistemi di IA ad alto rischio impongono:

[91] Cit. Art. 3 del testo "Emendamenti Del Parlamento Europeo alla proposta della Commissione";
[92] Cit. Considerando n. 111 del 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);
[93] In, particolare viene fissata una «soglia iniziale di operazioni in virgola mobile che, se raggiunta da un modello di IA per finalità generali, porta a presumere che il modello sia un modello di IA per finalità generali con rischi sistemici» (Considerando n. 111). La soglia è attualmente pari a 10 alla venticinquesima, tuttavia la Commissione ha il potere di modificare le soglie in considerazione degli sviluppi tecnologici;
[94] Cit. Vedi Supra;

- **sistema di gestione dei rischi** per identificare e analizzare tutti i rischi prevedibili al fine di mitigarli o eliminarli (art. 9);
- **dati e governance dei dati** per gestire l'utilizzo dei dati nel processo di addestramento, convalida e prova del funzionamento dell'IA e assicurare che i data base usati siano pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista (art. 10);
- **documentazione tecnica** per dimostrare la conformità del sistema di IA ai requisiti dell'AI Act (art. 11);
- **conservazione delle registrazioni** che consenta la registrazione automatica degli eventi ("log") per la durata del ciclo di vita del sistema (art. 12);
- **trasparenza e fornitura di informazioni ai deployer** per garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai deployer, autorità pubblica, agenzia che utilizza un sistema di IA sotto la propria autorità, di interpretare l'output del sistema e utilizzarlo adeguatamente. Devono essere allegate informazioni sull'identità del fornitore e istruzioni per l'uso che contengano tutte le informazioni rilevanti in merito a scopi dell'IA, livello di accuratezza e qualsiasi circostanza nota o prevedibile nella quale il sistema determini un rischio per i diritti fondamentali (art. 13);
- **sorveglianza umana** compiuta attraverso strumenti di interfaccia uomo-macchina che consentano alle persone fisiche alle quali è affidata la sorveglianza umana di avere la possibilità di monitorarne debitamente il funzionamento; anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese. Le misure di sorveglianza includono il potere di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio nonché la possibilità di interrompere tramite un pulsante di "arresto" il funzionamento del device (art. 14);
- **Accuratezza, robustezza e cibersicurezza** l'IA deve accludere nelle istruzioni il livello di accuratezza dei suoi responsi, includere piani di backup o fail-safe, ridurre il rischio di feedback loops (output potenzialmente distorti che influenzano gli input per operazioni future);

Un sistema è pertanto ritenuto sicuro, ed è libero di circolare in UE, se rispetta I requisiti sopracitati. Inoltre, il regolamento impone ai fornitori l'obbligo (art. 16) di

garantire che i loro sistemi di IA ad alto rischio siano conformi ai requisiti menzionati. La liceità del sistema viene dimostrata con il possesso di requisiti formali e sostanziali. I primi concernono l'osservanza della procedura di valutazione di conformità (artt. 17, 23), della necessaria marcatura CE e della registrazione presso le banche dati europee (art. 49). Costituiscono requisiti sostanziali l'implementazione di un sistema di gestione della qualità che curi il rispetto dei requisiti e l'adeguatezza delle misure di sicurezza adottate durante tutto il ciclo di vita del device, nonché la redazione di una valutazione di impatto (art. 17). Il fornitore deve inoltre conservare la documentazione tecnica obbligatoria per la durata di 10 anni (art. 18), e la registrazione degli eventi (*log*) per 6 mesi (art. 19). Lo stesso si impegna ad adottare misure correttive o ritirare e disabilitare il device sul mercato che non rispetti gli standard imposti (art. 20).

Per tutti gli altri sistemi, classificati nelle categorie di rischio inferiori a quelle citate, ma che interagiscono direttamente con le persone, sono previsti obblighi di trasparenza. Questi obblighi servono a garantire che gli utenti siano consapevoli di interagire con un sistema di IA; ad esempio rivelando l'origine artificiale di contenuti audio, immagine, video o testuali, apponendo una speciale etichetta. Mentre i sistemi di IA residuali, che non sono schedati quali ad alto rischio, si applicano le altre norme speciali previste dall'ordinamento europeo e nazionale come il GDPR (art. 50).

La strategia normativa adottata dall'AI Act non prescrive specificamente le misure che i fornitori devono adottare, ma fornisce linee guida generali su come produttori e commercianti devono garantire la sicurezza e l'affidabilità dei dispositivi. Ad esempio, il sistema di gestione dei rischi previsto dal regolamento richiede l'identificazione e l'analisi dei rischi noti o prevedibili, la stima e la valutazione di tali rischi, e l'adozione di misure di gestione adeguate e mirate. Tuttavia, il regolamento non specifica come debbano essere condotte queste valutazioni né quali misure debbano essere adottate. La scelta delle concrete misure da adottare ricade infatti sul produttore, *in primis*, ed in seconda istanza sul fornitore e deployer. Questa soluzione è nota ai legislatori come una particolare tecnica normativa, la cd. co-regolazione, che affida il potere di regolare una materia sia allo Stato sia ai privati coinvolti nel settore. Questa tecnica si pone quale soluzione intermedia tra il tradizionale modello di regolazione top-down, ovvero dall'alto, e i più moderni strumenti di bottom-up regulation. Rientrano nella prima categoria di strumenti le leggi e i regolamenti che contengano specifici obblighi ed istruzioni, mentre

appartengono al secondo gruppo codici di condotta, linee guida e strumenti di self-regulation normalmente adottati in forma volontaria da stakeholders del settore, organizzazioni non governative o associazioni di imprese[95]. Il middle-out approach invece si caratterizza per l'utilizzo nel medesimo schema regolatorio di entrambi gli approcci, includendo norme primarie che prescrivono i principi generali della materia, applicabili alla generalità degli obbligati, e norme secondarie, che delegano ai privati il potere di individuare le concrete azioni con le quali realizzare/rispettare i suddetti principi. L'utilizzo di formule più ampie della tradizionale norma "se A allora B", consente di trovare più facilmente un bilanciamento tra più atti normativi che intervengono sulla materia con ambiti di applicazione sovrapposti.

Questa particolare forma di co-regolazione, quale insieme di norme primarie e secondarie, era già prevista dal GDPR. In particolare, attraverso l'applicazione dei principi di privacy by design e by default il legislatore europeo ha trasferito in prima istanza a fornitori e produttori l'obbligo di identificare i rischi ragionevolmente prevedibili derivanti dall'utilizzo del sistema di IA, in base al contesto di riferimento ed alle istruzioni impartire dal produttore. Incombe quindi sul produttore la predisposizione di misure tecniche e organizzative finalizzate ad eliminare, o anche soltanto ridurre, la probabilità che il rischio si verifichi e la predisposizione di procedure o prassi che ù consentano di ridurre i danni causati dall'evento lesivo[96].

Invece il principio di accountability richiede che il fornitore si assuma la responsabilità del proprio operato e che ne dia conto, dimostrando di aver diligentemente rispettato, e come, gli obblighi di compliance by design and by default stabiliti dal regolamento. Questo approccio ha dimostrato di essere l'unico effettivamente praticabile per governare l'infinita varietà di software, che non permette la costruzione di una fattispecie unica e onnicomprensiva. Inoltre, la definizione di fattispecie troppo rigide e particolareggiate mal si adatterebbe al settore delle nuove tecnologie, dove la rapida evoluzione costringerebbe il legislatore ad intervenire continuamente per introdurre

[95] U. Pagallo, P. Casanovas e R. Madelin, *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*, in The Theory and Practice of Legislation, 2019, p. 2, disponibile al link: https://doi.org/10.1080/20508840.2019.1664543 ;

[96] Commissione UE, What does data protection 'by design' and 'by default' mean?, in https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en ;

nuove regolamentazioni. L'IA, in particolar modo, ha dimostrato la difficoltà di rincorrere uno strumento digitale con il veloce sviluppo dell'IA per finalità generali, completamente ignorata nella proposta della Commissione UE nel 2021, ha rivestito un'importanza centrale nelle successive versioni dell'atto; dimostrando come anche gli step evolutivi di una stessa tecnologia richiederanno interventi normativi ad hoc, qualora manifestino capacità e caratteristiche non affrontate dalla precedente legislazione.

Il middle out approach adottato nell'AI Act consente di raggiungere anche una maggiore efficacia normativa, dal momento che le obbligazioni imposte al fornitore incombono nella fase antecedente la verificazione del danno. Pertanto, il sistema di governance così costruito permette di sanzionare i soggetti responsabili per il solo illecito amministrativo per violazione della normativa di settore; ad esempio, per l'adozione di misure di sicurezza inadeguate o per informative sul trattamento poco chiare o fuorvianti. Tuttavia, non mancano opinioni contrarie secondo cui questo approccio non è applicabile alla governance dell'IA. I critici sostengono che manca un nucleo di principi condivisi, che i rischi e i danni potenziali dell'IA sono molto più vari rispetto a quelli contemplati nel GDPR e che esistono già diverse normative specifiche che regolano l'IA in determinati settori[97].

In conclusione, la società dell'informazione impone l'adozione di nuove regole, che non richiedano continui aggiornamenti, in modo da accompagnare il fisiologico avanzamento della tecnica, e consentire alle imprese di preventivare i costi giuridici e gli adempimenti burocratici grazie alla stabilità normativa, data da un quadro normativo chiaro. La certezza del diritto raggiungerà l'obiettivo parallelo di aumentare il flusso di investimenti. Il middle-out approach si propone quale soluzione intermedia rispetto l'inadeguatezza delle formule normative tradizionali perché capace di «adattarsi velocemente coinvolgendo le autorità, che definiranno un quadro normativo a tutela dei diritti civili, ed i privati che, in quanto primi responsabili della sicurezza dei sistemi, avranno tutto l'interesse ad elaborare nuovi protocolli tecnici per legittimare il lancio di

[97] sul punto U. Pagallo, P. Casanovas e R. Madelin, Op. cit. p. 13 chiariscono per quali ragioni il middle-out approach non costituisce una valida soluzione per la regolazione dell'IA: «three reasons suggest why this is not the case. First, we still lack a list of principles to be enforced through forms of co-regulation in all fields of AI, as occurs with Art. 5(1) of the GDPR. Second, the legal regulation of AI does not just concern personal data issues (e.g. non-discrimination law). Third, current AI regulation is already context-dependent: in addition to the rules on data protection, there are a multitude of rules in the fields of self-driving cars, drones, e-health, financial services, and more.»;

un nuovo prodotto tecnologico»[98]. Dall'altro lato, però, formule di indirizzo così generali scontano il prezzo dell'incertezza del diritto, soprattutto in assenza di best practice e linee guida che indichino per ciascun software le misure adeguate ad eliminare o a ridurre il rischio allo stato dell'arte. Inoltre, tali riflessioni devono essere messe in relazione con il principio della libera circolazione delle merci, che consente limitazioni al mercato libero soltanto se giustificate da ragioni imperative di interesse generale e proporzionate al livello di tutela perseguito[99].

3) La governance europea per l'Intelligenza Artificiale

Illustrato il reticolo di obblighi e requisiti imposti dall'AI Act, il presene paragrafo analizza i meccanismi di supervisione elaborati per affrontare e sanzionare le violazioni del suddetto regolamento. Il sistema di governance proposto dall'AI Act per l'intelligenza artificiale prevede un approccio centralizzato, che coinvolge istituzioni europee, autorità nazionali e organismi di certificazione. Il regolamento prevede che ciascuno Stato membro designi o istituisca «almeno un'autorità di notifica responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio»[100]. Le autorità nazionali sono preposte al controllo e coordinamento degli organismi di valutazione della conformità; pertanto, devono svolgere il loro ufficio assicurando indipendenza ed imparzialità. Inoltre, incombono sulle autorità nazionali doveri di comunicazione, sono deputate a notificare alla Commissione e agli altri Stati membri ogni organismo di valutazione della conformità.

Il principale obiettivo assegnato all'Autorità nazionale è assicurare che gli organismi siano capaci di svolgere le valutazioni di conformità sui sistemi per i quali si dichiarano

[98] Cit. C. *Scarpellino, Responsabilità nell'e-health,* in *Comparative Law Review* - Sostenibilità e innovazione: prospettive di diritto comparato Incontro di studi a cura dei giovani comparatisti dell'Associazione Italiana di Diritto Comparato – 13 maggio 2022 – Salerno, p.202;
[99] cit. F. Di Ciommo e C. Scarpellino, *Le priorità della Presidenza italiana del G7 sull'Intelligenza Artificiale*, Op cit. p. 9;
[100] Cit. Art. 28 del 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);

competenti. A tale scopo l'AI Act ha predisposto una procedura di notifica nel quale l'organismo di valutazione presenta una domanda di notifica all'Autorità nazionale dello Stato in cui è stabilito per ottenere l'autorizzazione ad operare quale ente di certificazione di sistemi di IA. La domanda di notifica contiene gli elementi per dimostrare la competenza ed adeguatezza dell'ente per la certificazione di sistemi di IA, a tal fine la domanda riporta una descrizione dell'«attività di valutazione della conformità, del modulo o dei moduli di valutazione della conformità e dei tipi di sistemi di IA per i quali tale organismo di valutazione della conformità dichiara di essere competente, nonché da un certificato di accreditamento»[101]. È importante considerare che, a causa della vasta e potenzialmente infinita varietà di sistemi di intelligenza artificiale, e della specifica expertise richiesta per ciascun sistema, gli organismi di valutazione devono possedere le competenze e professionalità necessarie per valutare determinati "dispositivi intelligenti" impiegati in particolari settori.

Gli organismi di valutazione della conformità sono organizzazioni private con personalità giuridica che hanno il compito di certificare la sicurezza ed accuratezza dei sistemi di IA introdotti nel mercato europeo. Attraverso la procedura descritta dimostrano di possedere i requisiti operativi, organizzativi, amministrativi e di cybersicurezza (ad es. gestione della qualità, risorse umane ed economiche) necessari per svolgere le valutazioni di conformità. L'organismo deve disporre stabilmente di «sufficiente personale amministrativo, tecnico, giuridico e scientifico dotato di esperienza e conoscenze relative ai tipi di sistemi di IA, ai dati, al calcolo dei dati pertinenti, nonché ai requisiti»[102] imposti ai sistemi di IA ad alto rischio. Gli organismi garantiscono una consulenza indipendente e imparziale per garantire valutazioni oggettive. Autorità e organismi di valutazione non possono svolgere attività di consulenza o qualsiasi altro tipo di attività che possa mettere a rischio la loro indipendenza di giudizio ed integrità. È inoltre prevista la possibilità per tali organismi di avvalersi, sotto la propria responsabilità, di affiliati e subappaltatori per la di conformità, a condizione di avere le risorse necessarie per valutare efficacemente i compiti svolti da parti esterne per loro conto. Tutti gli organismi autorizzati dall'Autorità

[101] Cit. art. 29 del 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);
[102] Cit art. 31 del 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);

nazionale sono inseriti in un elenco che riporta il loro numero di identificazione e le attività per le quali sono stati notificati (art. 35).

Infine, il regolamento prevede che a livello nazionale ciascuno Stato membro istituisca almeno un'autorità di vigilanza del mercato per agire come unico punto di contatto tra pubblica amministrazione e agenti di mercato per l'attuazione della legge sull'IA. L'Autorità deve possedere expertise approfondita delle nuove tecnologie, dei dati e del calcolo dei dati svolte dai sistemi di IA, della protezione dei dati personali, della cybersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza; nonché cognizione della legislazione speciale nazionale ed europea applicabile ai device. In particolare, ha il compito di monitorare l'attuazione del regolamento garantendo l'ottemperanza delle prescrizioni da parte degli enti e soggetti regolati e fornendo assistenza e consulenze alle PMI e start-up per agevolarle nell'attività di compliance (art. 70). A questa panoramica si deve aggiungere che il sistema delineato dal regolamento riflette l'approccio usato dall'Unione in materia di vigilanza del mercato dei prodotti, che contrariamente al meccanismo di applicazione nel settore dei servizi, affida poteri amministrativi e sanzionatori all'autorità del luogo in cui è stabilito il fornitore (principio del paese d'origine). Inoltre, allo stesso tempo, consente all'autorità del paese in cui il sistema è utilizzato di svolgere tutte le attività esecutive, compresa l'adozione di misure nei confronti dell'operatore o del prodotto. L'apparato di governance così delineato appare in linea anche con la natura di prodotto, e non di servizio, riconosciuta all'IA[103].

L'attività delle autorità nazionali è coordinata e coadiuvata da due organismi dell'Unione Europea: l'Ufficio per l'IA e il Consiglio per l'IA. Il primo costituisce il centro di competenze in materia di IA presso la Commissione europea, fornendo una base solida per la governance dell'IA a livello europeo. In particolare, l'organo è responsabile dell'attività di supervisione e monitoraggio dei modelli di IA per finalità generali. All'ente spettano inoltre tutti i poteri di un'autorità di vigilanza, per cui possono disporre istruttorie, presentare richiesta di informazioni ai fornitori e sviluppatori di un'IA generativa, sino alla condanna al pagamento delle sanzioni per quei modelli che, anche a seguito di una richiesta di informazioni, non rispetteranno gli standard europei. Inoltre,

[103] G. Mazzini, S. Scalzo, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts*, in Camardi (a cura di), *La via europea per l'Intelligenza artificiale*, 2023, disponibile al link: SSRN: https://ssrn.com/abstract=4098809 or http://dx.doi.org/10.2139/ssrn.4098809;

stimola l'applicazione coordinata del regolamento incoraggiando l'adozione di codici di condotta e buone pratiche a livello europeo. Parallelamente, il Consiglio per l'IA cura l'applicazione del regolamento attraverso l'esercizio di funzioni consultive, fornisce consulenza agli organi dell'Unione e agli Stati membri e formula raccomandazioni e pareri su qualsivoglia questione relativa l'applicazione del regolamento.

Il sistema di governance fin qui descritto appare piuttosto tradizionale, l'architettura disegnata dall'AI Act poggia il controllo, il monitoraggio e il coordinamento delle politiche attuate nei singoli Stati sulle autorità amministrative e organi consultivi. Oltre all'approccio centralizzato, il sistema è integrato dalla collaborazione dei privati che, in applicazione dei descritti principi di accountability e privacy by design and by default, sono i primi veri attuatori della normativa sull'IA, in quanto interpreti ed esecutori degli obblighi prescritti. Infatti, sono i produttori e i fornitori che devono garantire la presenza dei requisiti di cui alla sezione 2 del regolamento nel loro sistema. Inoltre, produttori, fornitori e deployer di IA ad alto rischio devono adempiere agli obblighi prescritti per tutta la durata del ciclo di vita del device, come la predisposizione e l'aggiornamento continuo del sistema di gestione della qualità.

L'attività di compliance trova espressione e rendicontazione nella valutazione di impatto sui diritti fondamentali (FRIA[104]) compilata dal deployer. La valutazione ha lo scopo di aiutare il deployer ad individuare e valutare i rischi specifici del sistema di IA calato nel suo contesto di utilizzo, evidenziando le categorie di persone, determinate o determinabili, che potrebbero essere interessate dai suddetti rischi. La valutazione deve essere compilata prima della messa in funzione del sistema, ed includere informazioni: sul periodo di tempo di utilizzo, i processi del deployer in cui il sistema è inserito, nonché frequenza di utilizzo e obiettivi per i quali è preposto. La valutazione comprende anche le misure adottate per affrontare i rischi evidenziati, in tale contesto rileva l'adozione di misure preventive del rischio, come le istruzioni per l'uso o i meccanismi di governance predisposti, e di misure reattive, come meccanismi che permettano il controllo e la sorveglianza umana sul sistema, nonché sistemi di gestione dei reclami (art. 27). In concreto, la FRIA prevede lo sviluppo di un piano dettagliato per mitigare i danni e gli impatti negativi identificati. Questo piano deve essere reso pubblico per assicurare

[104] L'acronimo si riferisce al nome dell'istituto in inglese "Fundamental Rights Impact Assessment";

trasparenza e responsabilità, infatti la FRIA viene notificata all'autorità di vigilanza del mercato. Il regolamento auspica inoltre il coinvolgimento di tutte le prospettive in gioco e suggerisce un confronto con associazioni di categoria, organizzazioni della società civile, autorità di settore ed esperti indipendenti che potrebbero meglio evidenziare problematiche o sensibilità dei gruppi di persone interessate[105]. Il documento che riporta la descrizione fedele delle caratteristiche, delle capacità e dell'impatto del sistema, deve essere costantemente aggiornato per aderire alle modifiche e sviluppi del sistema di deep learning e tenere traccia dei cambiamenti significativi del funzionamento del sistema.

Alle obbligazioni precedenti la messa in funzione del prodotto seguono adempimenti successivi. Il sistema di governance costruito dal regolamento si preoccupa di seguire ed adeguare le misure di sicurezza, di tipo preventivo e successivo, durante tutto il ciclo di vita del sistema. A questo proposito, è previsto un piano di monitoraggio post-marketing attuato dai fornitori, affiancato da un piano di valutazione pre-marketing per i sistemi di IA ad alto rischio. Questo duplice controllo garantisce che tali sistemi siano scrutinati tanto prima quanto dopo la loro immissione sul mercato, assicurando così un controllo continuo e approfondito volto a tutelare la sicurezza, la salute e i diritti fondamentali degli utenti.; il sistema dovrà essere descritto e comprovato nella documentazione tecnica obbligatoria di cui all'art. 18. Il piano deve assicurare un monitoraggio costante dei dati delle prestazioni dell'IA sul campo, in modo da accertare la costante conformità dei sistemi di IA ai requisiti imposti dall'AI Act (art. 72). I fornitori devono notificare gli incidenti arrecati dall'IA alle autorità di vigilanza del mercato degli Stati membri in cui si sono verificati tali incidenti e hanno inoltre l'obbligo di indagare sulle dinamiche dell'evento e adottare misure correttive per evitare che il pericolo si verifichi nuovamente (art. 73).

Questo rigoroso approccio nella gestione dei rischi e degli incidenti connessi all'utilizzo di sistemi di IA è inoltre presidiato dalle disposizioni sanzionatorie stabilite per garantire l'adempimento degli obblighi normativi. Infatti, l'attività di controllo e monitoraggio svolto dall'autorità di vigilanza per l'applicazione del regolamento culmina con un sistema sanzionatorio. L'art. 99 del regolamento prescrive le sanzioni pecuniarie

[105] Considerando 96 del 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);

in cui possono incorrere i soggetti responsabili (fornitori, rappresentanti autorizzati, importatori, distributori e utilizzatori), punendo tanto le violazioni minori, come la fornitura di informazioni inesatte, quanto l'inadempimento delle obbligazioni e dei principi disposti dagli artt. 5, 16, 22, 23, 26, 31, 33, 34, 50 del regolamento. Il sistema sanzionatorio previsto mira alla deterrenza attraverso pene pecuniarie «effettive, proporzionate e dissuasive», secondo cui l'ammontare viene stabilito tenendo conto della gravità della condotta illecita e del carattere doloso o colposo della violazione.

Il sistema di governance elaborato dal regolamento si compone di diversi livelli di compliance in cui sono coinvolti diversi soggetti in ambito pubblico e privato. La responsabilità, intesa come la capacità di rendere conto delle proprie azioni, si basa su tre pilastri: una fonte di autorità riconosciuta, procedure di indagine e l'esercizio dell'autorità. Il sistema analizzato appare allineato alla tradizionale relazione tra l'ente regolatore di settore e i soggetti regolati; dove i primi applicano e interpretano la norma mentre i secondi la osservano pena la sanzione. Al paradigma tradizionale si aggiungono però ulteriori livelli di compliance determinati dal middle-out approach e dai principi di accountability e di privacy by design and by default. Infatti, come anticipato nel precedente paragrafo spetta in prima istanza proprio al produttore/programmatore l'obbligo di costruire un'IA conforme ai principi stabiliti nel regolamento.

Pertanto, il sistema di governance elaborato dal regolamento è caratterizzato dalla presenza di diverse fasi di responsabilità in base agli obiettivi delle politiche perseguite. È possibile individuare le seguenti fasi: conformità, comunicazione, sorveglianza e attuazione. La fase di conformità prevede la stesura di linee guida, codici di condotta e standard tecnici che assistano gli operatori nella progettazione di un'IA che rispetti le normative legali. La fase di comunicazione si basa sul dialogo tra l'impresa e l'ente regolatore, durante il quale l'operatore chiarisce e dimostra come abbia soddisfatto i requisiti legali e adempiuto alle obbligazioni. Infine, si procede alla fase di indagine dell'autorità per accertare le dinamiche di un incidente e all'imposizione di sanzioni qualora si rinvenga che l'evento lesivo è stato causato dal software ovvero si accerti la non conformità del sistema rispetto ai requisiti e agli obblighi previsti dall'AI Act e dalle normative di settore applicabili al dispositivo specifico. Un sistema di governance efficace include strumenti relativi a tutte queste fasi, comprendendo approcci sia proattivi che reattivi alla responsabilità. In particolare, le fasi di conformità e sorveglianza

prevedono misure proattive ossia indirizzate alla costruzione di device accurati e sicuri, mentre la richiesta di comunicazioni e l'applicazione di sanzioni rappresentano misure di reazione dell'ordinamento rispetto ad illeciti che si sono già verificati[106].

L'AI Act riflette questa prospettiva combinata di strumenti legali, coinvolgendo nella governance dell'IA molteplici soggetti nei processi volti a garantire che gli operatori di IA agiscano in conformità al quadro disposto. Il quadro normativo fin ora descritto ha visto l'intervento del legislatore che ha stabilito i principi fondamentali della materia, definendo le pratiche vietate e le condizioni di liceità per la vendita in Europa dei sistemi di IA ritenuti ad alto rischio. Le scelte di politica pubblica sono state guidate da un approccio antropocentrico, che ha classificato quali sistemi di IA ad alto rischio quei device che, per l'attività condotta o il contesto di funzionamento, potrebbero ledere i diritti fondamentali della persona o i fondamenti dello Stato di diritto. La protezione dei diritti fondamentali non sarebbe stata altrettanto efficace se affidata esclusivamente a strumenti di soft-law e autoregolamentazione, poiché i soggetti privati spesso non riescono a bilanciare adeguatamente la tutela delle persone con gli interessi commerciali[107]. Il middle-out approach riesce dunque a coniugare le due istanze: tra chi chiede la tutela dei diritti fondamentali attraverso la definizione di limiti specifici, e coloro che chiedono maggiore flessibilità per promuovere una nuova tecnologia nel mercato.

Una volta stabiliti i principi fondamentali, le Autorità di settore concorrono all'applicazione del regolamento e coordinano gli organismi di valutazione, mentre questi ultimi svolgono un'attività di controllo e consulenza ai fornitori di IA. Gli organismi «aiuteranno i fornitori tech ad accertare e provare che il proprio prodotto intelligente è sicuro, affidabile e conforme ai requisiti previsti dall'AI Act»[108] svolgendo un ruolo di intermediazione tra l'autorità pubblica e i fornitori di software IA. In ultimo, ma non per importanza, gli operatori del settore sono i principali attori nella realizzazione del quadro

[106] C. Novelli, M. Taddeo, L. Floridi Luciano, *Accountability in Artificial Intelligence: What It Is and How It Works,* in AI & Society: Journal of Knowledge, Culture and Communication, Springer, 2022 https://doi.org/10.1007/s00146-023-01635-y , Disponibile al link SSRN: https://ssrn.com/abstract=4180366 or http://dx.doi.org/10.2139/ssrn.4180366 ;
[107] G. Resta, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?,* in Diritto dell'Informazione e dell'Informatica, 2022, p. 327;
[108] Cit. F. Di Ciommo e C. Scarpellino, *Le priorità della Presidenza italiana del G7 sull'Intelligenza Artificiale*, p. 19;

di governance descritto. Il regolamento attribuisce ai privati un ruolo importante nell'implementazione dei principi dell'AI Act; essi contribuiscono con un'attività di compliance rivolta al caso particolare, nella costruzione di un dispositivo che rispetti principi proposti e concorrendo all'elaborazione di codici di condotta (art. 39); al fine di promuovere l'applicazione volontaria di «alcuni o tutti i requisiti obbligatori applicabili ai sistemi di IA ad alto rischio, adattati in funzione della finalità prevista dei sistemi e del minor rischio connesso e tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore, come modelli e schede dati»[109].

In conclusione, possiamo osservare come il principio di accountability abbia posto al centro del meccanismo di governance dell'IA i fornitori e deployer. Questa scelta deriva dalla medesima *ratio* che riscontriamo nella legislazione sulla sicurezza dei prodotti e che ritiene che i produttori si trovino nella posizione migliore per garantire il rispetto degli standard previsti. In questo contesto la responsabilità civile per danni arrecati dai sistemi di IA deve inevitabilmente rapportarsi con lo schema di governance tracciato, che ha definito i principi ed i meccanismi per valutare la condotta dei soggetti responsabili imponendo doveri di accountability lungo tutto il ciclo di vita del prodotto. Pertanto, il sistema di responsabilità deve essere calato all'interno del nuovo quadro normativo sulle innovazioni e l'Intelligenza Artificiale, che prevede ulteriori strumenti (assicurazioni, sviluppo di standard etici e di sicurezza, requisiti di trasparenza) per garantire le funzioni di deterrenza dall'illecito e la ripartizione dei costi ad esso associati[110].

[109] Cit. Considerando 165 Regolamento (UE) 2024/1689;
[110] N. Muftic, *Understanding the Risks of Artificial Intelligence as a Precondition for Sound Liability Regulation*, Artificial Intelligence and Normative Challenges International and Comparative Legal Perspectives, in Law, Governance and Technology Series, Springer Nature Switzerland AG 2023, p. 86;

4) Spazi di sperimentazione normativa per regolare l'IA

I progressi tecnologici spesso necessitano di adattamenti normativi per regolare i nuovi prodotti, servizi e modelli di business che sfruttano le cd. disruptive innovation, ossia tecnologie che modificano «completamente la logica fino a quel momento presente nel mercato, introducendo comportamenti e interazioni nuove e rivoluzionando quindi le logiche correnti»[111]. Proprio perché capaci di rompere l'ordine economico precedente queste tecnologie dovrebbero attendere l'emanazione di normative nuove e speciali per comporre i contrasti che ne potrebbero derivare. Tuttavia, la procedura legislativa spesso implica lunghi iter parlamentari, determinati non soltanto dalle discussioni politiche relative agli interessi sociali coinvolti ma anche dalle scarse conoscenze tecniche dei burocrati sui nuovi ritrovati della scienza. Infatti, la cosiddetta "better regulation" impone un approfondimento su vari aspetti del fenomeno da regolare: la definizione chiara del problema, una comprensione effettiva del rapporto di causalità, una proposta normativa ragionevole e proporzionale agli obiettivi di tutela stabiliti, l'analisi dell'impatto ambientale della norma e la valutazione dei benefici derivanti dalla nuova soluzione di policy[112]. La complessità e i rallentamenti che caratterizzano l'iter legislativo fanno sì che la normativa non riesca a stare al passo con l'attuale avanzamento della tecnica, inoltre spesso si scontra con la resistenza degli operatori. Di fatto, le maggiori multinazionali del settore IT, i cd. GAFAM (Google, Apple, Facebook, Amazon, Microsoft), con sede in paesi extra UE, mal digeriscono l'iper-regolazione europea che ha imposto standard di sicurezza e requisiti di liceità per l'esportazione dei loro prodotti nel mercato europeo. La conformazione al quadro normativo descritto ha innalzato i costi professionali, materiali e tecnici per rendere i prodotti conformi alla legislazione europea; il GDPR, il Digital Market Act o il Digital Service Act costituiscono esempi di regolazione che hanno imposto agli operatori di mercato un'intensa attività di compliance per poter soddisfare gli standard europei. In questa prospettiva l'approccio garantista del vecchio continente non è apprezzato dagli attori economici provenienti da altre tradizioni normative, come

[111] Cit. la definizione di "innovazione disruptive" riportata da G. Prina, La disruption è di moda, ma spesso viene confusa con l'accelerazione tecnologica, in Il Sole 24h, 4 novembre 2019;
[112] Commissione UE, Better Regulation July 2023, https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_en ;

quelle rappresentate dal blocco statunitense e da quello asiatico, e che è da molti visto quale principale causa dell'arretramento tecnologico europeo rispetto ai mercati concorrenti[113].

Uno degli strumenti offerti dall'AI Act per ridurre le barriere normative per accedere al mercato europeo è la "regulatory sandbox", tradotta nel testo in lingua italiana del regolamento con la formula "Spazi di Sperimentazione normativa". L'istituto fornisce «un quadro controllato istituito da un'autorità competente che offre ai fornitori, o potenziali fornitori di sistemi di IA, la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare»[114].

Il concetto di "regulatory sandbox" è stato introdotto dalla Financial Conduct Authority (FCA) del Regno Unito nel 2016 per promuovere l'innovazione in ambito fintech, il settore che promuove l'impiego di strumenti digitali nel settore finanziario. La FCA attraverso le sandbox offre ai fornitori di tecnologie fintech la possibilità di testare i propri prodotti all'interno di uno spazio di sperimentazione che permette la deroga temporalmente limitata della normativa applicabile. Lo scopo assegnato all'istituto è proprio quello di ridurre le barriere normative per gli imprenditori fintech pronti a testare le loro innovazioni nel contesto reale. Dal 2016, diversi altri paesi hanno adottato sandbox regolamentari per il fintech, utilizzate per agevolare l'introduzione nel mercato di nuove tecnologie nei settori dei criptoasset, delle tecnologie di registro distribuito, crowdfunding, dei pagamenti mobili, dei prestiti peer-to-peer e servizi di consulenza automatizzati. Lo strumento è particolarmente utile se si considera che spesso i prodotti e servizi fintech sono esportati a livello globale, perché si tratta tecnologie sviluppate e distribuite contemporaneamente in diversi mercati finanziari. Tuttavia, le sandbox regolamentari sono state create solo a livello nazionale, e talvolta subnazionale; pertanto, permane una certa frammentazione tra i regimi normativi applicati alle innovazioni. Proprio per agevolare le imprese nel rapporto con le diverse giurisdizioni e autorità governative la FCA ha istituito il "Global Financial Innovation Network" (GFIN), un

[113] G. Maglio, Bilanciare Regolamentazione e Innovazione: Le Sfide del Mercato Digitale Europeo, disponibile al link: https://sog.luiss.it/policy-observatory/publications ;
[114] Cit. Art. 3 Regolamento (Ue) 2024/1689;

network di più di 70 organizzazioni che promuovono la circolazione delle innovazioni tecnologiche tutelando gli interessi di consumatori e investitori[115].

La sandbox costituisce anche un meccanismo di cooperazione pubblico-privato per aiutare gli apparati amministrativi a sviluppare best practice neutrali redatte da esperti per rendere il mercato competitivo minimizzando i pericoli per i consumatori e la stabilità economica del settore[116]. E' bene tuttavia specificare che introdurre una nuova tecnologia non sperimentata nel contesto socio-economico costituisce di per se' un rischio; la portata delle discriminazioni e delle violazioni della privacy che gli algoritmi dotati id IA potrebbero arrecare ai consumatori non possono essere individuati a prescindere. Altrettanto poco si conoscono le implicazioni per la stabilità finanziaria derivanti dall'uso di tali strumenti nella gestione del rischio. La complessità intrinseca di questi sistemi, unita alla loro capacità di apprendere e prendere decisioni in maniera autonoma, solleva preoccupazioni non solo in termini di equità e trasparenza, ma anche di affidabilità delle valutazioni del rischio e della capacità di risposta a situazioni di crisi economica[117]. Pertanto, sebbene le sandbox costituiscano uno strumento di apertura del mercato, sia l'apparato amministrativo che il pubblico di consumatori e risparmiatori devono essere consapevoli del trade-off sotteso alla sperimentazione normativa, che compromette i diritti personali ed economici dei consumatori per ottenere maggiori informazioni sulle innovative disruptive e attrarre flussi di investimenti dall'estero a cui auspicano i governi.

L'ulteriore vantaggio conseguito dalle amministrazioni, nell'istituzione delle sandbox, è costituito dal patrimonio informativo che potrebbero acquisire grazie alla supervisione dell'esperimento e all'interazione diretta con le aziende fornitrici. Tramite la sperimentazione normativa i policymaker avrebbero accesso diretto alle tecnologie emergenti, le loro caratteristiche e i modelli di business applicati. L'approfondita

[115] https://www.thegfin.com/, Mentre, un'iniziativa più recente è la "Digital Securities Sandbox" istituita congiuntamente da FCA e dalla Bank of England per agevolare la regolazione e diffusione di titoli tokenizzati, Maggiori informazioni sull'iniziativa sono contenuti nel link allegato: https://www.bankofengland.co.uk/paper/2024/cp/digital-securities-sandbox-joint-bank-of-england-and-fca-consultation-paper;
[116] H. J. Allen, *Sandbox Boundaries*, in Vanderbilt Journal of Entertainment & Technology Law 22, 2020, p. 300;
[117] H. J. Allen, *Sandbox Boundaries*, Op. cit. p. 307;

conoscenza del fenomeno consentirebbe ai regolatori di comprendere l'impatto della tecnologia sulle normative vigenti e le migliori soluzioni normative da adottare[118].

Perciò le sandbox regolamentari dovrebbero essere concepite e progettate massimizzando la raccolta e la condivisione di informazioni, anche quelle aventi sede in paesi diversi. Tuttavia, sussiste una forte competizione anche tra le diverse giurisdizioni, che spingono i governi a proteggere gelosamente le informazioni privilegiate ottenute attraverso le sandbox in quanto utilizzate non soltanto per redigere apparati di policy chiari ed efficaci, ma anche per predisporre un ecosistema più favorevole all'innovazione sperimentata Pertanto, le amministrazioni potrebbero preferire mantenere tali informazioni riservate, temendo che, se condivise, mercati e imprese straniere potrebbero trarre vantaggio dall'esperimento. Il fenomeno è anche conosciuto quale "disclosure dilemma", che descrive la posizione delle autorità nazionali chiamate a condividere informazioni commercialmente sensibili sulle attività delle loro imprese. È proprio allo scopo di agevolare la circolazione di informazioni che sono stati istituiti forum, come il GFIN, o altre organizzazioni internazionali. Tuttavia, la creazione di forum e maccanismi utili allo scambio di informazioni non raggiungerà il suo obiettivo a meno che non vengano forniti maggiori incentivi alle stesse autorità statali[119]. La competizione tra giurisdizioni potrebbe inoltre portare ad una "gara a ribasso" tra ordinamenti, attraverso l'emanazione di standard normativi più bassi al fine di creare un contesto tech-friendly per le aziende e attrarre maggiori capitali grazie ad una regolazione più flessibile ed "accondiscendente". Questa de-generazione dell'utilizzo della sandbox non rispetta la natura e lo scopo dell'istituto, le cui priorità è assicurare la stabilità finanziaria (nelle sandbox fintech) e la protezione dei consumatori[120].

Alla luce delle caratteristiche e degli scopi perseguiti dalle sandbox, esse potrebbero costituire un utile strumento di regolazione dei device dotati di IA per le aziende che vogliano esportare la loro tecnologia in Europa. Tuttavia, è bene precisare che, a differenza dei prodotti fintech, l'IA presenta una natura articolata e applicazioni diversificate, che impongono un approccio più flessibile e versatile nell'istituzione di

[118] R. Nabil, *Artificial Intelligence Regulatory Sandboxes*, in Journal of Law, Economics & Policy, 2024, p. 295;
[119] H. J. Allen, *Sandbox Boundaries*, Op. cit. p. 319;
[120] H. J. Allen, *Sandbox Boundaries*, Op. cit. p. 308;

sandbox ad esse dedicate. Infatti, mentre i prodotti fintech sono limitati al settore dei servizi finanziari, l'IA abbraccia un'ampia gamma di applicazioni in vari settori come sanità, manifattura e finanza. Questa diversità richiederebbe l'implementazione di regolamentazioni specifiche per ciascuna destinazione d'uso. Quindi per poter sfruttare le sandbox regolamentari in questo particolare settore innovativo, devono essere concepiti adattamenti o soluzioni settoriali per affrontare le sfide uniche poste dall'IA. Le medesime difficoltà si registrano anche nella regolazione degli strumenti di IA, a causa dell'impossibilità di ricondurre questa tecnologia all'interno di un'industria o di un mercato unitario nonchè l'assenza di una definizione legale condivisa. Per tutti questi motivi, l'ipotesi di una sandbox unica e generale per l'IA sembra meno efficacie della sua omologa fintech; peraltro, si deve considerare che le diverse applicazioni IA implicheranno la competenza e la supervisione di autorità di settore diverse, che dovranno essere adeguatamente coinvolte nel processo di supervisione dell'esperimento[121].

Per regolamentare efficacemente le applicazioni dei sistemi di IA in diversi settori, è fondamentale creare sandboxes normative specializzate. Questi spazi sperimentali dedicati a ciascun ambito permettono lo sviluppo di regole specifiche e ad hoc. Ad esempio, i settori dell'energia nucleare e della sanità richiedono conoscenze approfondite delle normative specifiche e delle leggi sull'IA applicabili.[122]. Tuttavia, spesso le aziende tech, soprattutto se ancora nella fase start-up, dispongono di limitate risorse legali, le quali non sono sufficienti per partecipare alle sandbox generali, anche qualora ne soddisfino i requisiti[123].

L'istituto, in circolazione dal 2016, appare ancora giovane anche se ha avuto un'eco globale; inoltre, sebbene sia un istituto nato in Europa, ha attratto l'attenzione di molteplici giurisdizioni. Infatti, tra i cd. BRICS il Brasile appare intenzionato ad istituire

[121] R. Nabil, *Artificial Intelligence Regulatory Sandboxes*, in Journal of Law, Economics & Policy, 2024, p. 304 che sostiene che per una regolamentazione efficace dell'IA sia necessaria una combinazione di diverse sandbox normative;

[122] Cfr. R. Nabil, *Artificial Intelligence Regulatory Sandboxes*, Op. cit, p. 320 riporta quale esempio di sandbox settoriale l'iniziativa avviata a Zurigo denominata "Innovation Sandbox for Artificial Intelligence." Specializzata in 5 aree di applicazione dell'IA«five areas: i) autonomous systems; ii) automated infrastructure maintenance (drone inspection with image recognition); iii) Al in education; iv) smart parking (image recognition); and machine translation»

[123] Cfr. R. Nabil, *Artificial Intelligence Regulatory Sandboxes*, in Journal of Law, Economics & Policy, 2024, p. 319 riporta una panoramica delle principali esperienze nazionali e internazionali di regulatory sandbox;

una sandbox per l'IA, mentre Singapore ha l'intenzione di istituire la GenAI sandbox, una speciale sandbox per l'IA generativa[124].

Nel frattempo, l'Unione Europea ha continuato ad investire sullo strumento assegnandogli una specifica sezione nell'AI Act. La Commissione Europea ha infatti proposto la creazione di "Spazi di sperimentazione normativa" già nel progetto di legge sull'IA dell'aprile 2021. Il primo Stato membro a muoversi in tal senso è stato la Spagna cha ha lanciato una sandbox per l'IA e istituito un'apposita Agenzia dedicata. Il testo finale dell'AI Act obbliga gli Stati membri ad istituire almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale; tuttavia è aperta la possibilità di avviare progetti congiunti con le sandbox di altri Stati membri o prendere pare ad esperimenti già in corso. Gli spazi di sperimentazione possono essere fisici, digitali o ibridi e devono essere dotati delle risorse finanziarie e umane necessarie[125]. Gli obiettivi assegnati all'istituto comprendono: la promozione dell'innovazione, il rafforzamento della certezza del diritto per gli innovatori e la comprensione dei rischi emergenti da parte delle autorità competenti. Inoltre, questi spazi dovrebbero coadiuvare gli operatori all'osservanza dell'AI Act grazie alla cooperazione e al dialogo tra organi pubblici e enti privati, così riducendo le barriere amministrative all'accesso del mercato digitale europeo per le piccole-medie imprese (PMI) e le start-up; alle quali è concesso un accesso gratuito alle sandbox. La supervisione dei sistemi di IA nello spazio di sperimentazione avrà ad oggetto: lo sviluppo, l'addestramento, la prova e la convalida dei sistemi IA, identificando e mitigando eventuali rischi significativi. Nel condurre tali attività le autorità competenti devono cooperare con le altre Autorità di settore, nonché laboratori di ricerca, organismi notificati e organizzazioni della società civile[126]. Per evitare un'attuazione frammentaria dell'istituto, la Commissione Europea interviene con atti distinti per regolamentare nel dettaglio la creazione, l'implementazione e il funzionamento delle AI sandbox. In particolare, si occupa di definire i requisiti e la procedura amministrativa per accedere all'istituto; tali informazioni vengono fornite in modo chiaro e accessibile su un'interfaccia web dedicata, in modo da coinvolgere le PMI e le start-up che dispongono

[124] Maggiori informazioni al riguardo in A. Sharon, *Empowering SMEs: Singapore's GenAI Sandbox Initiative*, febbraio 2024, disponibile al link: https://opengovasia.com/2024/02/09/empowering-smes-singapores-genai-sandbox-initiative/ ;
[125] Considerando 138 e art. 57 del Regolamento (UE) 2024/1689;
[126] Art. 58 del Regolamento (UE) 2024/1689;

di minori risorse legali e amministrative rispetto alle grandi aziende tecnologiche[127]. Infine, allo scopo di agevolare l'utilizzo e la regolazione dei sistemi di IA ad alto rischio, i fornitori interessati predispongono un piano di prova da presentare all'autorità di vigilanza del mercato specificando i limiti temporali dei test, le tutele aggiuntive per le persone più vulnerabili, nonché un accordo scritto che definisca i ruoli e le responsabilità dei potenziali fornitori e dei deployer[128].

In Italia sono attualmente attive due sandbox. La prima, istituita con il Decreto-legge n. 34/2019, è dedicata ai settori finanziario, bancario e assicurativo, e opera sotto la supervisione della Banca d'Italia, IVASS e Consob[129]. Per partecipare a questa Fintech Sandbox, gli operatori devono presentare un progetto "significativamente innovativo" che apporti valore aggiunto ai consumatori o aumenti l'efficienza del sistema economico-finanziario, oltre a essere economicamente sostenibile e sufficientemente sviluppato per la sperimentazione[130]. La seconda sandbox, denominata Sperimentazione Italia, ha un carattere più generale ed è aperta alle innovazioni in qualsiasi settore. È istituita e gestita dal Dipartimento per la Trasformazione Digitale e dal Ministero delle Imprese e del Made in Italy (MIMIT), è la prima del suo genere in Europa e potrebbe offrire un'opportunità significativa per le e le imprese che vogliono entrare nel mercato europeo e conformarsi alle sue normative. Tuttavia, finora sono state avviate solo due iniziative tramite Sperimentazione Italia. La scarsa adesione può essere attribuita principalmente alla limitata divulgazione pubblica dell'esistenza e delle caratteristiche della sandbox[131]. Infatti, il sito web di Sperimentazione Italia non sono presenti informazioni dettagliate sulle fasi e i tempi della procedura amministrativa, mancano indicazioni sui requisiti di partecipazione, i criteri di valutazione e i progetti precedenti. Questa carenza di

[127] Vedi Art. 58 del Regolamento (UE) 2024/1689 e F. Di Ciommo e C. Scarpellino, Le priorità della Presidenza italiana del G7 sull'Intelligenza Artificiale, Op. cit. p. 17;
[128] Art. 60 e Considerando 242 del Regolamento (UE) 2024/1689, secondo i quali il piano deve inoltre prevedere «tutele aggiuntive per garantire che le previsioni, le raccomandazioni o le decisioni del sistema di IA possano essere efficacemente ribaltate e ignorate e che i dati personali siano protetti e cancellati quando i soggetti hanno revocato il loro consenso a partecipare alle prove, fatti salvi i loro diritti in qualità di interessati ai sensi della normativa dell'Unione in materia di protezione dei dati.»
[129] Maggiori informazioni disponibili al sito:
https://www.bancaditalia.it/focus/sandbox/index.html?com.dotmarketing.htmlpage.language=1&dotcache=refresh ;
[130] S. Ranchordas, V.Vinci, *Regulatory sandboxes and innovation-friendly regulation : between collaboration and capture*, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4696442 ;
[131] S. Ranchordas, V. Vinci, *Regulatory sandboxes and innovation-friendly regulation: between collaboration and capture*, Op. cit.;

informazioni dissuade gli operatori di mercato dall'intraprendere una procedura burocratica con esiti incerti.

Illustrati gli scopi e le caratteristiche della sandbox è necessario soffermarsi sul regime di responsabilità previsto per i danni arrecati da un sistema di IA che operi nei confini dell'esperimento. Sul punto l'art. 57 espressamente prevede che i fornitori «rest[i]no responsabili ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione». Pertanto, la "messa in prova" del device all'interno delle sandbox consente di derogare alle norme di settore nel quale opera il sistema, non anche le disposizioni in materia di responsabilità per danni. Inoltre, l'impresa può evitare sanzioni amministrative per violazioni dell'AI Act qualora abbia rispettato il piano specifico concordato con l'Autorità competente.

5) L'IA generativa e le incongruenze nel sistema di allocazione delle responsabilità

Sebbene ancora lontani dall' "Intelligenza Artificiale generale" descritta nella fantascienza, i recenti progressi nell'apprendimento automatico e nell'IA hanno catturato l'interesse pubblico e legislativo. Oggi, i modelli linguistici di grandi dimensioni (LLM) sono in grado di superare esami di avvocatura, conversare su (quasi) ogni argomento, creare in pochi istanti nuove sinfonie e opere d'arte visiva, spesso indistinguibili da quelle umane[132]. Gli algoritmi, capaci di governare processi conoscitivi e decisionali, ora sono in grado non solo di conoscere la realtà raccogliendo autonomamente i dati, ma anche trasformarla, aggiungendo nuovi contenuti originali. È bene precisare che, mentre l'IA generativa si concentra sulla capacità creativa di generare contenuti nuovi, gli LLM rappresentano un sottoinsieme di IA generativa focalizzato sul linguaggio naturale, con

[132] M. Sag, *Fairness and Fair Use in Generative AI*, in Fordham Law Review, 2024, p.1888;

capacità avanzate grazie all'ampiezza e alla profondità dei dati su cui sono stati addestrati.[133].

Quindi l'IA generativa e gli LLMs costituiscono un nuovo ed avanzato step nello sviluppo degli algoritmi e le sue particolari funzionalità aprono ulteriori questioni giuridiche per stabilire un equilibrio tra i benefici tecnici, i costi a lungo termine, e la tutela dei diritti nell'era del colonialismo digitale[134]. Questi sviluppi sottolineano la necessità di regolamentazioni aggiornate per rispondere ai conflitti generati dall'IA, gestendone i potenziali rischi. L'IA generativa costituisce un valido esempio dell'alto tasso di obsolescenza delle norme che regolano il settore tech, che non riescono a seguire il veloce passo della tecnica.

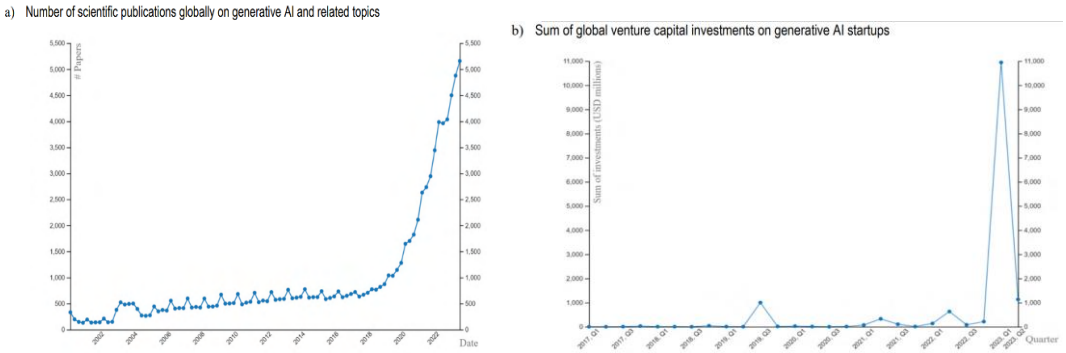

Figura 6. I grafici mostrano il trend registrato dall'IA generativa nel dibattito pubblico[135].

Infatti, l'IA generativa non era inclusa nella prima versione dell'AI Act, è stata aggiunta soltanto nel 2023, quando sono state presentate sul mercato le prime forme di modelli linguistici di grandi dimensioni (LLM), come GPT-4 e DALL-E di Open AI, DeepArt o StyleGAN attirando subito l'attenzione del pubblico e dell'industria.

[133] H. Torne, *What Are Generative AI, Large Language Models, and Foundation Models?*, in CSET, 12 maggio 2023, disponibile al link: https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models/ ;
[134] F. Maurizio, *Predizione algoritmica, intelligenza artificiale generativa e rischi di cristallizzazione dell'ermeneutica giurisprudenziale*, in Foro It., 2023, p. 2;
[135] OCSE, *G7 Hiroshima Process on Generative Artificial Intelligence (AI)- Towards a G7 Common Understanding on Generative AI*, disponibile al link: https://www.oecd-ilibrary.org/science-and-technology/g7-hiroshima-process-on-generative-artificial-intelligence-ai_bf3c0c60-en ;

La capacità dell'IA generativa di strutturare contenuti originali in modo autonomo riporta di nuovo al centro del dibattito giuridico l'imprevedibilità degli output, in particolare solleva profili di contrasto con l'attuale regime sulla responsabilità, sulla privacy, sulla proprietà intellettuale e sulla cybersicurezza. Le questioni rilevanti sotto il profilo privacy sono state denunciate subito dal Garante per la protezione dei dati personali che ha contestato a Open AI nel 2023 la violazione delle disposizioni privacy in merito alla tutela dei dati dei minori[136]. Ulteriori preoccupazioni si registrano in merito al trattamento dei dati personali svolto dai sistemi di LLMs durante la fase di training che implica la memorizzazione e conservazione dei dati e possibili attacchi di inversione[137]. Inoltre, potrebbero essere inseriti dati sensibili anche nei prompt i quali potrebbero essere a loro volta conservati e trattati. I problemi lato privacy hanno ad oggetto: la base giuridica per il trattamento dei dati dei prompt, obblighi informativi, data breach, diritto all'oblio, processo decisionale automatizzato e la limitazione delle finalità e la minimizzazione dei dati.

Senza approfondire tutte le criticità riscontrate tra il funzionamento dell'IA generativa e la protezione dei dati personali, si precisa che la raccolta deve essere strettamente limitata «a quanto necessario rispetto alle finalità per le quali sono trattati»[138]. L'AI Act riflette lo stesso principio all'art. 10, che impone «pratiche di governance e gestione dei dati adeguate alla finalità prevista del sistema di IA ad alto rischio». Tuttavia, questo principio è messo in crisi dalle molteplici finalità e task che l'IA generativa soddisfa; limitare gli scopi del trattamento dati di un software LLM potrebbe ostacolare il training della tecnologia e renderla meno performante[139]. Inoltre, ulteriori contrasti si registrano

---

[136] GPDP, *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori*, il provvedimento ha disposto «la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti di OpenAI, la società statunitense che ha sviluppato e gestisce la piattaforma.» il documento è disponibile sul sito web dell'autorità al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832 ;

[137] I sistemi di inversion attacks dei modelli permettono di inferire i dati personali utilizzati per addestrare un sistema di IA un esempio è riportato da M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart. *Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In USENIX Security Symposium*, 2014, p. 17–32 che illustra «in the context of genomic privacy shows a model inversion attack that is able to use black-box access to prediction models in order to estimate aspects of someone's genotype. Their attack works for any setting in which the sensitive feature being inferred is drawn from a small set. They only evaluated it in a single setting, and it remains unclear if inversion attacks pose a broader risk.»

[138] Cit. Art. 5 par c del Regolamento (UE) 679/2016;

[139] Sul fenomeno dell'IA generativa e i suoi contrasti con le disposizioni in materia di responsabilità, privacy e copyright vedi C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, *Generative AI in EU*

in merito al diritto d'autore sui dati utilizzati per addestrare l'IA generativa e che vengono utilizzati per creare nuovi contenuti. Infatti, l'IA generativa copia i dati trovati su internet per allenarsi, proprio la copia di contenuti coperti da diritto d'autore non autorizzata concreta una violazione della proprietà intellettuale del dato con valore artistico[140]. Il lecito sfruttamento di questi dati prevederebbe il permesso dei titolari dei diritti o una specifica autorizzazione legale. Il rispetto della proprietà intellettuale da parte dell'IA generativa sembra difficile da assicurare, in considerazione della miriade di dati usati e del numero di titolari di diritti coinvolti, e soprattutto delle tecniche di web scraping utilizzate per l'addestramento la cui legalità, peraltro, è ancora dibattuta[141]. Tuttavia l'AI Act ha imposto ai fornitori di modelli di IA generativa il rispetto del diritto d'autore dell'Unione Europea nonché una sintesi pubblica dei contenuti usati per l'addestramento[142]

Le questioni esposte non sono state affrontate dall'AI Act nella regolazione della fattispecie di IA per finalità generali, per la quale prescrive invece specifici obblighi di trasparenza, come l'apposizione di un marchio su tutti i contenuti generati artificialmente per informare il pubblico dell'origine artificiale di questi prodotti (art. 50). Maggiori obblighi sono imposti ai fornitori di modelli di IA per finalità generali sui quali si basano gli omonimi sistemi. Oltre a redigere e mantenere aggiornata la documentazione tecnica del modello, i fornitori devono condividere informazioni dettagliate agli sviluppatori di che intendano integrare il modello nei loro sistemi; questi ultimi devono conoscere le capacità e i limiti del modello stesso. È inoltre richiesto uno sviluppo dei modelli che rispetti il diritto d'autore dell'Unione Europea e una sintesi pubblica dei contenuti usati per l'addestramento[143]. Maggiori obblighi sono previsti invece per coloro che sviluppano modelli di IA per finalità generali con rischio sistemico, infatti i fornitori di tali modelli (oltre agli obblighi previsti dagli articoli 53 e 54) devono eseguire valutazioni standardizzate dei modelli, inclusi test contraddittori, per identificare e attenuare i rischi

Law: Liability, Privacy, Intellectual Property, and Cybersecurity, 2024. Disponibile su SSRN: https://ssrn.com/abstract=4694565 or http://dx.doi.org/10.2139/ssrn.4694565 ;

[140] M. Sag, *Fairness and Fair Use in Generative AI*, Op. cit., p.1892;

[141] C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity* Op. cit. p. 17;

[142] Art. 53 del Regolamento (Ue) 2024/1689 il quale inoltre precisa che questi obblighi non si applicano ai modelli IA open source, eccetto quelli con rischi sistemici;

[143] Art. 53 del 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);

sistemici. Devono valutare e mitigare tali rischi, e comunicare tempestivamente alle autorità competenti qualsiasi incidente grave e le misure correttive adottate. Inoltre, è necessario garantire un'adeguata protezione della cybersicurezza dei modelli e delle infrastrutture correlate (art. 55).

Questo è l'assetto normativo prescelto per affrontare le criticità evidenziate sull'IA generativa, tuttavia è bene precisare che le versioni precedenti dell'AI Act avevano assunto un atteggiamento molto più prudente, classificando tutti i sistemi di IA per finalità generali quali sistemi ad alto rischio. Questa scelta è stata giustificata dalla considerazione che l'algoritmo, essendo in grado di soddisfare molteplici compiti, potrebbe essere utilizzato anche per ledere i diritti fondamentali e i principi dello stato di diritto, capacità che qualificano il sistema come ad alto rischio. Le successive versioni dell'AI Act hanno eliminato l'automatica e preventiva classificazione ad alto rischio dell'IA generativa, imponendo invece la valutazione sulle circostanze e contesto di utilizzo del sistema nel quale il modello verrà integrato; qualora si riscontrino i requisiti di cui all'art. 6 il fornitore del sistema di IA è tenuto al rispetto degli obblighi e dei requisiti della sezione terza[144]. Questa impostazione permetterebbe di determinare il livello di rischio dell'IA generativa e degli LLM, imponendo un approccio più specifico e strutturato sulle caratteristiche del caso concreto. Questa lettura appare inoltre in linea con il nuovo comma dell'art. 6, per il quale i sistemi di IA utilizzati in aree di alto rischio non sono automaticamente qualificati tali, a meno che non pongano un rischio significativo per le persone o l'ambiente[145]. Questa valutazione potrebbe essere fatta in prima istanza dal fornitore del modello attraverso una valutazione dell'impatto sui diritti fondamentali (FRIA), la quale per ora è imposta solo per i sistemi già qualificati ad alto rischio[146].

Ulteriore punto di frizione tra l'IA per finalità generali e l'assetto determinato dal regolamento riguarda la distribuzione delle responsabilità lungo la catena del valore. Il regolamento, infatti, evidenzia spesso come la responsabilità del fornitore dell'IA

[144] illustrati nel secondo paragrafo di questo capitolo;
[145] Infatti il par. 3 dell'art. 6 ora prevede che «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.»
[146] C. Novelli, F. Casolari, P. Hacker, G. Spedicato, L. Floridi, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity* Op. cit. p 3;

coinvolga tutte le fasi di sviluppo, produzione e distribuzione del prodotto intelligente. Questa scelta normativa è apparsa una strada vincolata alla luce del sistema di governance elaborato dall'AI Act, che impone obblighi al fornitore di IA di gestione e controllo del prodotto anche dopo la messa in commercio. In assenza del regolamento i principi in materia di responsabilità da prodotto difettoso avrebbero condotto ad un'altra conclusione, la responsabilità del produttore si ferma lì dove il prodotto è progettato e costruito, i malfunzionamenti non possono essergli addebitati se il difetto non esisteva quando il prodotto è stato messo in circolazione. Il regolamento invece supera questo limite estendendo la responsabilità del fornitore anche ai difetti originati dopo la produzione e cessione del software.

Questa è stata la soluzione inaugurata per rispondere ai quesiti relativi la capacità adattiva dei sistemi di IA, e alla loro abilità di evolversi e modificare il loro comportamento e i patterns di "ragionamento" dopo la loro messa in commercio. L'AI Act all'art. 25 stabilisce le responsabilità e gli obblighi dei fornitori di sistemi di IA ad alto rischio, che permangono per tutto il ciclo di vita dell'IA, si interrompono qualora il distributore, l'importatore, il deployer o altro terzo abbiano modificato la finalità prevista di un sistema di IA. Il legame tra il fornitore e il funzionamento del suo modello di IA per finalità generali si spezza qualora un terzo integrasse il modello di IA per finalità generali nel proprio device «in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6». L'IA per finalità generali costituisce infatti l'eccezione alla responsabilità costante dei fornitori di sistemi di IA, in quanto la loro particolare versatilità gli permette di svolgere pressoché qualsiasi mansione li rende idonei a molteplici – e potenzialmente infinite – applicazioni a valle.

Il regolamento, inoltre, non si esime dal regolare i rapporti tra il fornitore del software di IA per finalità generali e lo sviluppatore del sistema di IA che intende integrare modello in un proprio prodotto; in particolare si premura di assicurare a quest'ultimo una conoscenza approfondita del sistema di IA generativa, necessaria per garantire il rispetto delle prescrizioni dell'AI Act[147]. È quindi necessario adottare adeguate misure di

[147] Considerando 85 del Regolamento (UE) 2024/1689, il considerando 88 continua specificando come questa collaborazione dovrebbe essere condotta «Tali parti svolgono un ruolo importante nella catena del valore nei confronti del fornitore del sistema di IA ad alto rischio in cui i loro sistemi di IA, strumenti, servizi, componenti o processi sono integrati e dovrebbero fornire a tale fornitore mediante accordo scritto le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari sulla base dello

trasparenza, inclusa la redazione e il continuo aggiornamento della documentazione tecnica, il cui contenuto è specificato all'interno di specifici allegati al regolamento; si prevede inoltre la possibilità per la Commissione di intervenire per modificare questi allegati tramite atti delegati, al fine di recepire ed adeguarsi ai progressi tecnologici[148].

Pertanto, il sistema di governance delineato dall'AI Act e il principio di accountability pongono al centro del sistema il fornitore che deve: individuare la categoria di rischio del proprio sistema di IA, progettare il sistema rispettando i requisiti previsti dall'AI Act per la particolare categoria, predisporre le misure di trasparenza, controllo e gestione dei dati necessarie durante tutto il ciclo di vita dell'IA. L'adempimento di questi presidi dovrebbe scagionare il fornitore nel caso in cui, pur avendo attuato i protocolli e le misure richieste, il sistema di IA arrechi danni a terzi. Tale conclusione consegue dalla lettura dell'articolo 25 del regolamento sulla responsabilità lungo la catena del valore dell'IA che richiama espressamente la responsabilità del fornitore – o di altro soggetto che abbia apposto il suo nome o marchio o modificato sostanzialmente il sistema – per l'adempimento degli obblighi del fornitore a norma dell'articolo 16 e dalle proposte di direttive sulla responsabilità. La Commissione UE il 28 settembre 2022 ha presentato due proposte di atti normativi, entrambe dirette a stabilire il quadro regolatorio sulla responsabilità civile per danni arrecati da sistemi di IA, entrambe basate sull'adempimento degli obblighi dell'AI Act. Il quadro normativo complessivo determinato dall'AI Act potrebbe costituire un «playbook chiaro che rimuova le ambiguità e promuova lo sviluppo delle nuove tecnologie»[149]. Questo approccio permetterebbe alle aziende di prefigurare i costi relativi allo sviluppo e all'immissione di un prodotto di IA sul mercato europeo, tra i quali i costi risarcitori connessi ai danni causati dai sistemi di IA ad alto rischio. Infatti, la categorizzazione dei sistemi di IA in base al rischio aiuta ad individuare i sistemi che, con più probabilità, potrebbero cagionare un danno ingiusto. Pertanto, urge chiedersi come

---

stato dell'arte generalmente riconosciuto, al fine di consentire al fornitore di adempiere pienamente gli obblighi di cui al presente regolamento, senza compromettere i propri diritti di proprietà intellettuale o segreti commerciali»

[148] Considerando 101 del Regolamento (UE) 2024/1689;

[149] Cit. Mc Kinsey & Company, *Leveraging generative AI in Europe: The opportunities and challenges*, riporta le parole di Yetunde Dada, Senior Director of product development in Mc Kinsey & Company a Londra sul nuovo apparato normativo per l'IA dell'Unione europea la quale per l'appunto afferma che: «Having a clear framework to be able to build up a case would make it a lot easier for companies around the world to adopt generative AI. This goes beyond the borders of Europe, because globally, companies have been speaking about these issues and looking for a pathway forward. So, I think it's really exciting in that way»;

verrà valutata la responsabilità dei soggetti coinvolti nella catena del valore dell'IA, i criteri che verranno utilizzati per accertarla e se il quadro previsto riuscirà a resistere alle istanze disruptive della moderna innovazione, che sembrano richiedere politiche ad hoc per ogni nuovo ritrovato della tecnica. D'altronde ciò è quanto già accaduto per l'IA generativa, la quale potrebbe ben configurare il successivo step evolutivo dei primi sistemi di matching learning e ha già richiesto soluzioni alternative *ad hoc* rispetto al quadro normativo tracciato nel 2021.

Capitolo III
La responsabilità civile dei sistemi di IA: tra ricostruzioni normative e proposte dell'Unione Europea

1) Il quadro normativo vigente e le prime proposte di riforma sulla responsabilità per danni arrecati da sistemi di IA

L'economia digitale, pur apportando benefici significativi tramite l'offerta di prodotti e servizi innovativi, solleva diversi interrogativi sull'adeguatezza dell'attuale regime di responsabilità civile. In particolare, emergono dubbi sulla sua capacità di rispondere alle sfide poste dalle nuove tecnologie emergenti, come l'IA, la robotica e l'Internet delle cose (IoT). Il quadro normativo sulla responsabilità civile mira a raggiungere tre obiettivi principali: garantire alle imprese certezza giuridica sui rischi connessi alle loro attività, promuovere la prevenzione dei danni e assicurare che le vittime ricevano un risarcimento adeguato. Ad esempio, la direttiva 85/374/CEE, regolando la responsabilità dei produttori per i danni causati da prodotti difettosi immessi sul commercio, aveva fissato un equilibrio tra la tutela della sicurezza dei prodotti e l'interesse a promuovere l'innovazione. Il quadro normativo relativo ai danni causati da prodotti e servizi viene completato dalle disposizioni nazionali, le quali generalmente presuppongono una condotta colposa da parte di soggetti quali produttori, fornitori di servizi o utenti stessi di un prodotto (responsabilità per colpa). Al contrario, altre disposizioni adottano un regime di responsabilità oggettiva, identificando come responsabili dei danni scaturiti dal servizio l'operatore, l'imprenditore o lo stesso utente che svolgono un'attività pericolosa. In questi casi, la responsabilità viene attribuita indipendentemente dalla condotta assunta precedentemente alla messa in commercio del prodotto.

La direttiva 85/374/CEE, armonizza a livello europeo le domande di risarcimento contro i produttori per danni causati ai consumatori da prodotti difettosi. I produttori vengono considerati responsabili per i danni causati dai loro prodotti, purché la parte lesa dimostri il danno, il difetto e il nesso causale tra questi ultimi. Questa direttiva copre

un'ampia gamma di prodotti, dalle materie prime ai dispositivi complessi basati sull'IA, e la sua applicazione dipende dalle normative nazionali riguardanti l'onere probatorio e l'accertamento del nesso causale[150].

Nonostante le numerose direttive e i passi verso un regime regolamentare armonizzato a livello europeo, il rapporto di valutazione del 2018 sulla Direttiva sulla Responsabilità per Danno da Prodotti Difettosi (PLD) ha messo in luce l'inadeguatezza dell'attuale regime di responsabilità civile nel compensare il pubblico dei danni arrecati da sistemi di IA. L'inadeguatezza deriva dall'incertezza giuridica sull'applicazione della norma a beni intangibili come software e dati, che costituiscono gli strumenti fondamentali per il funzionamento dei sistemi di IA. Dubbi vertono anche sull'identificazione del soggetto responsabile per i danni causati da tali dispositivi. A ciò si devono aggiungere le particolari vulnerabilità delle nuove tecnologie, il cui funzionamento comporta rischi non adeguatamente coperti dalla PLD, come la fragilità del sistema rispetto ad alcuni input di dati e i rischi di cibersicurezza. Inoltre, si osserva che le caratteristiche specifiche dell'IA, come l'opacità e l'autonomia, rendono difficile per il consumatore soddisfare l'onere della prova previsto dalla PLD, che richiede la prova del difetto del sistema di IA[151].

Alla luce delle diverse criticità evidenziate in merito alla possibilità di applicare la PLD nella sua attuale forma ai danni da algoritmo, le istituzioni dell'Unione europea hanno ritenuto necessario intervenire per evitare che il quadro normativo vigente venisse applicato troppo estensivamente a livello nazionale da tribunali e autorità di settore. Qualora gli Stati membri fossero intervenuti elaborando singole politiche di adattamento, avrebbero aumentato la frammentazione normativa e l'incertezza giuridica degli operatori sul trattamento normativo dei sistemi di IA nel mercato europeo. Pertanto, la Commissione Europea, nel White Paper on AI del 19 febbraio 2020, manifestava la necessità di un quadro normativo europeo comune per rispondere ai rischi associati a questa nuova tecnologia. Il Parlamento, in risposta, approvava la risoluzione del 20 ottobre 2020, sul regime di responsabilità civile per l'Intelligenza Artificiale, nella quale invitava la Commissione a redigere delle proposte di regolazione a tal riguardo. Il

[150] Commissione UE, Inception Impact Assessment, Ref. Ares(2021)4266516 - 30/06/2021, disponibile sul sito dell'organo;
[151] Parlamento UE, Artificial intelligence liability directive, redatto da EPRS - European Parliamentary ResearchService, disponibile sul sito web dell'organo;

documento sottolineava ancora una volta l'inadeguatezza delle norme vigenti, tra le quali i già menzionati Product Liability Directive (PLD) e General Data Protection Regulation (GDPR), ai quali si aggiunge la Digital Content and Services Directive. Di conseguenza, entrambe le autorità hanno ritenutp necessario un profondo intervento normativo per regolare la nuova tecnologia. La riforma avrebbe dovuto aggiornare la disciplina, partendo dalla stessa definizione di prodotto, la cui attuale definizione, infatti, non avrebbe incluso i nuovi ritrovati della tecnica. Allo stesso modo anche il concetto di difetto avrebbe dovuto adattare la fattispecie alla nuova casistica dei software. La risoluzione, sebbene non giuridicamente vincolante, non si è limitata ad evidenziare le criticità riscontrate nella PLD, ma si è spinta sino alla formulazione di un testo legale completo per la regolamentazione dell'IA, proponendo due regimi di responsabilità basati sul livello di rischio di tali sistemi[152].

La risoluzione del Parlamento sollecita la Commissione a elaborare un regolamento che assicuri una completa armonizzazione, stabilendo così un quadro legale omogeneo. Questo assetto dovrebbe completare la PLD e assegnare la responsabilità principalmente agli operatori dei sistemi di IA. Costoro si distinguono tra addetti di "frontend", definiti come «natural or legal person who exercises a degree of control over a risk connected with the operation and functioning of the AI-system and benefits from its operation», e operatori di "backend" che definiscono «the features of the technology, provides data and essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system»[153]. In merito al regime di responsabilità civile da adottare, la risoluzione propende per la responsabilità oggettiva esclusivamente nei confronti dei sistemi di IA ad alto rischio. Per tutti gli altri sistemi, si adotta invece la responsabilità per colpa, accompagnata da un'inversione dell'onere della prova. Inoltre, per quanto concerne i meccanismi di compensazione, il Parlamento suggerisce alla Commissione di consultare il settore assicurativo per creare prodotti che colmino le eventuali lacune residue nel sistema di compensazione previsto. Infine, la risoluzione incoraggia gli Stati membri a creare un fondo speciale, con lo scopo di corpire danni eccezionali o temporanei, come quelli arrecati ad un'intera collettività,

[152] Parlamento UE, Civil liability regime for artificial intelligence, disponibile sul sito dell'organo al link: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html ;
[153] Le definizioni di operatori di frontend e backend si trovano nella risoluzione del Parlamento UE, Civil liability regime for artificial intelligence,

ovvero per risarcire il danno prodotto da un sistema di IA non ancora classificato ad alto rischio, e pertanto non ancora assicurato[154].

Tuttavia, la proposta del Parlamento non risolve le principali criticità rilevate nell'applicazione della PLD. La critica principale riguarda proprio l'incerta definizione della terminologia utilizzata. In particolare, si rinviene una definizione troppo ampia dei sistemi di IA e della distinzione tra tecnologie ad alto e basso rischio. Ebbene, l'indeterminatezza delle fattispecie comporterebbe un aumento dell'incertezza giuridica, in quanto la qualificazione del sistema determina in modo diretto il regime di responsabilità applicabile. A seconda della categoria di riferimento del prodotto, si potrà applicare la responsabilità oggettiva o quella per colpa. Il sistema di responsabilità delineato opta per un doppio binario, che impone un regime di responsabilità oggettiva per tutti gli operatori di sistemi ad altro rischio[155], mentre richiede la prova della colpa per tutti gli altri; l'azione risarcitoria in tal caso sarebbe soggetta «in relation to limitation periods as well as the amounts and the extent of compensation, to the laws of the Member State in which the harm or damage occurred»[156]

Un'ulteriore critica avanzata verso l'assetto determinato dalla risoluzione consiste nella mancata previsione di regimi di responsabilità speciali per particolari attività o professioni (e.g. responsabilità sanitaria o responsabilità del vettore). Il regolamento proposto potrebbe infatti portare a un livellamento dei regimi speciali previsti dai singoli ordinamenti nazionali, orientandoli verso il regime di responsabilità per colpa, applicabile a tutti i sistemi non classificati come ad alto rischio. Si prevede che questi ultimi rappresenteranno la maggior parte dei prodotti sul mercato, con il risultato di alterare gli equilibri stabiliti dai precedenti regimi di responsabilità professionale e imprenditoriale. A ciò si deve aggiungere la difficoltà nell'accertamento del livello di rischio di un sistema di IA prima della sua messa in commercio, nonché la necessità di aggiornare continuamente l'allegato che elenca i sistemi di IA ad alto rischio.

[154] Vedi vedi considerando n. 22 della risoluzione del Parlamento UE, Civil liability regime for artificial intelligence, Doc. cit.
[155] Art. 4 della risoluzione del Parlamento UE, Civil liability regime for artificial intelligence, Doc. cit.;
[156] Cit. Art. 8 della risoluzione del Parlamento UE, Civil liability regime for artificial intelligence, Doc. cit.;

Anche la definizione dei soggetti responsabili, operatori di "front-end" e "back-end", è stata ritenuta eccessivamente ampia e generica, in quanto non permetterebbe di distinguere le responsabilità dei diversi attori coinvolti nella catena di produzione e distribuzione del prodotto. La distinzione è rilevante in quanto ogni operatore controlla un rischio specifico, e non è sempre chiaro a quale malfunzionamento si possa ricordurre il danno. L'incertezza nell'individuazione del soggetto responsabile in caso di concorso di cause alternative potrebbe pregiudicare l'effettività della tutela; infatti, se il ricorrente chiama in giudizio la parte sbagliata, potrebbe non ottenere il risarcimento o vedere lievitare le spese di giudizio.

In ultimo, il Parlamento ha suggerito di limitare l'importo[157] e il tipo di danni risarcibili, compensando soltanto quei danni che dipendano da «adverse impact affecting the life, health, physical integrity of a natural person, the property of a natural or legal person or causing significant immaterial harm that results in a verifiable economic loss»[158]. Ebbene le limitazioni previste potrebbero determinare delle disparità di trattamento tra le vittime di tecnologie avanzate e ad alto rischio rispetto a quelle che hanno subito danni da sistemi categorizzati a più basso rischio. Il differente regime giuridico potrebbe rifletteresi sul mercato e sulla ricerca, scoraggiando l'adozione, e ancor prima lo sviluppo, di sistemi di IA avanzati, determinando dunque un rallentamento del progresso tecnologico in Europa[159]. Di conseguenza, il quadro normativo delineato nella risoluzione del 2020 potrebbe disincentivare le imprese ad entrare nel mercato digitale europeo. Il regolamento diventerebbe la norma di riferimento per la responsabilità civile solamente per i sistemi ad alto rischio, lasciando tutti gli altri sistemi soggetti alle normative nazionali. Pertanto, il regolamento non semplificherebbe il quadro normativo applicabile, ma si aggiungerebbe alle disposizioni nazionali già in vigore. Il sistema a

[157] L'Art. 5 della risoluzione del Parlamento UE, Civil liability regime for artificial intelligence, Doc. cit. limita l'importo del risarcimento dei danni « up to a maximum amount of EUR two million in the event of the death of, or in the event of harm caused to the health or physical integrity of, an affected person, resulting from an operation of a high-risk AI-system; up to a maximum amount of EUR one million in the event of significant immaterial harm that results in a verifiable economic loss or of damage caused to property, including when several items of property of an affected person were damaged as a result of a single operation of a single high-risk AI-system»;

[158] Cit. Art. 3 lett *i* , della risoluzione del Parlamento UE, Civil liability regime for artificial intelligence, Doc. cit. ;

[159] Per una panoramica della risoluzione del 20 ottobre 2020 e delle sue criticità vedi A. Bertolini, *Artificial Intelligence does not exist! defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies*, in Europa e diritto privato, 2022, p. 384;

doppio binario, così delineato, determinerebbe difficoltà sia per le imprese che per i danneggiati. Da un lato, le imprese si troverebbero ad affrontare incertezze giuridiche causate dell'ambiguità dei termini e della qualificazione dei sistemi ad alto rischio, nonché difficoltà in merito all'applicazione di disposizioni nazionali antiquate e inidonee a trattare i danni arrecati da tutti i tipi di sistemi di IA. Dall'altro canto, le vittime incontrerebbero difficoltà nel finalizzare le richieste di risarcimento danni per le medesime incertezze che affliggono gli operatori.

Orbene, questo primo tentativo di regolazione della responsabilità civile per i danni prodotti dai sistemi di IA ha dimostrato come uno strumento normativo ambiguo possa incidere in modo rilevante sia sul pubblico, qualora non garantisca un sistema di compensazione sicuro ed efficacie, sia sul mercato, che apparirà a sua volta instabile a causa degli incalcolabili costi amministrativi e giudiziari.

L'inadeguatezza della soluzione proposta dal Parlamento UE potrebbe essere addebitata alla mancata considerazione delle caratteristiche degli algoritmi di IA che suscitano maggiori preoccupazioni: complessità, autonomia e opacità. L'autonomia operativa e la mancanza di trasparenza nelle risposte fornite dall'intelligenza artificiale pongono rilevanti difficoltà per i consumatori, a partire dalla fase di dimostrazione del malfunzionamento o dell'erronea valutazione effettuata dal sistema. La difficoltà nel soddisfare l'onere probatorio aumenta se si considera che il processo di programmazione e costruzione del sistema coinvolge diversi attori - tra scienziati, professionisti e imprenditori - non coordinati tra loro e spesso locati in giurisdizioni diverse. In un contesto tecnico così complesso, l'onere della prova per ottenere il risarcimento dei danni da algoritmo è particolarmente oneroso. Le difficoltà nel dimostrare il difetto, la colpevolezza e il nesso causale possono lasciare le vittime senza tutela; lasciare che siano i giudici a colmare la lacuna è imprudente, poiché potrebbe intensificare la diffidenza verso la tecnologia IA, soprattutto qualora le prime domande di risarcimento vengano rigettate a causa delle difficoltà probatorie[160].

Alla luce dell'incapacità della PLD nell'affrontare l'impatto disruptivo dell'IA e delle critiche mosse alla risoluzione del Parlamento, ad oggi perdura il dibattito sulla soluzione

[160] M. Faccioli, *La responsabilità civile per danni cagionati da sistemi di intelligenza artificiale nel prisma dell'onere della prova*, in Responsabilità Civile e Previdenza, 2024, p. 950;

giuridica più adatta per affrontare i danni prodotti dall'IA. Infatti, benché sia chiaro a istituzioni e attori del mercato la necessità di un nuovo e speciale regime di responsabilità civile per questi sistemi, la decisione appare ardua soprattutto in considerazione della molteplicità di funzioni da essa assolte nel sistema socioeconomico. Il sistema di responsabilità legale rappresenta *in primis* lo strumento per garantire il rispetto delle normative sul rischio e, *in secundis*, determina l'allocazione delle responsabilità tra le parti coinvolte, in base alla loro condotta ed i rischi associati alla loro attività[161]. Infine, il quadro regolatorio assicura una giusta compensazione alle persone danneggiate e funge da deterrente rispetto a condotte dannose o opportunistiche degli operatori di IA. La definizione del nuovo sistema di responsabilità, richiederà quindi in primo luogo di individuare la parte responsabile tra tutti gli attori coinvolti: produttori, operatori, detentori, utenti o il sistema di IA stesso. A loro volta sono molteplici anche i criteri papabili per allocare la responsabilità in modo efficiente; ad esempio: il controllo sul rischio potrebbe suggerire la responsabilità di produttori e operatori; i benefici derivanti dall'uso dell'IA potrebbero coinvolgere produttori, operatori e utenti; mentre l'autonomia della tecnologia potrebbe far propendere per la responsabilità dell'IA stessa[162]. Queste sono le considerazioni che hanno guidato la Commissione europea nella proposta di due direttive per la riforma della PLD e per uniformare alcuni aspetti della tutela extracontrattuale apportata dagli Stati membri per i danni da algoritmo.

2) Le proposte normative della Commissione Europea: la proposta di riforma della Product Liability Directive e l'AI Liability Directive

Le disposizioni attuali non riescono ad interfacciarsi con tutte le caratteristiche dell'IA: la PLD non risolve l'asimmetria informativa tra utente e produttore, mentre il GDPR affronta solo i rischi del trattamento automatizzato dei dati personali personale - che impatta significativamente sulla persona - ma non fornisce strumenti per rilevare le

[161] N. Muftic, *Understanding the Risks of Artificial Intelligence as a Precondition for Sound Liability Regulation*, Op. cit. p. 86;
[162] N. Muftic, *Understanding the Risks of Artificial Intelligence as a Precondition for Sound Liability Regulation*, Op. cit. p. 96;

discriminazioni algoritmiche, infine la Digital Content and Services Directive dispone solo in materia di responsabilità contrattuale tra cliente e provider. La Commissione, preso atto della lacuna normativa, ha pubblicato un pacchetto di atti strettamente interconnessi e volti a regolare le misure necessarie per minimizzare i rischi legati all'IA allo scopo di proteggere i diritti individuali. Gli atti menzionati prevedono, al contempo, disposizioni che regolano le ipotesi di responsabilità civile in caso di violazione. Sicurezza e responsabilità sono infatti due volti della stessa medaglia, si applicano in diversi momenti e si rinforzano l'un l'altra[163]. Questa stretta interconnessione ha ad oggetto l'AI Act e l'AI Liability Directive (AILD), che dovrebbero rappresentare i due pilastri fondamentali nella strategia dell'Unione Europea sulla Digital Age. Pubblicate nel settembre 2022, queste proposte mirano a integrare il nuovo Regolamento con la normativa esistente per rispondere ai nuovi rischi dell'economia digitale. Come premesso nel capitolo precedente, l'AI Act, entrato in vigore nell'agosto 2024, definisce un quadro normativo per la governance dei sistemi di IA, con particolare attenzione a quelli considerati ad alto rischio. Parallelamente, la proposta AILD cerca di armonizzare le questioni procedurali, come la divulgazione delle prove e l'onere della prova, nei regimi di responsabilità civile degli Stati membri, collegandosi strettamente agli obblighi e alle condizioni di liceità poste dall'AI Act. Accanto a queste, la Commissione ha proposto anche un intervento di riforma e aggiornamento della Liability for Defective Products Directive (PLD), che amplia l'ambito di applicazione ai prodotti digitali, con particolare attenzione all'IA. Questi atti normativi sono tra loro complementari ed evidenziano un approccio integrato: l'AI Act si concentra sulla regolamentazione specifica e la supervisione, mentre le proposte AILD e PLD mirano ad incentivarne la compliance attraverso il sistema di responsabilità civile. Questo approccio coordinato, diretto e indiretto, riflette l'obiettivo dell'UE di creare un ambiente regolatorio equilibrato che promuova l'innovazione tecnologica senza trascurare la protezione degli utenti e la compensazione dei danni. L'impatto globale della regolamentazione dell'IA da parte dell'UE, conosciuto come "effetto Bruxelles", potrebbe influenzare le normative di altre

[163] Cit. Commissione UE, Proposta di Direttiva Del Parlamento Europeo E Del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (AILD), Bruxelles, 28 settembre 2022 COM(2022) 496 final 2022/0303 (COD);

giurisdizioni, sottolineando l'importanza di una regolamentazione ben calibrata in un contesto altamente competitivo e innovativo[164].

L'interconnessione tra le direttive sulla responsabilità e l'AI Act ha ad oggetto le regole preventive che quest'ultimo dispone sull'immissione sul mercato, la messa in servizio e l'uso di tali sistemi. In particolare, le direttive concorreranno ad assicurare il rispetto del sistema di governance articolato su quattro livelli di rischio, ciascuno caratterizzato da requisiti di liceità e obbligazioni. Pertanto, sebbene l'AI Act non disciplini direttamente la responsabilità civile, esso incide su di essa in maniera indiretta, in quanto le sue disposizioni costituiranno i parametri utili a valutare la conformità della condotta dei soggetti obbligati. Come illustrato in precedenza, spetta agli stessi operatori classificare il loro sistema nel corretto livello di rischio e riportarlo in una valutazione d'impatto. In questa valutazione il fornitore, ad esempio, dovrà anche documentare le misure adottate per ridurre la portata del rischio e la probabilità che si verifichi[165]. Ne consegue che, per accertare la liceità della condotta del soggetto regolato, si dovrà fare valutare il livello di compliance rispetto alle prescrizioni dell'AI Act; per cui il fornitore sarà ritenuto responsabile qualora non abbia attuato «adeguate pratiche di governance e gestione dei dati»[166], o non abbia garantito set di dati di addestramento, convalida e prova che siano pertinenti, rappresentativi, esenti da errori e completi.

Pertanto, le due direttive poggiano direttamente sul quadro di norme dell'AI Act per definire gli elementi delle condotte illecite rilevanti ai fini del risarcimento del danno da algoritmo. Il sistema di responsabilità concorre in questo modo ad assicurare l'efficacia delle norme sull'IA all'interno di un sistema di governance che, in prima istanza, affida agli organismi di valutazione della conformità l'accertamento della liceità dei software prima di autorizzarne il commercio sul mercato europeo. In tale contesto la responsabilità civile costituisce lo strumento che consente l'accertamento e la coazione delle disposizioni dell'AI Act, in quanto il legislatore è consapevole che potrebbe residuare una percentuale di rischio che si verifichi il danno, o che nuovi rischi emergano a causa della capacità di autoapprendimento. In questa prospettiva è ben possibile osservare come le

[164] P. Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*, in Computer Law & Security Review, 2023, p. 1;
[165] M. Faccioli, *La responsabilità civile per danni cagionati da sistemi di intelligenza artificiale nel prisma dell'onere della prova*, Op. cit. p. 956;
[166] Considerando 67, del Regolamento UE 2024/1689;

direttive del 2022 mirino ad aggiornare le norme sulla responsabilità, creando un sistema integrato che si occupi sia della prevenzione (tutela ex ante) sia la compensazione (tutela ex post) dei danni causati dai sistemi di IA[167].Quindi, la Commissione europea ha adottato una strategia intermedia che combina l'aggiornamento della Direttiva 85/374/CEE e l'introduzione di norme specifiche per i danni causati dall'IA. Questo "pacchetto" di misure mira a garantire sia un adeguato funzionamento del mercato interno, sia un elevato livello di protezione per i consumatori e le vittime. Infatti, l'obiettivo primario è di assicurare che il mercato interno funzioni correttamente garantendo, in sostanza, gli stessi diritti fondamentali e principi democratici messi a rischio dai sistemi di IA ad alto rischio, per i quali sono previsti maggiori obblighi e requisiti.

In particolare, il primo obiettivo della Commissione è stato l'aggiornamento delle norme sulla responsabilità civile per adeguarle alle caratteristiche e ai rischi delle nuove tecnologie e dei modelli di business digitali, inclusi i prodotti e servizi dotati di IA. Ciò fornirà alle imprese la stabilità legale necessaria per pianificare i loro investimenti, valutare la loro esposizione alla responsabilità, assicurarsi e immettere sul mercato prodotti sicuri, innovativi e sostenibili. Il secondo obiettivo, invece, è ridurre tutte le difficoltà che le vittime potrebbero incontrare in giudizio per ottenere il risarcimento per i danni arrecati da un'IA assicurando, in questo modo, che le parti lese dai sistemi di IA siano protette in modo uniforme in tutta l'Unione europea. Infine, il terzo obiettivo ha ad oggetto valutazioni politico-economiche sottese alla necessità di un quadro di tutela uniforme rispetto ai danni da algoritmo al fine, da un lato, di evitare la fuga verso regole nazionali percepite come più favorevoli ai danni causati dall'IA, e dall'altro di attrarre investimenti pubblici e privati nel settore. Allo scopo di tutelare l'innovazione il legislatore europeo ha scongiurato regole troppo penalizzanti per le imprese, in particolare per le PMI e le start-up[168]. Inoltre, una scelta politica unitaria è cruciale, specialmente considerando la competizione tecnologica con altre potenze economiche e geopolitiche rappresentate Stati Uniti e Cina. Dunque, il "pacchetto IA" composto dal regolamento e dalle proposte direttive dovrebbe così guadagnare la fiducia nei prodotti e

[167] E. Bellisario, *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, in Danno e responsabilità, 2023, p. 153;
[168] E. Bellisario, *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, Op. cit. p. 155, l'A. concorre a specificare anche che «Sul fronte della tutela ex post, meno numerose, ma comunque varie sono le discipline complementari alla Dir. 85/374/CEE: alcune volte ad offrire una tutela contrattuale, altre dirette a coprire danni diversi»;

nei servizi innovativi, incoraggiando l'adozione delle nuove tecnologie da parte di consumatori e imprenditori, per ora intimoriti dall'incerta applicazione delle norme[169].

Ebbene, le soluzioni papabili per adeguare il sistema di compensazione e rimuovere gli ostacoli evidenziati sono molteplici. Una prima opzione è quella di alleggerire l'onere della prova, obbligando il produttore a fornire informazioni tecniche alla parte lesa e permettendo ai tribunali di dedurre il difetto di un prodotto o il nesso causale tra la loro condotta ed il danno[170]. Un'altra soluzione potrebbe consistere nell'inversione dell'onere della prova, imponendo al produttore di dimostrare la sicurezza del prodotto o la sua irrilevanza rispetto al danno. Potrebbe essere utile adattare la nozione di "difetto" e alleviare o invertire l'onere della prova in presenza di software più a rischio, eliminando l'eccezione del rischio di sviluppo, che potrebbe elidere totalmente la responsabilità dei produttori in presenza di un software dotato di deep learning; che pertanto includono lo sviluppo tra le caratteristiche del prodotto.

La soluzione proposta dalla Commissione, che trova fondamento legale nell'art. 114 del TFUE, ha suggerito un regime a doppio binario articolato in uno strumento di armonizzazione massima rappresentato dalla PLD e da un regime di responsabilità con armonizzazione minima previsto dalla proposta dell'AILD. Nonostante i riconosciuti vantaggi che deriverebbero dall'assunzione di un unico armonizzato regime di compensazione al livello europeo, la maggior parte degli Stati membri ancora preferisce mantenere autonomi meccanismi di perequazione degli interessi. Perciò, lo schema normativo proposto dalla Commissione ha strutturato due proposte separate, una specifica per l'IA e l'altra per la responsabilità dei prodotti, tra i quali ora sono inclusi anche quelli dotati di IA[171]. Tuttavia, questa scelta comporta problemi di delimitazione degli ambiti applicativi delle due direttive. La difficoltà nel distinguere tra i due strumenti è

[169] Cfr. la Commissione UE nell' "Inception Impact Assessment" sopra citato e suggerisce come superare I potenziali ostacoli che i danneggiati potrebbero incontrare nel«(i) ensure that injured parties are equally protected throughout the EU and (ii) create trust in innovative products and services, and in justice systems, while promoting consumer uptake of innovative technologies, including AI. This initiative will take into account the proposed AI Act, including, in particular, (i) the definition of AI, (ii) the requirements of the AI Act and (iii) risk-related considerations, as well as other EU safety legislation to ensure consistency and complementarity, while providing effective and proportionate solutions for liability»;

[170] Vedi Supra, si propone quale esempio di circostanza dalla quale dedurre il difetto del prodotto «when other products in the same production series have already been proven to be defective or when a product clearly malfunctions»;

[171] P. Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*, Op. Cit. p. 5;

giustificata anche dalla parziale sovrapposizione del loro ambito applicativo, la scelta non appare casuale, infatti, le due direttive presentano molti elementi comuni.[172].

Nello specifico la proposta revisione alla PLD allarga l'ambito di applicazione della direttiva agli smart-products e ai sistemi di IA, sovrapponendosi in questo modo allo "scope" della AILD. Infatti, secondo l'articolo 4 della nuova PLD, con il termine "prodotto" si intende qualsiasi bene mobile, compresi elettricità, file digitali e software, (anche se integrato in altri beni mobili o immobili). Inoltre, la direttiva qualifica quale "componente" «qualsiasi articolo, tangibile o intangibile, o qualsiasi servizio correlato, integrato in un prodotto o interconnesso». Tuttavia, contemporaneamente esclude il codice sorgente del software dalla nozione di prodotto, così come i software in open source sviluppati o forniti in un contesto non commerciale[173].

Ulteriore elemento in comune tra AILD e PLD è il riferimento agli obblighi imposti dall'AI Act, il cui inadempimento costituisce un difetto del software. Infine, entrambe le norme introducono lo strumento della esibizione delle prove, al fine di agevolare l'onere probatorio a vantaggio del danneggiato e di ridurre l'asimmetria informativa tra le parti. Proprio a causa di questi elementi comuni, alcuni esperti hanno paventato la sovrapposizione dei due strumenti normativi, sostenendo che i due siano tra loro assolutamente fungibili. Ciononostante, la Commissione UE si è dimostrata cosciente delle sovrapposizioni normative e ha confermato il proprio indirizzo legislativo statuendo scelta normativa «la PLD non è isolata e le vittime hanno spesso la possibilità di scegliere su quale base giuridica fondare la propria azione»[174], di conseguenza sembrerebbe che i due strumenti siano tra loro fungibili.

---

[172] T. S. Cabral, *Op-Ed: "The proposed AI Liability Directive: another piece of the puzzle for AI Regulation in the EU"*, che sul punto osserva: «unless significant amendments are introduced within the context of the legislative procedure, with the new Product Liability Directive offering a frequently more beneficial framework, it is possible that the AI Liability Directive will end up being a less important instrument in the context of liability arising from damage caused by AI-systems»;

[173] Considerando 13 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi, Bruxelles, 28.9.2022 COM(2022) 495 final, disponibile sul sito https://eur-lex.europa.eu/ ; Per un'analisi più approfondita sulle nuove categorie di prodotti inclusi nella nuova PLD vedi A. Cioni, *Nuovi pregi e vecchi difetti della proposta di direttiva sulla responsabilità da prodotto difettoso, con particolare riferimento all'onere della prova*, in Responsabilità Civile e Previdenza, 2023, pag. 661 e G. F. Simonini, *La responsabilità del fabbricante nei prodotti con sistemi di intelligenza artificiale*, Danno e Responsabilità, 2023, p. 442;

[174] Commissione UE, *Questions and answers on the revision of the Product Liability Directive Brussels*, 28 settembre 2022, in www.ec.europa.eu;

Quindi, sebbene le due proposte direttive abbiano ambiti di applicazione parzialmente sovrapposti, questo sistema duale offre una duplice opportunità al danneggiato: utilizzare un regime di responsabilità oggettiva ovvero uno che accerti la colpa. Facendo appello alla AILD, il danneggiato non dovrà dare prova del difetto del sistema di IA, bensì della mancanza di diligenza, rendendo più facile per il danneggiato provare il comportamento negligente del produttore. Questo approccio ha suscitato grande interesse tra le imprese, poiché offre incentivi per lo sviluppo di prodotti innovativi senza esporli a rischi legali insostenibili, come invece potrebbe avvenire in applicazione del regime di responsabilità oggettiva[175]. Pertanto, il sistema del doppio binario permette alle vittime di scegliere lo strumento normativo più aderente alle esigenze del caso concreto. Tale per cui, se il danno è stato causato da sistemi più semplici l'attore potrà rivolgersi alla PLD, in quanto appare ancora possibile provare il difetto del prodotto, grazie alle presunzioni accordate dalla direttiva. Invece, in tutti quei casi dove i danni sono provocati dai sistemi di IA impenetrabili, ad effetto scatola nera, si potrà far ricorso alla AILD. Quest'ultima consente all'attore di sostituire la prova del difetto del device dimostrando la negligenza del produttore nella fase di progettazione e sviluppo. Questa politica sembra avvicinare il sistema europeo al modello nordamericano che predilige l'uso della responsabilità per negligenza, rispetto al regime di responsabilità oggettiva[176].

La distinzione tra i due strumenti si rinviene anche nella modalità di utilizzo dell'IA nel contesto che ha prodotto il danno. La PLD pone l'accento sul ruolo del software quale prodotto o componente di altro prodotto, venduto o scambiato nel corso di un'attività commerciale. La AILD, invece, è diretta a risarcire solo i danni causati da un output o dalla mancata produzione di un output da parte di un sistema IA, anche qualora il danno venga arrecato indirettamente tramite l'attività del fornitore o dell'utilizzatore[177]. Questa seconda circostanza potrebbe occorrere, ad esempio, nel caso in cui un assicuratore

[175] G. F. Simonini, *La responsabilità del fabbricante nei prodotti con sistemi di intelligenza artificiale*, Op. cit., p. 450;
[176] G. F. Simonini, *La responsabilità del fabbricante nei prodotti con sistemi di intelligenza artificiale*, Op. cit. l'autore sul punto argomenta «Ci avviciniamo al sistema nordamericano di responsabilità per negligence, molto usato dai danneggiati anche rispetto a quello di strict liability (responsabilità oggettiva). L'azione in negligence parte dall'assunto che i soggetti che operano sul mercato vendendo prodotti ai consumatori sono tenuti dall'ordinamento ad una serie di cautele (duties of care) tese ad evitare la commercializzazione di prodotti insicuri. Appartengono a questa categoria di soggetti i produttori ed i venditori. Gli effetti dannosi inaspettati corroborano la richiesta dal danneggiato»
[177] Considerando 15 Proposta di Direttiva Del Parlamento Europeo E Del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale;

utilizzi un software per calcolare il grado di rischio di un cliente e determinarne una polizza. In tal senso la direttiva sembra richiamare il funzionamento dei processi decisionali automatizzati[178], comprendendo i casi in cui l'azione lesiva venga concretamente compiuta da un terzo che (colpevolmente o meno) faccia affidamento sulla valutazione automatizzata. Alla luce di queste considerazioni, l'AILD allarga l'ambito di applicazione della PLD, nel senso che non pone una tutela nei confronti degli esercenti del software in commercio, bensì nei confronti di chiunque metta in pericolo i diritti fondamentali in quanto faccia uso o venda un sistema di IA, nell'ambito della sua attività economico professionale. È quindi possibile che il danneggiato pretenda il risarcimento anche qualora non sia entrato a contatto diretto con il sistema IA, ma abbia patito danni a causa dell'utilizzo dell'operatore.

Il danno è imputabile al fornitore/utilizzatore del sistema di IA, se provata anche la negligenza o il difetto del prodotto. I due presupposti, negligenza e/o difettosità, sono definiti in modo diverso dalle due direttive. La PLD si basa sul criterio della mancanza di sicurezza che ci si può ragionevolmente aspettare dal prodotto. L'AILD, invece, considera difettosa o illecita l'IA che non rispetti i requisiti e le misure di sicurezza imposti dall'AI Act. In alcuni casi, queste definizioni coincidono, poiché entrambe richiedono che i software garantiscano l'adeguato livello di sicurezza informatica, obbligatorio per legge[179]. L'accezione di difetto per la PLD ha confini più ampi, ma non indefiniti in quanto l'accertamento del vizio deve essere condotto oggettivamente e non più in base alla personale aspettativa di sicurezza del danneggiato[180]. Questa asserzione deve però essere coordinata con il riferimento alle «specifiche aspettative degli utenti finali cui è destinato il prodotto»[181], usato dall'art. 6 della proposta riforma alla PLD per definire i prodotti difettosi. Sicché, la riformata PLD introdurrebbe una definizione di difetto basata sulle aspettative del grande pubblico, piuttosto che su quelle del singolo consumatore,

[178] Vedi art. 22 del Regolamento UE 679/2016 e il commento fatto nel par. 2 del Capitolo II di questo studio;
[179] Art 4 Ai Liability Act e considerando 24 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;
[180] Considerando 22 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;
[181] Cit. Art. 6, par. 1 lett. *h* della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;

come previsto dalla Direttiva 85/374/CEE[182]. In realtà, la proposta si rivolgerebbe alle specifiche aspettative degli utenti finali, cui è destinato il prodotto, confermando che se un prodotto è rivolto a una nicchia di utenti, le aspettative legittime da considerare sono quelle di questo specifico gruppo[183]. Attraverso questa precisazione la PLD dimostra di essere consapevole degli aspetti specifici dell'IA, come la capacità dei sistemi IA di apprendere dopo l'immissione sul mercato ed estendere la responsabilità dei produttori anche ai difetti emergenti; assicurando che le funzionalità adattive non causino comportamenti rischiosi. Infatti, la proposta considera l'obbligo di monitoraggio continuo del fornitore sui sistemi di IA ad alto rischio, e la conseguente responsabilità di quest'ultimo finché tale controllo è mantenuto, incluso il caso di controllo remoto. Infine, menziona tra i requisiti di sicurezza del prodotto intelligente la cibersicurezza, allineandosi con le normative esistenti e future dell'UE, con particolare attenzione ai software IA[184].

In conclusione, esiste una potenziale sovrapposizione tra le due direttive, tuttavia sussistono numerosi elementi che contraddistinguono i due strumenti, tali da distinguere, in fatto, i rispettivi ambiti applicativi: la PLD inquadra i danni arrecati dall'utilizzo dei prodotti intelligenti, mentre la AILD quelli che derivano, anche indirettamente, dall'output di un software. La fattispecie concreta quindi è ben delimitata, soprattutto perché raramente gli individui acquistano sistemi decisionali automatizzati ad alto rischio, rendendo l'AILD lo strumento adatto a perseguire i danni arrecati da istituzioni, professionisti o provider che ne fanno uso. Infine, acquistano importanza elementi di fatto nella scelta tra le due direttive, come: il tipo di sistema di IA implicato, il suo grado di trasparenza e, soprattutto le prove a disposizione dell'attore. Ciò in quanto l'attore propenderà per la AILD nel caso sia impossibile provare il difetto, altrimenti potrà beneficiare della responsabilità oggettiva della PLD.

[182] Infatti, l'art. 6 della Direttiva 85/36/CEE nella definizione di prodotto fa appello a delle considerazioni più ampie perché non fanno riferimento ad una particolare categoria di utilizzatori ma ritengono che «un prodotto è difettoso quando non offre la sicurezza che ci si può legittimamente attendere»;
[183] A. Cioni, *Nuovi pregi e vecchi difetti della proposta di direttiva sulla responsabilità da prodotto difettoso, con particolare riferimento all'onere della prova*, Op. cit. p. 664;
[184] P. Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*, Op. Cit. p. 15;

3) L’obbligo di esibizione delle prove e la presunzione “punitiva”

La principale innovazione introdotta nel regime di responsabilità extracontrattuale sui danni da IA concerne la prova del nesso causale che costituisce, nell’attuale quadro normativo, un ostacolo nell’imputazione della responsabilità per danni causati dai sistemi di IA. Le tecniche di autoapprendimento impediscono di collegare efficacemente il malfunzionamento dell’IA al processo di fabbricazione, sia per le diverse specializzazioni che vengono coinvolte nel processo di produzione, sia perché l’IA può modificare il proprio comportamento in base alle informazioni apprese dopo la sua cessione, per cui fuori dal concreto controllo del produttore. A questo scopo, La PLD, benché preveda ancora una responsabilità oggettiva, introduce dei meccanismi presuntivi per facilitare la prova del difetto e del nesso causale. Infatti, anche dimostrare il difetto nei prodotti dotati di sistemi di IA risulta particolarmente complesso a causa della natura autonoma e opaca degli algoritmi; questo richiede una comprensione dettagliata del loro funzionamento, degli obiettivi del sistema e dei dati utilizzati per l'addestramento. Tale difficoltà aumenta qualora l'IA sia integrata nei sistemi di IoT, dove molteplici dispositivi e servizi interagiscono tra loro, rendendo ancora più ardua l'identificazione della causa del danno e del soggetto responsabile[185].

Alla base della difficoltà nella prova del nesso causale risiede la necessità di garantire la trasparenza dei nuovi sistemi sviluppati. Questa deve essere assicurata attraverso documentazione e istruzioni chiare, anche riguardanti i possibili rischi per i diritti fondamentali e la discriminazione. L'opacità degli algoritmi, in particolare quelli basati sul machine learning, rende difficile comprendere il loro funzionamento e gli effetti prodotti, spesso caratterizzati da causalità non lineari e regole probabilistiche. Ad esempio, sarebbe utile per i conducenti di vetture dotate di sistemi avanzati di assistenza alla guida (ADAS), comprenderne le logiche operative, particolarmente in occasione di malfunzionamenti dell’IA nell’interpretazione di segnali stradali. Considerata l'opacità e l'imperfezione intrinseca dei sistemi di IA, il requisito del difetto diventa un ostacolo insormontabile nell’attuale regime della responsabilità da prodotto. Di conseguenza, si

[185] G. F. Simonini, *La responsabilità del fabbricante nei prodotti con sistemi di intelligenza artificiale*, Op. cit. p. 445;

tende a fare affidamento sul requisito della colpa, legato a una gestione aziendale inadeguata da parte del fornitore o dell'utente.

Orbene, proprio in considerazione del ruolo che assumono le regole sulla distribuzione dell'onere della prova nella valutazione del danneggiato sull'opportunità di intraprendere o meno un'azione risarcitoria, il pacchetto di regolamentazione sull'IA ha cercato di armonizzare le disposizioni in materia a vantaggio del danneggiato. In particolare, PLD e AILD adottano un approccio bilanciato composto da presunzioni legali e obblighi di divulgazione tra loro strettamente interconnessi. Tuttavia, è bene precisare che le presunzioni contemplate dalle direttive operino solo al verificarsi di determinate circostanze previste dalla legge, riducendo così la discrezionalità del giudice e aumentando la certezza del diritto. Le presunzioni sono accompagnate da obblighi di divulgazione, che consentono al danneggiato di ottenere le informazioni tecniche necessarie per dimostrare la responsabilità del produttore. Qualora il produttore non ottemperasse a tali obblighi, il giudice potrebbe dedurne la colpa o il difetto del prodotto, influenzando in modo determinante l'esito della causa[186].

Pertanto, la AILD accorda ai tribunali nazionali il potere di ordinare l'esibizione delle prove qualora il produttore non abbia ottemperato alla richiesta diretta del danneggiato di fruire la documentazione rilevante del sistema ad alto rischio sospettato di aver causato il danno. Entrambe le norme attribuiscono ai giudici il compito di limitare la divulgazione delle prove a quanto necessario, e in modo proporzionato per sostenere l'azione legale. L'ordine di divulgazione può essere emesso solo dopo che il danneggiato abbia dimostrato la plausibilità della sua richiesta. Il giudice deve pertanto garantire che la divulgazione sia necessaria e proporzionata, e che rispetti il segreto commerciale, bilanciando quindi le esigenze di entrambe le parti coinvolte. Il giudice nel determinare se la disclosure sia proporzionata o meno, deve operare un bilanciamento tra gli interessi legittimi delle parti e dei terzi; in particolare, devono essere salvaguardati i documenti protetti dalla tutela sul know-how e sulle informazioni commerciali riservate, ai sensi della direttiva (UE)

[186] E. Bellisario, *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, Op. cit. p. 160; Cfr. M. L. Scognamiglio, *Intelligenza artificiale e responsabilità civile: l'approccio dell'Unione europea – 1) Il quadro generale*, in n *ForoNews*, 5 dicembre 2023;

2016/943[187]. È possibile per l'autorità giurisdizionale contemperare l'interesse al segreto adottando le misure specifiche per preservare la riservatezza di tali informazioni qualora vengano menzionate nel corso del procedimento giudiziario[188].

La disclosure of evidence dovrebbe porre dunque rimedio all'asimmetria informativa tra le Big Tech ed il pubblico degli utenti; una simile soluzione era stata precendemente adottata dall'Unione Europea per agevolare le azioni di risarcimento dei danni derivanti da illeciti concorrenziali ai sensi della Dir. 2014/104/UE[189]. La disclosure garantisce una tutela giurisdizionale effettiva[190], come avallato dagli articoli 6 della CEDU e 47 della Carta di Nizza, in base ai quali il diritto a una tutela giurisdizionale presuppone il diritto alla difesa, la parità delle armi, l'accesso all'autorità giurisdizionale e la possibilità di farsi assistere da un legale.

In effetti, la difficoltà nel reperire le prove documentali è una questione affrontata dal legislatore anche in altre fattispecie. Ne è un esemptio il caso dell'azione di accertamento di una simulazione, in cui è concesso ai terzi interessati di impiegare presunzioni e testimonianze per provare l'accordo simulato, in deroga alle limitazioni imposte sull'accertamento dei rapporti contrattuali *ex* art. 2721 c.c. Questa opzione è apparsa necessaria nella dimostrazione della simulazione, poiché l'accordo dissimulato poteva essere anche solo verbale e completamente privo di documentazione scritta. Le direttive in commento, invece, fanno appello alla disclosure of evidence in quanto, grazie all'AI Act, i soggetti responsabili della produzione, del commercio e dell'utilizzo di IA ad alto rischio devono conservare la documentazione attestante le informazioni di cui all'allegato IV[191]. Pertanto, l'attore puó richiedere l'esibizione di documenti la cui conservazione è

[187] Cit. Art. 3 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale e art. 8 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;

[188] Vedi *supra.*

[189] Per una disamina della disclosure of evidence garantita dalla direttiva 2014/104/UE G. Finocchiaro, *La disciplina dell'esibizione delle prove risarcitori per violazione delle norme antitrust in attuazione della Dir. 2014/104/UE*, in *Nuove Leggi Civili Commentate*, 2018, p. 415;

[190] Considerando 32 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi e 20 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale;

[191] L'art. 11 del Regolamento UE 679/2024 dispone in merito alla forma e contenuto della documentazione tecnica che deve essere «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

obbligatoria per legge per il convenuto, al fine di certificare la conformità dei suoi sistemi. Sul punto si deve evidenziare che la documentazione tecnica obbligatoria è prevista solo per i sistemi di IA ad alto rischio, quindi, non coinvolge l'impiego di qualsiasi software; infatti l'art. 8 della direttiva di revisione della PLD, titolato "disclosure of evidence", seppur simile all'art. 4 della AILD, non comporta gli stessi effetti.

Entrambe le proposte direttive corredano la disclosure con delle presunzioni "punitive". In particolare, l'art. 3 della AILD rende evidente il legame a doppio filo tra divulgazione degli elementi di prova e presunzione relativa di non conformità in quanto previste nel medesimo dettato. L'inadempimento all'obbligo di esibizione comporta una presunzione di colpa a carico del fornitore per aver messo in commercio un sistema di IA ad alto rischio non conforme alle prescrizioni dell'AI Act. La presunzione puó essere superata in giudizio dimostrando di aver predisposto tutte le misure di riduzione del rischio, e di aver così rispettato l'obbligo di proteggere il pubblico dai danni potenziali associati all'IA. L'inadempimento a tale ordine comporterebbe la presunzione di veridicità degli elementi richiesti dall'attore, implicando la violazione del duty of care imposto dal Regolamento, che peraltro impone la tenuta della documentazione obbligatoria di cui all'art. 11[192]. Inoltre, sebbene l'AI Act preveda requisiti e obblighi specifici principalmente per i sistemi di IA ad alto rischio, tale presunzione può essere applicata anche ai sistemi a rischio minimo, qualora l'organo giudicante riconosca che per l'attore risulti eccessivamente complesso provare l'esistenza del nesso causale. Per espressa menzione dell'art. 3, par. 1, l'ordine di esibizione può essere rivolto solo a fornitori e utenti, poiché L'AI Act attribuisce obblighi esclusivamente a queste categorie. La scelta normativa è motivata dal fatto che solo il fornitore, che ha sviluppato il sistema, ovvero l'utente professionista, che lo utilizza in conformità con le istruzioni e le finalità previste, dispongono di una conoscenza sufficentemente approfondita e immediata del sistema stesso. Questo poichè, in determinate circostanze, entrambi avrebbero la capacità di esercitare controllo o autorità su di esso.

notificati, in forma chiara e comprensibile, le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti.»;

[192] L. M. Lucarelli Tonini, *L'IA tra trasparenza e nuovi profili di responsabilità: la nuova proposta di "Ai Liability Directive",* in Diritto dell'Informazione e dell'Informatica, 2023, p. 343 che in merito a

Diversamente, la direttiva di riforma della PLD conserva il difetto quale elemento centrale della fattispecie di responsabilità, e costruisce un sistema presuntivo per agevolare il danneggiato nella dimostrazione del malfunzionamento. L'art. 8 della PLD prevede una disclosure molto simile a quella prevista all'art. 3 della AILD. Infatti, anch'esso richiede all'attore di espletare un preventivo e stragiudiziale tentativo di accesso alla documentazione rilevante, nonchè la prova della plausibilità della domanda giudiziale. La presunzione del carattere difettoso del prodotto viene però disposta nel successivo art. 9, che si configura al ricorrere di una delle seguenti condizioni:

"a) il convenuto non ha rispettato l'obbligo di divulgare i pertinenti elementi di prova a sua disposizione a norma dell'articolo 8, paragrafo 1;

b) l'attore prova che il prodotto non rispetta i requisiti obbligatori di sicurezza stabiliti dal diritto dell'Unione o nazionale intesi a proteggere dal rischio del danno verificatosi; oppure

c) l'attore prova che il danno è stato causato da un malfunzionamento evidente del prodotto durante l'utilizzo normale o in circostanze ordinarie"[193].

Orbene, in merito alla prima condizione, riguardante la disattesa divulgazione degli elementi probatori, si possono riproporre le medesime considerazioni menzionate per l'art. 3 dell'AILD; in quanto anche in questo caso la presunzione opera quale conseguenza del mancato rispetto degli obblighi da parte del produttore. Tuttavia, la seconda condizione, pur condivisibile in astratto, non sembrerebbe realmente agevolare l'onere della prova per i danneggiati. Sebbene il mancato rispetto degli standard obbligatori da parte del produttore possa far presumere la difettosità del prodotto, per i prodotti particolarmente complessi, risulta estremamente difficile per il consumatore dimostrare tale inadempimento a causa dell'elevata tecnicità delle norme applicabili. Anche la terza condizione, per quanto corretta, non apporterebbe un miglioramento significativo alle condizioni processuali del consumatore. Infatti, come rilevato anche dalla Corte di Giustizia, le corti consentono già oggi di dedurre l'esistenza di un difetto attraverso la prova presuntiva, soprattutto qualora il danno fosse manifestamente il risultato di un

[193] Cit. Art. 9 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;

malfunzionamento evidente del prodotto occorso durante il suo normale utilizzo[194]. Tuttavia, mentre è relativamente semplice inferire il difetto per prodotti generalmente considerati innocui, risulta ben più complesso stabilire il nesso causale in casi in cui tale collegamento non sia immediatamente evidente.

Anche la nozione di difetto viene aggiornata per includere le caratteristiche dei sistemi di IA. Infatti, la nuova definizione di "prodotto difettoso" introdotta dall'art. 6 della PLD stabilisce che un prodotto è considerato tale quando non garantisce il livello di sicurezza che il grande pubblico può legittimamente aspettarsi. Il riferimento al "grande pubblico" costituisce un'evoluzione rispetto alla Direttiva del 1985, in cui il parametro di riferimento era basato sulle aspettative di sicurezza di un singolo individuo; pertanto, la nuova formula sposta l'attenzione sulla sicurezza e percezione della collettività. Inoltre, il regolamento amplia le circostanze rilevanti per l'accertamento del difetto, includendo le caratteristiche dell'IA, come la capacità del prodotto di continuare ad apprendere dopo la sua diffusione e gli effetti di eventuali interazioni con altri prodotti. Di particolare interesse è il riconoscimento che, per i prodotti destinati a specifiche categorie di utenti, le aspettative di sicurezza devono essere valutate tenendo conto delle esigenze particolari di quei gruppi. Infine, come evidenziato dal considerando 22[195] e in accordo con la giurisprudenza della Corte di Giustizia, i giudici possono dichiarare un prodotto difettoso anche senza accertarne il difetto effettivo, se questo appartiene a una serie di produzione già associata a difetti precedentemente riscontrati, per i prodotti connessi a rischi elevati per la persona[196].

La revisione del concetto di difetto appare doveroso in considerazione del particolare processo produttivo dei sistemi di IA. Nello specifico, i difetti nei sistemi di IA tendono a derivare più frequentemente da errori di progettazione piuttosto che da difetti di

[194] Vedi Corte giust. Ue, 21 giugno 2017, causa C-621/15, N.W e a. contro Sanofi Pasteur MSD SNC e altri; A. Cioni, *Nuovi pregi e vecchi difetti della proposta di direttiva sulla responsabilità da prodotto difettoso, con particolare riferimento all'onere della prova*, op. cit. p. 668;

[195] Il considerando 22 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi dispone che «La valutazione del carattere difettoso dovrebbe comprendere un'analisi obiettiva, senza prendere come riferimento la sicurezza che una determinata persona può legittimamente attendersi. La sicurezza che il grande pubblico può legittimamente attendersi dovrebbe essere valutata tenendo conto, tra l'altro, della finalità prevista, delle caratteristiche oggettive e delle proprietà del prodotto in questione, così come dei requisiti specifici del gruppo di utenti cui il prodotto è destinato. Alcuni prodotti, come le apparecchiature vitali, presentano un rischio particolarmente elevato di danno alle persone, per cui generano aspettative di sicurezza altrettanto elevate»;

[196] A. Cioni *Vedi Supra* p. 667;

produzione. Questo poiché la progettazione di tali sistemi coinvolge algoritmi complessi e decisioni cruciali che possono influenzarne significativamente il comportamento, in contrapposizione con i processi di produzione dei componenti software e hardware che seguono procedure standardizzate e controllate, riducendo così la probabilità di difetti legati alla produzione. Pertanto, la condotta dei produttori di sistemi di IA deve essere valutata in base a criteri di diligenza, il che implica un onere probatorio più elevato per i querelanti, i quali devono dimostrare che il difetto derivi da scelte progettuali inadeguate piuttosto che da errori di produzione[197]. Peraltro, il difetto di produzione nei sistemi di IA richiede l'intervento di esperti tecnici, in considerazione della complessità e varietà di componenti implicati nel funzionamento dell'IA. Il difetto potrebbe manifestarsi nell'hardware, ad esempio come problemi nell'assemblaggio o nella configurazione dei componenti, o più comunemente nel software, a causa di errori di programmazione nel codice sorgente. Tuttavia, la questione spesso si concentra sui difetti di progettazione, che vengono valutati secondo il criterio della "ragionevole alternativa di design". Poiché confrontare un sistema di IA con tecnologie tradizionali sotto controllo umano è complesso, dato che i sistemi di IA potrebbero eccellere in termini di sicurezza e prestazioni rispetto alle loro controparti non intelligenti, risulta più appropriato confrontarli con un sistema di IA di riferimento, funzionalmente comparabile e operante nelle stesse condizioni. La valutazione della sicurezza del prodotto intelligente dovrebbe quindi essere eseguita su base statistica rispetto a un sistema di IA di riferimento, «whereby this performance may be lowered by a certain percentage without resulting in a qualification as a defective product»[198]. Tuttavia, aprirebbe la questione sulla scelta di un sistema di IA da utilizzare quale parametro di riferimento. Data la capacità di autoapprendimento del software, due sistemi gemelli all nascita ma esposti ad ambienti differenti potrebbero non necessariamente manifestare gli stessi difetti.

Alla luce dell'analisi della presunzione e della definizione di prodotti rilevanti ai sensi della nuova PLD, si rivela un significativo ampliamento del suo campo d'applicazione. In particolare, un prodotto è considerato difettoso se il produttore non ha soddisfatto l'obbligo di divulgare prove rilevanti, se non rispetta i requisiti di sicurezza obbligatori, o

[197] M. C. Buiten, *Product liability for defective AI*, European Journal of Law and Economics, 2024, p. 255;
[198] Cit. J. De Bruyne, E. Van Gool e T. Gils, *Tort law and damage caused by ai systems*, in Artificial Intelligence, Law Cambridge University Press, 2021, p. 383;

se l'attore dimostra che il danno sia stato causato da un malfunzionamento evidente del prodotto durante un utilizzo normale[199]. L'ampiezza delle circostanze addotte dalla norma rispecchia l'estensione dell'applicazione della PLD, che ora copre sia i prodotti analogici sia quelli digitali, estendendo così la gamma di difetti da considerare. Inoltre, l'accoglimento delle istanze di risarcimento secondo le norme europee è subordinato alla presentazione di fatti e prove che ne sostengano efficacemente la plausibilità.

Il commento delle direttive rende evidenti le similitudini tra i meccanismi presuntivi da esse previsti, tuttavia sussistono differenze strutturali tra i due sistemi. La AILD, ad esempio, indirizza la richiesta di esibizione della documentazione «al fornitore, a una persona soggetta agli obblighi del fornitore o a un utente»[200], mentre la PLD si riferisce genericamente al convenuto. Inoltre, la proposta AILD introduce un sistema di divulgazione delle prove più articolato rispetto a quello previsto dalla PLD. Diversamente dalla PLD, la AILD impone al richiedente di chiedere preventivamente al convenuto la divulgazione delle prove, includendo anche una disposizione specifica per l'adozione di misure cautelari per la conservazione delle prove. Un ulteriore elemento distintivo della proposta AILD è la possibilità di attivare il meccanismo di divulgazione sia prima che durante il processo, mentre la PLD limita tale possibilità al momento in cui la causa è già stata registrata in tribunale. Questa differenza può incidere significativamente sui costi procedurali, riducendo le barriere economiche per l'accesso al risarcimento[201].

Le differenze procedurali introdotte dalle due norme potrebbero avere implicazioni dirette sulle modalità con cui i produttori affrontano le responsabilità legali. Nello specifico, l'articolo 10 della PLD dispone sulle esenzioni dalla responsabilità, elenca sette[202] circostanze che scagionano il produttore dalla responsabilità per il prodotto

[199] Art. 9 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;
[200] Cit. Art. 3 della Proposta di Direttiva Del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale)
[201] [201] P. Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*, Op. cit. p.18;
[202] L'articolo prevede le seguenti situazioni quali condizioni di esenzione della responsabilità (ad eccezione della lett. e) citata nel testo): a) nel caso del fabbricante o dell'importatore, che non ha immesso il prodotto sul mercato né lo ha messo in servizio; b) nel caso di un distributore, che non ha messo il prodotto a disposizione sul mercato; c) che è probabile che il difetto che ha causato il danno non esistesse al momento in cui il prodotto è stato immesso sul mercato, messo in servizio o, nel caso di un distributore, messo a disposizione sul mercato, o che tale difetto è sopravvenuto dopo tale momento; d) che il carattere difettoso è dovuto alla conformità del prodotto a regole imperative emanate dai poteri pubblici; f) nel caso del

difettoso messo in commercio. Tra queste, in particolar modo risalta la lett e) che esclude la responsabilità del fabbricante qualora «lo stato oggettivo delle conoscenze scientifiche e tecniche al momento dell'immissione del prodotto sul mercato o della sua messa in servizio oppure durante il periodo in cui il prodotto era sotto il controllo del fabbricante non permetteva di scoprire l'esistenza del difetto». Dal dettato citato sembrerebbe proprio che la proposta normativa preservi la controversa difesa del rischio da sviluppo, peraltro obbligando tutti gli Stati membri a integrarla, anche in quei Paesi che attualmente la escludono per alcuni o tutti i prodotti. Tuttavia, la norma non specifica chiaramente quale sia il riferimento temporale preciso per valutare tali conoscenze, generando ambiguità interpretative. Questa mancanza di chiarezza è particolarmente problematica nei settori altamente innovativi, dove l'applicazione della difesa del rischio da sviluppo risulta meno chiara, ma di maggiore importanza[203]. In realtà, l'eccezione del rischio da sviluppo potrebbe essere utilmente applicata anche ai sistemi di IA, ma richiederebbe una valutazione continua delle conoscenze scientifiche e tecniche, quindi prendendo in considerazione anche le fasi successive all'immissione in commercio del prodotto. Tuttavia, questa difesa dovrebbe essere esclusa nei casi in cui è ragionevole che possano emergere sviluppi imprevisti[204].

Per la struttura della disclosure la Commissione UE prende spunto dall'omologo strumento di common law[205], dove la discovery opera in sede stragiudiziale tra il potenziale attore ed il potenziale convenuto con ad oggetto qualsiasi documento rilevante per la causa, che le parti allegheranno nel fascicolo. In Italia l'istituto più vicino è l'"ordine di esibizione alla parte o al terzo" *ex* art. 210 c.p.c., che ricorre nel caso in cui le parti in giudizio vogliano produrre un documento o altro oggetto nella disponibilità della controparte, o di un terzo, e ne richiedono l'esibizione tramite un ordine del giudice. L'istituto non opera d'ufficio, è quindi necessaria la previa istanza dell'interessato (ad

fabbricante di un componente difettoso di cui all'articolo 7, paragrafo 1, secondo comma, che il carattere difettoso del prodotto è dovuto alla concezione del prodotto in cui è stato integrato il componente o alle istruzioni date dal fabbricante di tale prodotto al fabbricante del componente; oppure g) nel caso di una persona che modifica il prodotto come indicato all'articolo 7, paragrafo 4, che il difetto che ha causato il danno riguarda una parte del prodotto non interessata dalla modifica;

[203] A. Cioni *Vedi Supra* p. 676;

[204] J. De Bruyne, E. Van Gool e T. Gils, *Tort law and damage caused by ai systems*, Op. cit. p. 387;

[205] A. Higgins, *Open door disclosure in civil litigation*, in The International Journal of evidence & proof, 2012, p. 298;

eccezione del rito del lavoro dove i poteri istruttori del giudice sono più ampi[206]), la quale deve contenere: la specifica indicazione del documento o dell'oggetto, il suo contenuto e la rilevanza della prova nell'accertamento del diritto. In ultimo, ai sensi dell'art. 94 disp. att., si deve dimostrare, anche tramite presunzioni, il possesso in capo al destinatario dell'ordine dell'oggetto o del documento richiesto.

L'unico limite menzionato dalle direttive in commento all'obbligo di divulgazione è il rispetto del know-how, grazie al richiamo della direttiva UE 2016/943. All'art. 210 c.p.c., invece, si applicano gli artt. 200-202 c.p.c sull'inviolabilità del segreto professionale, del segreto di stato o del segreto d'ufficio. Ne consegue che, anche nella disciplina italiana, la tutela brevettuale o del diritto di proprietà intellettuale non è ostativa all'obbligo di produzione in giudizio. Tuttavia, sia il GDPR[207] che le direttive[208] in commento, riconoscono la rilevanza del segreto industriale, il quale comunque non dovrebbe giustificare un diniego alla richiesta dell'interessato dei documenti utili ad affermare il proprio diritto. Il software, quindi, gode di diversi strumenti di tutela; il diritto d'autore protegge la sua componente "scritta" (i.e. il codice sorgente), la tutela brevettuale[209] ed il segreto industriale[210], garantiscono una protezione che, pur essendo

[206] Artt. 421 e 437 c.p.c. ;
[207] Al considerando 63 afferma «Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.»;
[208] Entrambe le direttive richiedono che «When determining whether the disclosure is proportionate, national courts shall consider the legitimate interests of all parties, including third parties concerned, in particular in relation to the protection of confidential information and trade secrets within the meaning of Article 2, point 1, of Directive (EU) 2016/943", negli articoli che dispongono sulla disclosure of evidence.»
[209] Sul punto si osserva che in effetti, la tutela che meglio risponde alle caratteristiche e finalità del software è sicuramente quella di carattere industriale, il codice sorgente pur essendo un prodotto dell'ingegno manca del carattere creativo, inteso quale "forma espressiva", artistica, intellettuale. Il software è invece apprezzabile dal punto di vista funzionale quale elaboratore elettronico, destinato ad elaborare informazioni per ottenere l'output desiderato, quindi l'arricchimento dell'utilizzatore non si ferma al caricamento del programma ma si ottiene attraverso il risultato al quale il software è preposto[209]. In questo senso il software sembra più vicino all'oggetto del brevetto, in quanto assimilabile ad un metodo di produzione di beni immateriali o di realizzazione di un servizio. Infatti, la principale distinzione tra l'opera d'ingegno e l'invenzione è l'utilità pratica di quest'ultima, che quindi non esaurisce la sua funzione nell' attività puramente estetica o speculativa. Le tutele brevettuale e autoriale divergono sia per oggetto che per estensione, il diritto d'autore permette una tutela immediata sin dalla stesura del codice, mentre il brevetto prevede la presentazione della documentazione tecnica e dell'istanza patendo, però, il peso della disclosure avendo consegnato i dati tecnici cfr. E. Arezzo, *Protezione del segreto e tutela del software: convergenze, sovrapposizioni, conflitti*, in Il *Diritto Industriale*, 2018, 145;
[210] al quale la summenzionata direttiva UE 2016/943 ha fornito un riferimento normativo.

gratuita, dipende esclusivamente dalla capacità del titolare di impedire la divulgazione delle informazioni.

Ebbene, nessuna di queste tutele si pone quale generale ostacolo alla divulgazione delle informazioni tecniche del software, né ai sensi della normativa in commento, né ai sensi del vigente quadro normativo. La prova del malfunzionamento del software può dipendere dalla logica impostata dai programmatori, dal training condotto con un set di dati incompleto o fallace, o ancora dai criteri richiesti dall'acquirente per elaborare la decisione di loro interesse. Da ciò consegue che una discovery sul codice sorgente potrebbe essere utile solo nel primo caso, quello in cui il danno derivi dalle istruzioni sul quale il software è codificato[211]. Per gli altri casi, si rendono necessarie informazioni supplementari come le metodologie, le tecniche di addestramento e i set di dati utilizzati durante l'addestramento. Pertanto, nell'ottica di bilanciamento e proporzionalità tra esigenze istruttorie e interessi commerciali, sarebbe prima opportuno esaminare i criteri usati per compilare il codice o i dati impiegati nell'addestramento. A sostegno di questa soluzione "graduale", si deve notare che gli utilizzatori e gli acquirenti dell'IA tipicamente non dispongono del codice sorgente, bensì del codice oggetto, che consiste in un insieme di istruzioni e criteri espressi in linguaggio informatico. Pertanto, è più efficace analizzare inizialmente la descrizione dell'algoritmo e i criteri su cui è basato, per poi estendere la ricerca ad altri elementi qualora la causa del malfunzionamento resti oscura.

Alla luce di quanto detto, si evince come le direttive abbiano affrontato in modo coordinato la sfida di aprire la black-box, per accedere alle logiche di funzionamento e stabilire se e come l'IA abbia causato il danno. Entrambe le direttive superano l'opacità

[211] Sul punto si sofferma E. Prospetti in "*Accesso al software e al relative algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronounce del Tar Lazio"*, in *Dir. Inf*, 2019 nel quale commenta le pronunce del Tar Lazio nn. 3742 e 3769 del 2017, dove «Ad avviso dei giudici del TAR Lazio, infatti, le moderne modalità dell'azione amministrativa, che prevedono l'utilizzo di software per importanti parti di procedimenti amministrativi, giusticaficano una interpretazione del concetto di documento amministrativo particolarmente ampia e, in particolare, tale da ricomprendere anche il codice sorgente dei software utilizzati per svolgere elaborazioni nel corso del procedimento." In base a questo ragionamento il codice sorgente dovrebbe essere oggetto di accesso agli atti al pari di un normale e analogico provvedimento amministrativo, tuttavia l'autore osserva che "Il ragionamento potrebbe essere diverso in presenza di evidenza e nesso causale tra errori nelle indicazioni per la realizzazione del software ed errori nell'elaborazione. Tale aspetto avrebbe forse meritato una analisi maggiore a fronte di richieste di accesso al codice sorgente e, oltre a rilevare — come in una passaggio delle sentenze si legge — che vi sono incongruenze tra il contratto collettivo e i criteri di elaborazione riferiti dall'Amministrazione»;

del procedimento automatizzato con una presunzione di illiceità, qualora il produttore si rifiuti di esibire la documentazione tecnica necessaria per chiarire il funzionamento dell'algoritmo. Come osservato, infatti, il codice sorgente non è un dato indispensabile per analizzare il comportamento dell'automa, potrebbero essere sufficienti le informazioni così raccolte dalle parti e valutate del giudice che conduce l'istruttoria. Tuttavia, la nuova PLD continua a presentare delle lacune nel sistema di responsabilità civile da lei delineato. Infatti, la PLD conferma l'eccezione del rischio da sviluppo già presente nella versione attuale. Questa eccezione, pur offrendo protezione ai produttori di tecnologie avanzate e incentivi all'innovazione, esonera i produttori dalla responsabilità civile in molteplici settori; così trasferendo, di fatto, rispettivi rischi e costi sui consumatori. L'accoglimento del rischio da sviluppo presuppone che il fornitore dimostri che quando il prodotto è stato messo in commercio, il livello delle conoscenze scientifiche e tecniche disponibili non consentiva di individuare la presenza del difetto.

L'inversione dell'onere della prova in capo al danneggiato risulta inoltre un eccessivo aggravio nei confronti del consumatore, il quale non sempre è dotato di mezzi o delle conoscenze tecniche necessari per comprovare difetti tecnicamente complessi. Una soluzione equilibrata potrebbe consistere nell'istituzione di un fondo di compensazione specificamente dedicato alle vittime di rischi tecnologici. Il fondo sarebbe destinato a risarcire le persone danneggiate che, in assenza della difesa del rischio da sviluppo, avrebbero avuto diritto a un risarcimento, assicurando così una compensazione equa senza gravare ingiustamente sugli utenti finali. Inoltre, questo meccanismo contribuirebbe a ridurre i premi assicurativi per i produttori, mantenendo al contempo gli incentivi a prevenire danni evitabili. Pertanto, sarebbe auspicabile l'introduzione di un fondo di compensazione a livello europeo per i danni causati da difetti di sviluppo all'interno della proposta di direttiva sulla responsabilità del prodotto[212].

4) La presunzione di causalità, dal difetto dell'IA al danno

Una lettura sistematica del pacchetto AI rivela un'ulteriore discrepanza tra i due regimi di responsabilità, stavolta riguardante la prova del nesso causale e dell'elemento

[212] P. Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*, in Computer Law & Security Review, 2023, p. 29;

soggettivo. L'AILD testualmente presume l'esistenza della colpa ogni qual volta il soggetto responsabile non adempia alle misure imposte dal diritto UE, finalizzate a ridurre il rischio che si verifichi il danno lamentato[213]. Pertanto, la mancata tenuta ed esibizione della documentazione tecnica, attestante l'implementazione delle suddette misure di cui al capo II dell'AI Act, costituisce dato utile per dedurre la violazione del particolare duty of care imposto dal regolamento sul produttore. Tuttavia, non tutte le violazioni hanno lo stesso peso, spetta infatti ai giudici il compito di determinare se le misure non documentate fossero effettivamente destinate a prevenire il danno che si è verificato.

Invece, la proposta revisione della PLD ha mantenuto la propria impostazione no-fault, per cui non si richiede alcun accertamento sulla colpa, bensì la prova del difetto del prodotto e del nesso causale tra difetto e danno. Ebbene, come sopra riportato, il difetto può essere alternativamente presunto dalla mancata esibizione della documentazione obbligatoria (in caso di IA), dalla carenza dei requisiti di sicurezza o dallo stretto collegamento tra il malfunzionamento ed il danno. Sembrerebbe dunque che il regime introdotto da quest'ultima sia più vantaggioso per il danneggiato rispetto a quello dell'AILD, che, invece, prevede la prova della colpa. Il quadro delineato dalla Commissione nelle due direttive appare caratterizzato da una forte continuità, al punto da adattare l'istituto della disclosure of evidence e la presunzione ad essa associata in funzione della complessità tecnica e scientifica del caso. Va osservato che non tutti i software presentano la medesima complessità; solamente i produttori di software ad alto rischio sono obbligati a presentare la documentazione che comprovi il loro regolare funzionamento. In tutti gli altri casi, l'ordine di esibizione potrebbe non essere satisfattivo in quanto non vige l'obbligo di tenuta della documentazione di cui all'AI Act. Il quadro costruito dalle due direttive ha stabilito un regime adatto a rispondere a qualsiasi circostanza. Pertanto, si elencano tutte le fattispecie previste:

- IA a rischio moderato o minore deputata ad elaborare informazioni per produrre un output: il danneggiato dovrà provare solo il difetto ai sensi della PLD, alla cui tutela si aggiunge quella di cui all'art. 22 del GDPR sulla possibilità di accedere alla logica del funzionamento dell'IA;

[213] Cit. Considerando 22 Ai L. Directive;

- IA ad alto rischio deputata ad elaborare informazioni per produrre un output con il quale il danneggiato ha solo un contatto indiretto (ad es. perché l'IA utilizzata dall'assicuratore per valutare il livello di rischio dell'assicurato): il danneggiato potrà pretendere l'esibizione della documentazione obbligatoria imposta dall'allegato IV dell'AI Act in base agli artt. 3 e 4 dell'AILD per provare il malfunzionamento e la colpa dell'utilizzatore;

- IA ad alto rischio deputata a produrre un output che determina il funzionamento del prodotto nel quale è integrato: il danneggiato potrà avvalersi alternativamente di entrambe le direttive che prevedono la disclosure of evidence e la presunzione di illecito in caso di omessa o errata predisposizione della documentazione obbligatoria.

Ebbene, quest'ultima fattispecie, alla quale effettivamente potrebbero essere applicate entrambe le disposizioni in commento, implica un identico onere probatorio. Ciò poichè la violazione delle disposizioni dell'AI Act costituisce sia il difetto del sistema che l'inadempimento del dovere di diligenza, il quale configura la negligenza del produttore ai sensi dell'AILD. Pertanto, benchè in astratto la seconda richieda la prova dell'elemento soggettivo, questa può essere assolta con la medesima documentazione di cui si ordina l'esibizione.

Quindi è possibile osservare che l'opacità della black box è stata risolta dalla Commissione UE riportando al centro dell'attenzione la violazione del regolamento, piuttosto che il nesso causale tra difetto e danno. La AILD propone un'alternativa al regime di responsabilità oggettiva, proponendo un regime di responsabilità per colpa, che consente di individuare con maggiore certezza il soggetto responsabile. Tuttavia, è necessario agevolare il danneggiato in questo processo imponendo l'obbligo di divulgazione degli elementi di prova. Questo obbligo potrebbe includere la trasparenza, la comprensibilità e persino l'explainability dell'algoritmo, oltre a prevedere il controllo obbligatorio del sistema ad opera di un essere umano. Sebbene tale obbligo riguardi principalmente i sistemi di IA ad alto rischio, il principio di trasparenza che lo sottende può coinvolgere anche sistemi meno complessi, rendendoli più accessibili per chi intenda avanzare una richiesta di risarcimento[214].

[214] L. M. Lucarelli Tonini, *L'IA tra trasparenza e nuovi profili di responsabilità: la nuova proposta di "Ai Liability Directive"*, Op. cit. p. 344;

In questo contesto, si collocherebbe la presunzione di causalità tra la colpa del convenuto e l'output generato da un sistema di IA, come previsto dall'art. 4 della AILD. Tale presunzione si configura quando il danneggiato riesce a soddisfare tre condizioni cumulative: dimostrare la violazione di un obbligo di diligenza, dimostrare la plausibilità che tale violazione abbia influenzato l'output del sistema, e fornire la prova che il danno sia stato effettivamente causato da quell'output. Questa presunzione, concepita per agevolare la posizione del danneggiato, acquisisce particolare rilevanza nel contesto dei sistemi di IA ad alto rischio, dove il mancato rispetto delle norme tecniche rigorose può far emergere la responsabilità del fornitore. Nei confronti degli utenti, la presunzione si applica qualora non abbiano rispettato gli obblighi di monitoraggio, abbiano disatteso le istruzioni allegate al software o abbiano «esposto il sistema di IA a dati di input sotto il suo controllo che non sono pertinenti alla luce della finalità prevista del sistema a norma»[215]. Le ultime due condizioni sono indispensabili per correlare materialmente l'autonomia decisionale dell'IA con il danno arrecato, secondo il criterio civilistico della ragionevole probabilità[216].

Al contrario, l'art. 9, comma 3, della PLD introduce una presunzione di causalità tra il difetto di un prodotto e il danno subito, purché si dimostri che il prodotto sia difettoso e che la natura del danno sia coerente con il difetto in questione. Questa presunzione, apparentemente ispirata dalla normativa tedesca, opera principalmente sul piano della causalità individuale, richiedendo al danneggiato di provare l'esistenza del difetto e la coerenza tra il difetto stesso e il danno, basata su una legge scientifica di copertura. Tuttavia, l'utilizzo dell'espressione "generalmente coerente" solleva potenziali ambiguità interpretative, poiché potrebbe portare a una confusione tra causalità generale e individuale, lasciando spazio all'idea che sia sufficiente una mera plausibilità eziologica. La Commissione sembra voler ridurre l'onere probatorio a carico del danneggiato, ma senza un chiarimento, il nuovo meccanismo rischia di sovrapporsi alle presunzioni già esistenti, rendendosi di fatto ridondante[217].

---

[215] Cit. Art. 4, par. 3, Proposta di Direttiva Del Parlamento Europeo E Del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale);

[216] G. F. Simonini, *La responsabilità del fabbricante nei prodotti con sistemi di intelligenza artificiale*, Op. cit. p. 454;

[217] A. Cioni, *Nuovi pregi e vecchi difetti della proposta di direttiva sulla responsabilità da prodotto difettoso, con particolare riferimento all'onere della prova*, Op. cit. p. 670, che in merito alla vicinanza alla

Infine, qualora la divulgazione degli elementi di prova non sia risolutiva, il legislatore europeo ha previsto un regime di presunzione del nesso causale, applicabile a tutti i sistemi di IA, qualunque sia il rischio che li contraddistingue. Di fatto, entrambe le Direttive estendono le presunzioni descritte anche a sistemi di IA non ad alto rischio «qualora un giudice nazionale ritenga che il ricorrente abbia di fronte eccessive difficoltà nella prova del difetto o del nesso causale, a causa di complessità tecnica o scientifica del prodotto»[218]. La AILD, invece, riconosce la presunzione qualora sia «eccessivamente difficile per l'attore dimostrare l'esistenza del nesso di causalità»[219]. L'estensione della presunzione anche ai sistemi non classificati come ad alto rischio, che rappresentano la maggior parte dei software di IA, mira a conciliare due obiettivi. Da un lato, il principio della neutralità tecnologica, che impone al legislatore di non favorire una tecnologia rispetto a un'altra, permettendo a individui e organizzazioni di scegliere il prodotto più adatto alle proprie esigenze. Dall'altro, risponde alla necessità di una regolamentazione adeguata e proporzionata di fronte alla complessità intrinseca dei sistemi di IA. Tuttavia, il concetto di "difficoltà eccessive" appare ambiguo, rischiando di attribuire al giudice un'eccessiva discrezionalità su una questione cruciale come il riparto dell'onere della prova. Alcuni studiosi suggeriscono che, piuttosto che mantenere un approccio di neutralità tecnologica, sarebbe più efficace riconoscere la peculiarità di alcuni prodotti e predisporre regole di responsabilità specifiche. Qualora si decidesse di proseguire con la neutralità, sarebbe opportuno definire un elenco, seppur non esaustivo, di prodotti che presentano particolari difficoltà probatorie, o almeno chiarire che il parametro di riferimento per valutare tali difficoltà deve essere il "grande pubblico" e non il singolo consumatore[220].

Nonostante lo scopo comune delle due direttive sia quello di sostenere il mercato delle nuove tecnologie e difendere il pubblico dall'opacità dell'algoritmo, esse presentano

---

legislazione tedesca rileva che « nel § 84 dell'Arzneimittelgesetz, per far scattare la presunzione di causalità individuale, si richiede che il medicinale — almeno teoricamente — sia «in grado» di essere la causa del danno, dando così evidentemente per assunta l'esistenza di una verificata legge scientifica»

[218] Cit. Art. 9, par. 4, della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;

[219] Cit. art. 4 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale);

[220] A. Cioni, *Nuovi pregi e vecchi difetti della proposta di direttiva sulla responsabilità da prodotto difettoso, con particolare riferimento all'onere della prova*, Op. cit. p. 682;

notevoli divergenze strutturali, come l'ambito di applicazione, le fattispecie di danno rilevante e il regime risarcitorio. Di fatti, la PLD si rivolge ai danneggiati che hanno acquistato un prodotto smart difettoso, mentre la AILD risarcisce i danni conseguiti ad un errata decisione del software. Ed ancora, mentre la PLD afferma che "la responsabilità senza colpa dell'operatore economico resta l'unico mezzo per risolvere adeguatamente il problema di una giusta ripartizione dei rischi inerenti nella moderna produzione tecnologica"[221], la AILD prevede la dimostrazione della colpa intesa quale "atto o un'omissione che non soddisfa l'obbligo di diligenza imposto, dal diritto dell'Unione o dal diritto nazionale, direttamente destinato a proteggere contro il danno che si è verificato"[222].

Pertanto, illustrato il meccanismo presuntivo ordito dalle due direttive, si devono tuttavia evidenziare alcune criticità. Tra queste figura la possibilità che i giudici, non avendo una conoscenza preliminare della rilevanza delle informazioni in possesso del convenuto, possano ordinare una divulgazione generica, rischiando di innescare contenziosi tecnici complessi e costosi per l'attore. Inoltre, esiste il rischio che il convenuto possa confondere la controparte fornendo una quantità eccessiva di informazioni irrilevanti. In secondo luogo, il meccanismo presuntivo previsto dalla AILD e dalla PLD, sebbene familiare agli ordinamenti giuridici, non comporta una vera inversione dell'onere della prova, ma lo alleggerisce solo in presenza di specifiche circostanze. Inoltre, in Italia, dove la giurisprudenza tende già ad agevolare l'onere probatorio dell'attore, l'introduzione di presunzioni legali potrebbe sembrare di scarsa rilevanza. Tuttavia, si auspica che la formula adottata dalla norma garantisca maggiore certezza del diritto, riducendo la discrezionalità dei giudici. Resta però incerta l'efficacia di disposizioni basate su concetti elastici come probabilità e ragionevolezza[223]. Infine, si rileva che le agevolazioni probatorie risultano efficaci soprattutto in occasione di malfunzionamenti evidenti del sistema di IA, spesso riscontrati nelle operazioni di classificazione svolte dall'algoritmo. Tuttavia, in presenza di attività complesse, come quelle di scoring, i richiedenti potrebbero trovarsi obbligati a sostenere costi significativi

[221] Cit. considerando 2 della Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi;
[222] Cit. considerando 22 della AI L Directive;
[223] M. Faccioli, *La responsabilità civile per danni cagionati da sistemi di intelligenza artificiale nel prisma dell'onere della prova*, Op, cit. p. 29;

per ingaggiare esperti di IA e professionisti di vario genere al fine di dimostrare l'errore o il bias del software. Di conseguenza, è essenziale che le proposte includano strategie concrete per facilitare l'accesso a finanziamenti destinati al contenzioso, al fine di supportare i richiedenti che non dispongono delle risorse necessarie per coprire autonomamente tali costi[224].

Dall'analisi svolta sulle direttive è possibile evincere che la *ratio* del fault-based liability system adottato dalla AILD risponda ai rilievi esposti durante le consultazioni con le parti interessate, per i quali "la responsabilità oggettiva è stata considerata sproporzionata dalla maggior parte delle imprese interessate". Ciononostante, ciò conferma che un regime di responsabilità oggettiva sarebbe svantaggioso per il mercato, poiché aumenterebbe le barriere all'ingresso per le piccole e medie imprese (PMI), a fronte di costi assicurativi così elevati da risultare proibitivi[225]. Allo stesso tempo, le associazioni per la difesa dei consumatori e le istituzioni accademiche sostenevano "con forza le misure relative all'onere della prova e all'armonizzazione della responsabilità civile (riferita a armonizzazione della responsabilità senza colpa (definita "responsabilità oggettiva") con l'obbligo di assicurazione"[226]. Pertanto, la soluzione normativa di compromesso è stata individuata in una direttiva che riducesse l'onere probatorio dei danneggiati, eliminando le asimmetrie informative tra le parti in sede di giudizio[227].

È bene osservare che, benché la Commissione abbia optato per un regime di responsabilità per colpa, la AILD «segue un approccio di armonizzazione minima. Tale approccio consente ai danneggiati […] dai sistemi di IA di invocare le norme nazionali più favorevoli. Pertanto, le legislazioni nazionali potrebbero, ad esempio, mantenere l'onere della prova predisposto dai regimi domestici basati sulla colpa o sulla

[224] P. Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*, Op. cit. p.
[225] Sul punto la AI L. Directive nei "risultati e valutazioni ex post, le consultazioni con imprenditori interessati e valutazione di impatto" riporta che «Furthermore, it would reduce legal uncertainty and prevent fragmentation, thus helping companies, and most of all SMEs, that want to realise the full potential of the EU single market by rolling out AI-enabled products and services cross-border. The preferred policy option also creates better conditions for insurers to offer coverage of AI-related activities, which is crucial for businesses, especially SMEs to manage their risks. It is namely estimated that the preferred policy option would generate an increased AI market value in the EU-27 between ca. EUR 500mln and ca. EUR 1.1bln in 2025.»;
[226] Cit. Policy option 3 riportata nei "risultati e valutazioni ex post, le consultazioni con imprenditori interessati e valutazione di impatto";
[227] *Vedi supra*;

responsabilità oggettiva»[228]. Il ruolo della AILD non consiste nell'armonizzare gli obblighi di diligenza o di responsabilità, né nel creare nuove forme di responsabilità extracontrattuale; piuttosto, il suo scopo è introdurre oneri probatori facilitati a favore delle vittime di sistemi di IA[229]. Infatti, la direttiva non ha imposto un regime di responsabilità oggettiva ma consente ai danneggiati di beneficiare della disclosure of evidence e della presunzione di colpevolezza qualunque sia il regime risarcitorio previsto dall'ordinamento interno. D'altro canto, la PLD non prevede una presunzione assoluta di colpevolezza, ma include esenzioni di responsabilità che permettono ai fornitori di sfruttare la propria conoscenza settoriale per confutare la presunzione di colpa, come nel caso del rischio da sviluppo.

Si può quindi osservare come le istituzioni europee non abbiano accolto del tutto le istanze contenute nella risoluzione del 20 ottobre 2020, le quali spingevano verso un regime di responsabilità oggettiva a carico degli operatori di front-end e back-end. Inoltre, la Commissione ha evitato una decisione definitiva sul regime risarcitorio da adottare, limitando il proprio intervento agli aspetti "procedurali", ovvero alla regolazione della ripartizione dell'onere probatorio, indipendentemente dal regime risarcitorio prescelto.

Il nesso di causa rimane un argomento di costante dibattito, con difficoltà di accertamento che superano l'ambito dell'intelligenza artificiale. Infatti, nella maggior parte dei casi, l'unica certezza sulla causa di un evento si ottiene seguendo il principio del "when we see it"[230]. Quindi, sebbene il principio generale sia quello della *condicio sine qua non,* si deve evidenziare la tendenza dei legislatori ad attenuare lo standard probatorio relativo all'elemento causale. Ciò avviene in presenza di prodotti, servizi o attività connotate da intrinseca pericolosità e dove un largo numero di persone sarebbe esposta a

[228] Cit. considerando 14 AI L. Directive;

[229] Sul punto la AI L. Directive nei "risultati e valutazioni ex post, le consultazioni con imprenditori interessati e valutazione di impatto" afferma che «At the same time, this proposal does not create or harmonise the duties of care or the liability of various entities whose activity is regulated under those legal acts and, therefore, does not create new liability claims or affect the exemptions from liability under those other legal acts. This proposal only introduces alleviations of the burden of proof for the victims of damage caused by AI systems in claims that can be based on national law or on these other EU laws. By complementing these other strands, this proposal protects the victim's right to compensation under private law, including compensation for fundamental rights breaches.»

[230] S. Wojtczak e P. Ksiezak, *Op. cit.* che riprende la celebre frase di M. Moore (nel suo libro 'Causation in the Law', Stanford Encyclopedia of Philosophy 2019, p 43), 'like hard-core pornography, causation is something we can "know when we see it" (Potter Stewart's language about pornography in Jacobellis v. Ohio);

tale pericolo. Da notare una profonda differenza tra l'armonizzazione massima operata tramite la PLD, che costituisce autonomo titolo risarcitorio in sede di giudizio, e il livello di armonizzazione minima proposta dalla AILD, che, invece, si appoggia al panorama normativo di ciascuno Stato membro, consentendo ad essi di mantenere regimi interni più favorevoli al danneggiato. La scelta della Commissione di intervenire soltanto per assicurare un'agevolazione sul piano probatorio è giustificata da diverse considerazioni, quali la difficoltà di intervenire in materia di responsabilità civile e tutela dei diritti, la volontà di colmare quel liability gap determinato dai sistemi di IA, la loro opacità e il numero di attori che intervengono nella catena produttiva e distributiva del sistema. Questi fattori hanno influenzato la struttura della direttiva, che è intervenuta nell'armonizzare solo l'aspetto che solleva maggiori preoccupazioni, ossia l'asimmetria informativa tra danneggiato e fornitore. Per quanto concerne invece altri profili di diritto come la legittimazione passiva e l'identificazione del danneggiante da convenire in giudizio, la direttiva amplia il novero di soggetti responsabili, contemplando oltre ai fornitori/produttori anche gli utenti. D'altro canto, un approccio che si limita a un'armonizzazione minima non assicura una protezione uniforme in tutto il mercato europeo, specialmente se gli Stati membri mantengono regimi speciali di responsabilità oggettiva. Questa scelta potrebbe minare la certezza giuridica per gli operatori economici. Inoltre, la mancata armonizzazione delle condizioni relative al danno tra i vari ordinamenti nazionali potrebbe generare discrepanze significative, influenzando la risarcibilità di danni, incluso quelli di natura psicologica, risultanti dall'utilizzo di sistemi di IA.

In un contesto normativo caratterizzato da un sistema di responsabilità civile multilivello, la parte danneggiata ha la possibilità di intraprendere diverse vie per ottenere il risarcimento. In particolare, il danneggiato può scegliere l'opzione più favorevole tra le varie normative applicabili, come quella prevista dalla direttiva PLD, che stabilisce una responsabilità oggettiva per difetto del prodotto, o le disposizioni del diritto nazionale, armonizzate dalla direttiva AILD, le quali possono contemplare la responsabilità per colpa o altri criteri di imputazione. Inoltre, il danneggiato ha la possibilità di invocare più discipline in subordine, in funzione della convenienza giuridica, sfruttando le peculiarità

delle diverse normative disponibili in base al corredo probatorio di cui dispone[231]. In sintesi, il pacchetto IA ha cercato di porre rimedio ai limiti della tecnologia, ancora non in grado di dare conto dei propri processi informatici, tramite l'obbligo di esibizione della documentazione relativa al programma del software e alle misure di riduzione del rischio adottate, così ricollegando l'evento illecito ad un errore di produzione o di manutenzione. Infatti, se i consulenti tecnici potessero comprendere le cause degli incidenti, sulla sola scorta delle prove assunte in ragione dell'accesso al software, non vi sarebbe la necessità di prevedere tali presidi. Invece, dal momento che i sistemi di IA non sono dotati di una scatola nera che riporti tutti i processi svolti dalla macchina, il giudice dovrà usare le presunzioni per stabilire l'esistenza del fatto.

5) Prospettive legali sulla responsabilità civile delle Intelligenze Artificiali tra vecchie e nuove soluzioni: la responsabilità per fatto altrui, artt. 2047, 2048 e 2049 c.c

Il pacchetto IA proposto dalla Commissione tenta di risolvere l'asimmetria informativa che connota il rapporto tra operatore di IA e vittime lese dal sistema. Come illustrato nei paragrafi precedenti la difficoltà di provare la logica e la causa del malfunzionamento costituisce, aprendo così una breccia nell'attuale sistema di responsabilità civile. Il gap di tutela emerge sin dal principio, ossia nel momento in cui occorre identificare il responsabile dei danni arrecati da un algoritmo. L'onere probatorio costituisce la maggiore preoccupazione delle istituzioni europee, e la principale difficoltà che i danneggiati incontrano nel sostenere la propria pretesa in giudizio. A tal fine la Commissione ha fornito agli attori anche una soluzione alternativa la possibilità di ordinare l'esibizione delle prove a richiesta del danneggiato che produca «prove sufficienti a sostenere la plausibilità della domanda di risarcimento del danno»[232].

Non vi sono ulteriori indicazioni che aiutino gli aventi diritto ad orientarsi nella scelta della controparte. Sul punto la AI L. Directive si riferisce genericamente a utenti e fornitori. Tuttavia l'AI Act, al quale fa spesso riferimento, menziona le ulteriore categorie

[231] E. Bellisario, *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*, Op. cit. p. 163;
[232] Art. 3 AI L. Directive;

degli importatori e distributori del sistema di IA. Sicché, l'ambito di applicazione soggettivo così strutturato intende includere tutti gli operatori coinvolti nella catena di produzione dell'IA, dovrebbe essere ritenuto responsabile per il danno prodotto dall'algoritmo. In secondo luogo, l'attore è responsabile anche di scegliere il titolo in forza del quale agire nei confronti del convenuto. È evidente come sia necessario interpretare e completare l'attuale quadro normativo per renderlo chiaro e definito, soprattutto in merito agli obblighi legali che impongono la costruzione di sistemi di IA sicuri ed accurati.

La capacità dell'IA di imparare e modificare i propri patterns elimina l'ordinario collegamento che normalmente sussiste tra il malfunzionamento del software e i suoi creatori. Peraltro, in assenza di un metodo scientifico in grado di comprendere cosa accade nella black box, il legislatore dovrà fare appello ad altri criteri per imputare la responsabilità su uno, o più, dei molteplici attori coinvolti nella catena del valore dell'IA. Sebbene non vi siano normative interne che si occupino specificatamente della responsabilità della macchina, la "United Nations Convention on the Use of Electronic Communications in International Contracts"[233] nel 2005 regola l'utilizzo dei messaggi automatici impiegati nelle trattative del contratto disponendo che:

"A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract."

Il contratto stipulato tramite messaggi automatici è ritenuto valido anche se perfezionato senza la supervisione dell'avente diritto, in presenza di una svolta tra "electronic agents". Inoltre, la citata Convenzione delle Nazioni Unite stabilisce che la responsabilità per i messaggi generati da un computer ricade sulla persona, fisica o giuridica, per conto della quale il sistema è stato programmato[234]. Questo principio riflette

[233] La Convenzione è disponibile al link: https://treaties.un.org/doc/source/RecentTexts/X-18_english.pdf ;

[234] Nazioni Unite, Commento all'art. 12 "Use of automated message systems for contract formation" della United Nations Convention on the Use of Electronic Communications in International Contracts, al paragrafo "Attribution of actions performed by automated message systems" afferma che «UNCITRAL also considered that, as a general principle, the person (whether a natural person or a legal entity) on whose

la regola generale secondo cui chi utilizza uno strumento è responsabile dei risultati prodotti, poiché lo strumento stesso non possiede volontà autonoma. Nel contesto dell'IA, la responsabilità oggettiva è spesso paragonata a quella derivante dal comportamento di animali, bambini o dipendenti, e si fonda sul concetto di responsabilità vicaria, o indiretta, come previsto dal principio del *Respondeat Superior*[235]. Ebbene le fattispecie di responsabilità extracontrattuale possono essere ricondotte esemplificativamente a tre categorie legali: illeciti dolosi, responsabilità per colpa o negligenza e responsabilità oggettiva. Il codice civile consente di interpretare le fattispecie con una certa flessibilità, circostanza che le distingue dalla responsabilità penale, dove invece vige il principio della tassatività del reato. Infatti, i tribunali civili possono accertare l'illiceità di una condotta sfruttando l'interpretazione analogica di norme che regolano casi simili, a condizione che la nuova fattispecie possa essere regolata con la medesima ratio della disposizione a cui si fa appello. Tuttavia, questo approccio non affida la politica risarcitoria alla totale discrezionalità delle corti, pertanto è necessario valutare come e se applicare le tradizionali categorie giuridiche alle nuove tecnologie e come queste possano affrontare le questioni fattuali poste dall'IA. In risposta a tali considerazioni, una parte della dottrina tradizionale in materia di responsabilità civile propone di assimilare i robot ad animali o entità pericolose, soggetti a regole di responsabilità oggettiva. Questo approccio consentirebbe di superare le difficoltà legate alla prova del nesso causale, spostando l'attenzione del giudice sull'accertamento della ragionevole prevedibilità del danno, sulla responsabilità vicaria e sul rispetto degli standard tecnici[236].

Pertanto, in base alle categorie tradizionali della responsabilità civile sopra riportate, urge chiedersi chi debba essere ritenuto responsabile per un danno provocato da un'IA e «whether such machines should be understood as: (i) legal persons; (ii) proper agents; or (iii) sources of responsibility for other agents in the system»[237]. Tra le ipotesi regolamentari proposte dalla dottrina figura la responsabilità vicaria per le azioni di un

behalf a computer was programmed should ultimately be responsible for any message generated by the machine»;

[235] Secondo C. Bieber, A Ramirez, *What Is Respondeat Superior?,*in Forbes Advisor « Respondeat superior is a Latin phrase that literally means "let the master answer." It is also a legal doctrine applicable in many civil claims throughout the United States. Under the legal doctrine, an employer can be held accountable for negligence or wrongdoing committed by their employee or agent. The employer is the "master" who must answer for the actions of those acting on their behalf.»;

[236] U. Pagallo, *The Laws of Robots Crimes, Contracts, and Torts,* Springer, 2013, p. 121;

[237] Cit. U. Pagallo, p. 37;

sistema di IA, come quella di un genitore per il figlio, di un'insegnante per il minore, di un tutore per l'incapace, o di un datore di lavoro per i propri dipendenti. In questo contesto, la responsabilità ricade su chi utilizza o supervisiona l'IA, come utenti o proprietari. Nonostante alcune differenze tra i sistemi giuridici, il principio di base rimane che la responsabilità è imposta non per l'atto illecito in sé, ma in forza del rapporto tra l'autore dell'illecito e colui che era tenuto ad evitare la condotta lesiva[238]. Appartengono a questa categoria la responsabilità per il danno cagionato dall'incapace ex art. 2047 c.c. e la responsabilità dei genitori e degli insegnanti ex art. 2048 c.c. Le due fattispecie presentano profili comuni, infatti sia il minore che l'incapace sono soggetti di diritto, ma non rispondono degli illeciti commessi, perché non ritenuti in grado di autodeterminarsi. Infatti, la capacità giuridica si acquista con la maggiore età e con essa la possibilità di stipulare contratti ed essere titolare di obbligazione, quindi anche le obbligazioni *ex delicto*. Invece l'interdetto e inabilitato non rispondono delle proprie azioni a causa di un'abituale infermità mentale, di alcolismo o dipendenti da sostanze stupefacenti o gioco d'azzardo, che non gli permettono di tutelare adeguatamente i loro interessi; in ogni caso non esiste un catalogo di circostanze che determinino l'incapacità, in quanto accertata caso per caso dal giudice. Pertanto, alla base di entrambe le esenzioni della responsabilità sussiste la mancanza di capacità di "intendere e volere" determinata da una scelta di politica legislativa o da un riscontro fattuale di infermità di mente. Alcuni studiosi ritengono che l'art. 2047 c.c. costituisca una fattispecie di responsabilità per fatto altrui, in quanto chi è tenuto al risarcimento non coincide con l'autore diretto del danno[239]. Tuttavia, sul punto la dottrina non è concorde, infatti una seconda ricostruzione ritiene il sorvegliante direttamente responsabile per non aver adeguatamente controllato il terzo ed impedito l'evento[240].

Applicando la prima interpretazione il danneggiato deve provare che il danno sia stato causato da un incapace mentre il sorvegliante, deve dimostrare l'inevitabilità del danno per ritenersi liberato dall'obbligo risarcitorio. La norma non prevede una presunzione di colpa, ma semplicemente ripartisce l'onere probatorio tra le parti, chiedendo al sorvegliante di dimostrare di non aver agevolato o lasciato persiste situazioni di pericolo.

[238] P. Cerka, J. Grigiene, G. Sirbikyt, *Liability for damages caused by artificial intelligence*, in Computer Law & Security Review, 2015, p. 385;
[239] Scognamiglio, Responsabilità civile per fatto altrui, in NN.D.I., XV, Torino, 1968, 693
[240] ALPA, La responsabilità civile, i n Tratt. Alpa, Milano, 1999, 665;

Infatti, spetta al danneggiato dimostrare che l'incapace abbia causato il danno, mentre il sorvegliante deve dimostrare di aver fatto quanto in suo potere per evitare l'evento lesivo, oppure la presenza di un impedimento oggettivo e l'impossibilità di reperire un aiuto o un sostituto per superare tale impedimento[241]. L'obbligo di sorveglianza, tuttavia, è una condizione di diritto di natura speciale, prevista specificatamente da disposizioni di legge o da particolari situazioni di fatto, purché percepibili all'esterno. L'obbligo può essere assunto anche volontariamente, ad esempio accogliendo un incapace nella propria sfera familiare, assumendosi così il compito di prevenire o impedire eventuali danni a terzi causati dal suo comportamento. Inoltre, non è necessario un legame parentale, ad esempio, al convivente *more uxorio* per l'illecito commesso dal figlio altrui. La responsabilità, inoltre, si applica a chiunque abbia la custodia dell'incapace, anche se solo temporaneamente[242].

Si riscontra una *ratio* simile nell'applicazione analogica dell'art. 2048 c.c. sulla responsabilità dei genitori e degli insegnanti per i danni commessi dai minori. Questo titolo configura una responsabilità solidale, affiancando alla responsabilità del minore, capace di intendere e volere, quella dei genitori o precettori. In caso di danno ingiusto causato dal minore, questi risponde direttamente secondo le norme generali della responsabilità civile, mentre la responsabilità dei genitori o degli altri soggetti indicati dall'art. 2048 si aggiunge a quella del minore. Questa struttura consente al danneggiato di richiedere il risarcimento sia al minore, autore dell'illecito, sia ai genitori. Pertanto, l'art. 2048 c.c. funge da garanzia per i terzi, estendendo la responsabilità inizialmente attribuita al minore anche ai genitori, tutori, precettori e maestri d'arte. I soggetti responsabili sono strettamente indicati nel testo dell'articolo, rispondono genitori legittimi e illegittimi a condizione che esercitino la responsabilità genitoriale *ex* art. 316 c.c. La responsabilità dei genitori per gli illeciti commessi dai figli minori è strettamente connessa alla coabitazione, che permette loro di adempiere ai doveri di vigilanza e educazione. La coabitazione, intesa come "consuetudine di vita comune"[243], costituisce un elemento fondamentale per l'attribuzione di tale responsabilità. Anche un'assenza prolungata del minore, come un periodo di studio all'estero, non interrompe il vincolo della coabitazione

[241] Monateri, La responsabilità civile, in Tratt. Sacco, Torino, 1998, p. 939;
[242] Vedi Art. 2047 c.c. - Danno cagionato dall'incapace, in Codice Civile commentato a cura di G. Bonilini, M. Confortini, C. Granelli;
[243] Monateri, La responsabilità civile, in Tratt. Sacco, Torino, 1998, p. 17;

ai fini della responsabilità, poiché non annulla gli effetti dell'educazione impartita. La responsabilità genitoriale rimane, inoltre, quando l'allontanamento del minore è dovuto a motivi di lavoro o svago del genitore[244], o se i genitori hanno contribuito, in qualche misura, a provocare l'allontanamento. Tuttavia, la responsabilità non sussiste in assenza del presupposto della coabitazione, come nel caso in cui il minore abbia stabilmente lasciato la casa familiare per ragioni non imputabili al genitore. Nonostante ciò, l'allontanamento del minore dalla casa dei genitori non esonera automaticamente questi ultimi da responsabilità, qualora l'illecito del figlio sia riconducibile a carenze educative oggettive «che si manifestino nel mancato rispetto delle regole della civile coesistenza, vigenti nei diversi ambiti del contesto sociale in cui il soggetto si trovi ad operare»[245].

La genericità e ampiezza dell'elemento delle "carenze educative oggettive" apre la fattispecie ad una gamma di "errori" del genitore più ampia rispetto a quanto previsto dall'art. 2047 c.c. A differenza della "coabitazione", presupposto di fatto semplice da accertare, la prova dell'inottemperanza dei doveri inderogabili di educazione e vigilanza codificati all'art. 147 c.c. Infatti, la prova liberatoria che i genitori devono fornire a loro difesa non si limita alla semplice dimostrazione di non aver potuto impedire l'illecito, ma implica una valutazione complessiva del sistema educativo impartito. La genericità della formula, unitamente alla grande varietà di casi che possono prospettarsi nella realtà, ha condotto gli interpreti a rilevare l'inadeguatezza dell'educazione e della vigilanza in base alla gravità dell'evento ed alle sue circostanze, rendendo estremamente rigorosa la prova liberatoria. Pertanto, qualora il giudice si trovi a esaminare la condotta di un ragazzo che abbia causato un evento lesivo di particolare gravità e riprovevolezza per le modalità con cui è stato commesso, potrà dedurre dal fatto stesso la carenza di adeguate direttive impartite dai genitori, che hanno compromesso lo sviluppo di empatia, coscienza e senso di responsabilità sociale nel minore.

Questo orientamento giurisprudenziale ha delineato una duplice natura della responsabilità prevista dall'art. 2048 c.c. Nei casi di particolare gravità, la responsabilità assume un carattere oggettivo, poiché l'inadeguatezza dell'educazione viene presunta dalle circostanze stesse del fatto. In tali situazioni, i genitori sono chiamati a rispondere

[244] Franzoni, *Dei fatti illeciti*, in Comm. Scialoja, Branca, sub art. 2048, Bologna-Roma, 1993, p. 364;
[245] Cit. massima della Cass. Civ. Sez. III, sentenza n. 7050 del 14 marzo 2008;

esclusivamente in virtù del loro ruolo, anche se non hanno direttamente causato il danno[246]. Al contrario, nei casi di minore gravità, i genitori possono essere esonerati dalla responsabilità presentando una prova generica che dimostri l'adeguatezza dell'educazione impartita al minore e la corretta vigilanza esercitata sui suoi comportamenti[247]. Il concetto di *culpa in educando* e *in vigilando* viene quindi modulato in base alle circostanze in cui si è verificato l'illecito: una responsabilità oggettiva per illeciti particolarmente riprovevoli, mente in tutti gli altri casi si configura una responsabilità per colpa. Infine, i precettori sono responsabili per gli atti commessi dagli allievi durante il periodo in cui questi si trovano sotto la loro vigilanza, che include le ore di lezione, la ricreazione, le gite scolastiche e a tutto il tempo trascorso nei locali della scuola. Pertanto, l'attore dovrà dimostrare solo che l'evento dannoso si sia verificato mentre l'alunno si trovava sotto la custodia dell'insegnante al momento del fatto. I precettori rispondono in solido con i genitori dell'alunno, il cui comportamento dannoso potrebbe essere sintomo di un'inadeguata educazione impartita nell'ambiente domestico[248].

Le disposizioni esaminate potrebbero trovare applicazione anche al danno arrecato da un sistema di IA. La letteratura ha infatti ipotizzato una analogia tra il minore e il software, dove quest'ultimo, proprio come un bambino, nasce, cresce, si sviluppa, e soprattutto trasgredisce, se non ben educato. Pertanto, si suggerisce di riconoscere progressivamente una capacità giuridica alle IA, in base al loro livello di apprendimento. In breve, si suggerisce di attendere il raggiungimento della maggiore età del sistema, per concedergli pari diritti e doveri attribuiti agli esseri umani. Questo approccio permetterebbe di assegnare responsabilità educative ai produttori e sviluppatori di IA, con responsabilità vicarie per i "genitori" (i creatori dell'IA) e, successivamente, responsabilità direttamente a carico dell''IA "matura".

Quindi, come per gli esseri umani, un'IA potrebbe essere considerata autonomamente responsabile delle proprie azioni, una volta raggiunto un certo livello di autonomia, indipendentemente dall'educazione ricevuta. Tuttavia, per rendere questa teoria effettivamente praticabile dovrebbero essere elaborati criteri legali per valutare

[246] R. Pardolesi, *Danni cagionati dai minori: pagano sempre i genitori?*, in Fam. e dir., 1997, p. 227;
[247] F. Di Ciommo, Minore maleducato e responsabilità dei genitori, in Danno e Resp, 1998, p. 1090;
[248] Art. 2048 c.c. - Responsabilità dei genitori, dei tutori, dei precettori e dei maestri d'arte, in Codice Civile commentato a cura di G. Bonilini, M. Confortini, C. Granelli;

l'educazione e il livello di apprendimento del software. Solo in questo modo potrebbe essere accertata la capacità dell'IA di autodeterminarsi nel mondo circostante e valutare le conseguenze delle proprie azioni, condizioni necessarie per imputare correttamente la capacità giuridica[249]. Continuando a percorrere le fila di questa teoria "provocatoria", si dovrebbe optare per un approccio educativo condiviso a livello internazionale, facendo appello, ad esempio, a quei principi etici di benessere, inoffensività, giustizia, autonomia e trasparenza (evidenziati nel primo capitolo di questa tesi) riscontrati nella maggior parte di dichiarazioni e codici di condotta per un'IA sostenibile e sicura. Un programma formativo differenziato tra le varie giurisdizioni comporterebbe lo sviluppo di sistemi di IA diversi perché portatori di scale di valori differenti. Tuttavia, dal momento che i sistemi di IA sembrano già in grado di comunicare tra loro, non è difficile immaginare che presto o tardi i software si contamineranno, comunicando tra loro e condividendo principi etici, direttive, processi loro impartiti[250]. Pertanto, una politica "educativa" frammentaria a livello internazionale non riuscirebbe in ogni caso a valutare la condotta dei sistemi che potrebbero nel tempo condividere principi diversi da quelli inizialmente impartiti.

Infine, sulla base di assunti molto simili ai precedenti, alcuni autori hanno proposto di estendere analogicamente l'applicazione dell'art. 2049 c.c., attribuendo la responsabilità all'imprenditore per i danni causati da un sistema intelligente nello svolgimento di compiti connessi alla propria attività professionale[251]. Questa fattispecie è caratterizzata dalla presenza di un rapporto di subordinazione tra il sistema intelligente e l'imprenditore, l'esercizio di un potere di "direzione e sorveglianza" da parte del committente nei confronti del preposto, nonché l'esistenza di un nesso causale tra l'esecuzione delle mansioni affidate al sistema e il danno arrecato a terzi. Qualora sussistano tutte queste circostanze non è necessario, perché si configuri la fattispecie, anche il contratto di lavoro subordinato ma è sufficiente l'esistenza di un rapporto fattuale

[249] L. Arnaudo, R. Pardolesi, *Ecce robot. Sulla responsabilità dei sistemi adulti di intelligenza artificiale*, in Responsabilità, p. 415;
[250] Focus, *Innovazione La lingua segreta dei bot di Facebook*, l'articolo riporta la notizia di due chatbot di Facebook che hanno iniziato a dialogare tra loro in una lingua sconosciuta e sono stati subito spenti dai loro programmatori. La scelta è stata motivata non dal pericolo che i software si unissero contro il genere umano ma perché avevano escluso i programmatori dalla loro conversazione, pertanto non avrebbero potuto ultimare il training; (articolo disponibile al link: https://www.focus.it/tecnologia/innovazione/la-lingua-segreta-dei-bot-di-facebook-intelligenza-artificiale-robot);
[251] M. Costanza, "Robot e impresa", in U. Ruffolo (a cura di), "Intelligenza artificiale e responsabilità", Milano, 2017, p. 112 s;

di direzione e controllo, anche soltanto in forma occasionale e temporanea, tra datore di lavoro nei confronti del soggetto che ha arrecato il danno. Pertanto, l'art. 2049 c.c. configura una responsabilità indiretta dell'imprenditore, infatti la fattispecie, le cui radici risalgono al Codice Napoleonico, implica una *culpa in eligendo* e una *culpa in vigilando* del committente nella gestione dei propri dipendenti. Tuttavia, questi riferimenti storici sono spesso considerati più formali che sostanziali nelle decisioni giuridiche. Inoltre, la disposizione prevede una responsabilità oggettiva a carico del datore di lavoro, senza che quest'ultimo possa dimostrare l'assenza di colpa nella scelta o nel controllo del dipendente. Il committente è responsabile del preposto, anche se la scelta è stata imposta da leggi o regolamenti[252].

Questa tesi ha trovato riscontro anche nella letteratura internazionale, che ha elaborato una serie di criteri per accertare in quali casi la macchina agisca in nome e per conto dell'utilizzatore:

1) a human principal (or an organization) delegates a task to an algorithm;
2) the delegation requires the agent's freedom of decision;
3) the agent's action is neither foreseeable nor explainable by a programmer;
4) the action violates a contractual/tortious duty of care;
5) causation between action and damage can be established."[253]

Ebbene, l'applicazione della responsabilità per danno del commesso al terzo consentirebbe di beneficiare della responsabilità oggettiva a carico dei genitori o dell'imprenditore, per i danni dei figli o dei preposti; diversamente il sorvegliante potrebbe evitare la condanna dimostrando l'inevitabilità del danno. Inoltre, l'art. 2048 c.c. includerebbe altri soggetti coinvolti nell'"educazione" dell'automa, come sviluppatori, programmatori e utilizzatori. Per di più la prova liberatoria configurata dal "non aver potuto evitare il fatto", di cui agli art. 2048 e 2047 c.c., imporrebbe ai soggetti

[252] Art. 2049 c.c. - Responsabilità dei padroni e dei committenti, in Codice Civile commentato a cura di G. Bonilini, M. Confortini, C. Granelli;
[253] Cit. A. Beckers, G. Teubner, *Three Liability Regimes for Artificial Intelligence Algorithmic Actants, Hybrids, Crowds,* Bloomsbury Publishing, p. 139; gli autori ultimano l'elenco riportando le conseguenze legali della vicarious liability «(6) As a consequence, the algorithm' s user as the principal is the liable person. (7) Compensation of damage is not limited to the narrow compensation principles of strict liability for industrial hazards but follows established principles of contract and tort law, particularly regarding the question of whether or not merely monetary damages will be compensated»;

coinvolti nello sviluppo dell'IA l'obbligo di dimostrare di aver predisposto le misure preventive e successive necessarie per evitare lo specifico evento dannoso.

L'applicazione analogica di queste disposizioni ai sistemi di IA è stata tuttavia criticata da chi sostiene che gli art. 2048 e 2047 c.c. siano disposizioni speciali poiché previste per particolari tipi di individui; quindi, non potrebbero essere applicate per tutti i sistemi di IA. Queste disposizioni sono talmente peculiari, con criteri di attribuzione della responsabilità così specifici, da impedire una semplice estensione analogica delle stesse alle responsabilità, sarebbe invece necessari. Invece, la suggerita applicazione analogica dell'art. 2049 c.c risulta inconciliabile con il nostro ordinamento, in quanto estenderebbe la fattispecie ad una nuova e molto estesa gamma di illeciti. La *ratio* della norma risiederebbe invece nel principio di responsabilizzazione del committente per gli errori derivanti dall'intelligenza (umana) del dipendente; infatti, quest'ultimo risponderebbe a titolo di colpa o dolo dell'illecito commesso. Quindi, estenderla ai software di IA impiegati in un'attività di impresa estenderebbe la responsabilità oggettiva dell'imprenditore ad una serie molto più ampia di illeciti[254].

Infine, la letteratura sottolinea anche che le disposizioni in commento presuppongono il libero arbitrio dell'individuo che commette il danno, elemento non riscontrabile invece per l'IA[255]. Alla luce di tali critiche l'applicazione della responsabilità per fatto altrui è stata allontanata dalla letteratura e dai legislatori consapevoli che, mancando i sistemi di IA di personalità giuridica, la disciplina della responsabilità aquiliana *ex* art. 2043 cod. civ., risulta di difficile applicazione.

6) Le fattispecie di responsabilità oggettiva: l'artt. 2050, 2051 e 2052 c.c.

Il capitolo prosegue vagliando le seguenti disposizioni nazionali che potrebbero fungere da fondamento giuridico in forza del quale agire per i danni causati da un sistema di IA, lette in combinato disposto con la AILD e i suoi meccanismi di tutela (ossia la

[254] U. Ruffolo, *Intelligenza Artificiale e diritto - Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in Giur. It., 2019, p. 1689

[255] F. Caroccia, *Ancora su responsabilità civile e uso delle intelligenze artificiali*, in Contratto e impresa, 2022, p. 418;

disclosure of evidence e le presunzioni del malfunzionamento e della colpa). Una delle fattispecie più additate dalla dottrina è la responsabilità per attività pericolosa di cui all'art. 2050 c.c., che disciplina la responsabilità per l'esercizio di attività pericolose, ai danni prodotti da IA; questa ricostruzione si fonda sul presupposto che l'utilizzo e lo sviluppo dei sistemi intelligenti possa configurarsi come un'attività intrinsecamente rischiosa. Si ritiene, infatti, che l'interazione tra un automa dotato di capacità adattative e di apprendimento e un essere umano possa comportare un rischio significativo per i diritti di terzi, con il rischio che tali sistemi agiscano in modo dannoso[256]. La norma in esame si applica a quelle attività che, pur essendo considerate lecite in virtù della loro utilità sociale, comportano un rischio elevato di arrecare danni. Il legislatore, nel consentire tali attività, ha previsto un regime di responsabilità particolarmente rigoroso per chi le esercita, per agevolare le istanze di risarcimento dei soggetti danneggiati e imputare le conseguenze negative dell'attività su coloro che ne beneficiano economicamente. Se in un primo momento la dottrina interpretava questa norma configurandola quale responsabilità per colpa lieve, a partire dagli anni Sessanta si è affermata una visione che riconosce la natura oggettiva della responsabilità in questione[257].

Tale responsabilità non si fonda sulla colpa dell'esercente, ma sulla mancata adozione di tutte le misure necessarie per prevenire il danno, indipendentemente dalle condizioni psico-fisiche del soggetto. Pertanto, anche minori o incapaci possono essere chiamati a rispondere. Le attività pericolose non si limitano esclusivamente a quelle svolte per profitto o vantaggio personale, ma includono anche quelle che, per loro stessa natura o per i mezzi utilizzati, comportano un alto rischio di causare danni. È compito del giudice determinare la pericolosità di tali attività, valutando tutti i fatti e le circostanze del caso. Esistono attività pericolose tipiche, già normate, e atipiche, la cui pericolosità viene accertata caso per caso. La pericolosità può derivare da una condotta imprudente o dalla natura intrinsecamente rischiosa dell'attività. Per determinare se un'attività è intrinsecamente pericolosa, si può fare riferimento alla frequenza e alla gravità dei danni da essa causati. Sul punto si distinguono due diversi correnti, la prima sostiene la tipicità delle attività ritenute pericolose, mentre la seconda si apre alla prospettiva che anche

[256] G. D'Alfonso, *The Regime of Liability from Things in Custody between Traditional Issues and 'Algorithm Liability*, in European Journal of Privacy Law & Technologies, 2022, p. 104;
[257] P. Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961, p. 48;

attività atipiche possano comportare l'applicazione dell'art. 2050 c.c. La valutazione della pericolosità deve essere svolta *ex ante,* ossia prima del verificarsi del danno; infatti, solo il pericolo prevedibile può essere effettivamente evitato dal responsabile adottando le misure preventive adeguate. Il giudice deve anche accertare che il danno sia derivato dall'esercizio di quella attività pericolosa, senza dover dimostrare un collegamento diretto tra un'azione specifica dell'agente e l'evento dannoso. Spetta al danneggiato provare la relazione causale tra il danno e l'attività pericolosa.

Anche in questa fattispecie è contemplata una prova liberatoria, l'esercente può esimersi dalla responsabilità solo dimostrando di aver preso tutte le misure necessarie per evitare il danno. Tuttavia, ad avviso della giurisprudenza, non basta dimostrare di aver rispettato le norme vigenti, è necessario provare di aver fatto tutto il possibile per prevenire l'evento dannoso. Tuttavia, questa interpretazione potrebbe condurre al paradossale risultato per cui, pur avendo adottato tutte le misure necessarie, un soggetto non risulti comunque aver dimostrato di aver fatto tutto il possibile. Pertanto, al fine di evitare che la prova liberatoria diventi in questi termini irrealizzabile, questi concetti non dovrebbero essere interpretati in modo letterale, in quanto sarebbe diabolica la prova di aver messo in atto tutte le misure possibili che avrebbero potuto in astratto evitare il danno (in quanto la valutazione doveva essere ex ante). Di conseguenza, la responsabilità sarebbe attribuita – quasi oggettivamente - all'esercente, non perché non abbia preso tutte le precauzioni possibili, ma perché l'attività in questione è considerata intrinsecamente pericolosa[258]. La prova liberatoria si ridurrebbe così alla dimostrazione del caso fortuito o della forza maggiore, non imputabile all'esercente, che ha interrotto il nesso causale tra l'attività pericolosa e il danno[259]. Di conseguenza l'interpretazione data dalle corti all'art. 2050 c.c. costituisce una responsabilità oggettiva, secondo il quale il semplice verificarsi del danno può essere considerato come prova dell'insufficienza delle misure adottate[260].

Ebbene, alla luce degli elementi e dell'interpretazione giudiziale dell'art. 2050 c.c. numerosi autori hanno associato l'elevato rischio associato allo sviluppo delle macchine auto-apprendenti ad un'attività intrinsecamente pericolosa. Questo approccio presenta il

[258] M. Franzoni, *Dei fatti illeciti*, in Comm. Scialoja, Branca, sub artt. 2043-2059, Bologna-Roma, 1993, 521;
[259] P. G. Monateri, *La responsabilità civile*, in Tratt. Sacco, Torino, 1998, p. 1036;
[260] *Art. 2050 c.c. - Responsabilità per l'esercizio di attività pericolose*, in Codice Civile commentato a cura di G. Bonilini, M. Confortini, C. Granelli;

vantaggio di attribuire la responsabilità per l'adozione delle misure necessarie a prevenire i danni e i costi derivanti da eventuali eventi dannosi, a chi esercita il controllo.

Questa soluzione normativa permetterebbe di estendere la copertura anche a quei danni non inclusi nella responsabilità da prodotto e che risulterebbero esclusi, ad esempio, dall'eccezione del rischio di sviluppo. Tale eccezione, infatti, non è applicabile in questa specifica fattispecie.[261] Tale differenza potrebbe risiedere nella *ratio* delle due disposizioni. L'art. 2050 c.c. alloca i rischi di un'attività che il legislatore, o l'interprete, ritenga intrinsecamente pericolosa ma che, per i particolari benefici che essa apporta alla società, viene accettata nell'ordinamento. Il rischio viene per l'appunto allocato su colui che ne trae profitto e che, presumibilmente, costituisce il deep pocket tra tutti coloro che sono coinvolti nell'esercizio dell'attività; tra i quali potrebbe figurare anche lo Stato, come nel caso della fabbricazione, importazione e distribuzione di farmaci e terapie mediche in generale, che contribuiscono alla tutela della salute pubblica ed individuale[262].

Al contrario la direttiva sulla responsabilità da prodotto difettoso non presuppone la pericolosità del prodotto e, sulla base di questa considerazione, vuole limitare la responsabilità del produttore al caso eccezionale in cui questo immetta nel mercato un prodotto difettoso in un momento in cui le conoscenze scientifiche e tecniche disponibili non consentivano di considerarlo tale.

La ratio di questa eccezione risiede nelle gravi conseguenze economiche che potrebbero derivare dall'applicazione di una responsabilità oggettiva a carico di imprenditori e artigiani. Infatti, autorevole dottrina evidenzia che una responsabilità oggettiva comporterebbe principalmente l'aumento dei premi assicurativi per i produttori, senza incentivarli ad investire nella ricerca per trovare misure di sicurezza più avanzate. Quindi un regime di responsabilità oggettiva che non contempli i rischi da sviluppo potrebbe avere il collaterale effetto di rallentare l'innovazione all'interno delle imprese, disincentivando gli investimenti nello sviluppo di prodotti più sicuri e, di fatto, avvantaggiando quelle aziende che non investono in innovazione scientifica. Questo tema è oggetto di dibattito, poiché si sostiene che un regime di responsabilità basato sulla colpa

[261] F. Caroccia, *Ancora su responsabilita` civile e uso delle intelligenze artificiali*, Op. cit. p. 418;
[262] *Art. 2050 c.c. - Responsabilità per l'esercizio di attività pericolose*, Op. cit. il commento riporta la casistica relativa alla disposizione;

possa, al contrario, promuovere maggiormente la sperimentazione di nuovi prodotti, suggerendo che sia proprio la colpa a rappresentare lo strumento più efficace per incentivare l'innovazione[263].

In virtù del confronto tra le caratteristiche e gli obiettivi dell'art. 2050 c.c. e della dir. 85/374/CE, si evince come la prima costituisca uno strumento ulteriore per il danneggiato per ottenere il risarcimento, rappresentando un'alternativa alla responsabilità per prodotto difettoso. Pertanto, in caso di comportamento anomalo di uno smart product, oltre alla disciplina specifica del danno da prodotto, può trovare applicazione anche le norme generali di responsabilità civile, come l'art. 2050 del codice civile italiano. La scelta del primo o del secondo titolo quale fondamento dell'azione risarcitoria determina importanti ricadute pratiche, come l'ampiezza dei termini di prescrizione: qualora sia scaduto il termine triennale previsto per il danno da prodotto, il danneggiato potrebbe comunque ricorrere alla responsabilità extracontrattuale, che prevede un termine di prescrizione più lungo. La giurisprudenza italiana riconosce la concorrenza tra l'applicazione dell'art. 2050 c.c. e le norme sul danno da prodotto, qualora la stessa produzione e/o distribuzione del prodotto costituisca attività pericolosa. Le due norme, entrambe oggettive perché escludono l'elemento della colpa, si fondano su presupposti distinti; la direttiva richiede la difettosità del prodotto, mentre la seconda si concentra sulla sua pericolosità intrinseca. L'art. 2050 c.c. presenta un campo di applicazione più ampio rispetto alla normativa sulla responsabilità per danno da prodotto, in quanto si applica non solo ai prodotti difettosi, ma anche a quelli che, pur conformi agli standard di produzione, risultano intrinsecamente pericolosi. Un caso di scuola è rappresentato dalle sigarette, che arrecano danni alla salute, anche in assenza di difetti. Inoltre, i criteri per escludere la responsabilità differiscono: nel caso della responsabilità per danno da prodotto, il produttore deve dimostrare che il difetto non gli è imputabile, mentre ai sensi dell'art. 2050 c.c., è necessario provare di aver adottato tutte le misure idonee per prevenire il danno[264].

---

[263] C. Fabrizio, *Responsabilità da prodotto difettoso: appunti di analisi economica del diritto*, in *Foro It.*, 1989, fasc. 3, colonna 119, l'autore sul punto ci riporta l'interessante ipotesi secondo la quale «A proposito di state of art defense, meriterebbe più che una segnalazione una recente proposta di considerare responsabile l'impresa che non attui un efficiente programma di ricerca (da valutarsi, in termini di costi e benefici, da parte dei giudici, o più plausibilmente da parte di appositi organismi amministrativi)»;
[264] U. Ruffolo, *Intelligenza Artificiale e diritto - Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, Op. cit. p. 1694;

Pertanto, è necessario comprendere se l'IA possa costituire attività pericolosa. Il concetto di maggiore fonte di pericolo si articola su due teorie principali: la prima ha ad oggetto oggetti fisici che non possono essere completamente controllati, mentre la seconda riguarda attività che comportano rischi significativi per i terzi. L'intelligenza artificiale, in quanto entità dotata di capacità decisionali autonome, soddisfa i criteri per essere considerata una maggiore fonte di pericolo, a causa dell'autonomia, dell'opacità e dell'incontrollabilità dell'automa descritte nel primo capitolo di questa tesi. Di conseguenza, sviluppatori e fornitori dovrebbero essere ritenuti responsabili dei rischi associati all'uso dell'IA, anche in assenza di colpa. L'art. 2050 si fonda sulla teoria del rischio, la quale sostiene che, quando un individuo non ha completo controllo di un'attività pericolosa, il semplice rispetto delle norme di sicurezza non è sufficiente, e le esternalità negative da essa prodotte dovranno essere assorbite da colui che ne trae profitto[265].

L'estensione analogica della responsabilità presunta ai sensi dell'art. 2050 del codice civile richiede un'attenta valutazione delle conseguenze normative che ne deriverebbero, specialmente in ambiti dove l'IA è ampiamente utilizzata nei processi produttivi. Se i prodotti e servizi che sfruttano l'IA dovessero essere considerati attività pericolose, in virtù delle nuove dinamiche introdotte dall'uso della tecnologia, questo potrebbe trasformare settori precedentemente ritenuti sicuri in ambiti soggetti al regime rigido di responsabilità presunta dell'art. 2050 c.c.. Ad esempio, settori come quello automobilistico, con l'introduzione di veicoli autonomi, o quello medico, con l'uso di dispositivi diagnostici basati sull'IA, potrebbero essere classificati come attività pericolose a causa dei rischi intrinseci legati al malfunzionamento o agli errori dell'IA. Produttori e operatori in questi settori sarebbero automaticamente ritenuti responsabili dei danni arrecati dal software di IA impiegato nella catena di produzione e distribuzione, salvo che dimostrino di aver adottato tutte le misure idonee a prevenirli. Questo paradigma legislativo potrebbe avere un impatto significativo sull'innovazione, sugli investimenti e sui costi di gestione del rischio in tali settori[266]. Ciò comporterebbe per le imprese un significativo aumento dei costi, sia in termini di risarcimenti, sia per

[265] P. Cerka, J. Grigiene, G. Sirbikyt, *Liability for damages caused by artificial intelligence*, in Computer Law & Security Review, 2015, p. 385
[266] U. Ruffolo, *Intelligenza Artificiale e diritto - Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, Op. cit. p. 1697;

l'implementazione di misure preventive adeguate a mitigare i rischi associati all'utilizzo di tecnologie intelligenti. Peraltro, seguendo l'impostazione il rischio da sviluppo, ossia il difetto non rilevabile al momento della messa in commercio del prodotto, dovrebbe essere indice di una maggiore pericolosità dell'IA e non scagionare il produttore. Tuttavia, come precedentemente osservato, il criterio è stato confermato quale eccezione dalla proposta PLD.

Una quinta ricostruzione giuridica, suggerita dalla letteratura, si concentra invece sull'utilizzo del sistema, ed in particolare, sul soggetto che ne detiene il controllo. La letteratura ha infatti fatto appello anche alla fattispecie di cui all'art. 2051 c.c., la quale stabilisce che ciascuno è responsabile per il danno cagionato dalle cose che ha in custodia, salvo che provi la sopravvenienza del caso fortuito. Per attribuire la responsabilità al custode, è sufficiente che il danneggiato dimostri l'esistenza del danno e il nesso causale con il bene custodito, inoltre non è necessaria la pericolosità intrinseca. Una teoria storica collega il concetto di custode all'uso, al godimento e allo sfruttamento economico del bene, attribuendo la responsabilità a chi ne trae profitto[267]. Un'altra interpretazione, invece, qualifica il custode come colui che ha il dovere di controllare il rischio derivante dal bene, identificandolo come il soggetto che ha un rapporto stabile e continuativo con il bene, rendendo prevedibili i rischi che esso potrebbe comportare per i terzi[268]. Pertanto, presupposto della responsabilità non è la titolarità di un diritto di proprietà, ma l'effettivo controllo sul bene, perciò sia il detentore che il possessore possono essere responsabili. Inoltre, perché si configuri la responsabilità da cosa in custodia il danno deve derivare direttamente dal bene e non dall'azione del custode. La nozione di custodia implica un controllo fisico sulla cosa, incombe sul custode l'obbligo di vigilanza e gestione per prevenire eventuali danni. Infine, come esplicita la lettera della norma, soltanto il caso fortuito può esimere il custode dalla responsabilità.

Il caso fortuito prescinde da qualsiasi elemento inerisca la colpa, sebbene l'orientamento tradizionale la qualificasse come responsabilità da colpa presunta per non aver predisposto le misure di sicurezza necessarie per impedire l'evento lesivo. Tuttavia, questa interpretazione non trova riscontro nella lettera della norma, difatti l'art. 2051 c.c.

[267] E. Valsecchi, *Responsabilità aquiliana oggettiva e caso fortuito*, in Riv. dir. comm., 1947, p. 167;
[268] Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961, p. 244;

non ha alcun riferimento alla condotta del custode. Ne consegue che la norma prevede una fattispecie di responsabilità oggettiva, basata sulla relazione tra il custode e il bene[269].

La *ratio* sottesa a questa seconda forma di responsabilità oggettiva intende responsabilizzare colui che ha la concreta possibilità di conoscere e gestire i rischi della cosa. Pertanto, l'art. 2051 c.c. potrebbe trovare applicazione anche per i danni attribuibili unicamente ad un dispositivo intelligente. Pertanto, il presupposto che consente di agire *ex* art. 2051 c.c. è il "potere di controllo" sul sistema di IA, l'ordinamento in questo modo sceglierebbe ancora una volta di attribuire le responsabilità di uno strumento a chi ha il potere concreto di gestirne i rischi. Pertanto, in un sistema chiuso in cui il produttore conserva il controllo sia sull'hardware che sul software, l'art. 2051 c.c. non trova applicazione, trasferendo la responsabilità direttamente al produttore. In un sistema aperto, invece, dove il titolare ha un certo grado di controllo e può influenzare le condizioni di rischio, l'art. 2051 c.c. torna ad essere applicabile. L'applicazione analogica coinvolgerebbe anche chi addestra i sistemi di IA introducendo dati e feedback che ne influenzano il comportamento; quindi, questa interpretazione implicherebbe nel giudizio l'addestratore, il produttore del dispositivo e il creatore dell'algoritmo. Il fondamento della responsabilità da custodia di IA si riscontra nel ruolo dell'addestratore nello sviluppo comportamentale del software, che se non gestito con gli adeguati meccanismi di controllo potrebbe degenerare nei bias e discriminazioni di fatto descritte nei capitoli precedenti. Di conseguenza, l'addestratore potrebbe essere ritenuto responsabile per i danni causati dall'IA, qualora derivino da un cambiamento inatteso nel comportamento dell'IA stessa[270].

Infine, si analizza la fattispecie parallela della responsabilità dei padroni per danni cagionati dai propri animali, di cui all'art. 2052 c.c. che, come il precedente art. 2051 c.c., stabilisce una forma di responsabilità oggettiva. Il testo riconosce la responsabilità del «proprietario di un animale, o di chi se ne serve per il tempo in cui lo ha in uso, per danni cagionati dall'animale, sia che fosse sotto la sua custodia, sia che fosse smarrito o fuggito, salvo che provi il caso fortuito». Le similitudini tra le due fattispecie comprendono anche

[269] *Art. 2051 c.c. - Danno cagionato da cosa in custodia*, in Codice Civile commentato a cura di G. Bonilini, M. Confortini, C. Granelli;
[270] G. D'Alfonso, The Regime of Liability from Things in Custody between Traditional Issues and 'Algorithm Liability', in European Journal of Privacy Law & Technologies (EJPLT), 2022, p. 106;

il presupposto della custodia quale elemento essenziale della responsabilità. Il testo infatti sottolinea che ne è responsabile il titolare o un terzo che lo abbia in custodia per trarne vantaggio. La custodia non si limita al controllo fisico, ma implica anche la capacità di gestire e governare l'animale. Inoltre, per il trasferimento della responsabilità il codice richiede che l'animale venga utilizzato per un interesse autonomo del terzo. La prova liberatoria legata al sopravvenire di un caso fortuito non è soddisfatta, ad esempio, dalla fuga dell'animale; in quanto questa circostanza è inclusa tra i rischi prevedibili nella custodia dell'animale. Pertanto, il caso fortuito può consistere soltanto nell'evento eccezionale e imprevedibile che supera qualsiasi resistenza dell'uomo[271].

Peraltro, anche in questo caso la responsabilità si configura senza distinzioni tra le varie specie e categorie di animali; ad esempio, non modifica l'onere probatorio la pericolosità dell'animale anche se legata alla razza, al tipo di addestramento o all'ambiente di vita (applicando soltanto per gli animali selvaggi una responsabilità dello Stato [272]). Invece, nel diritto americano e inglese, la responsabilità dei proprietari varia in base alla natura dell'animale, così i proprietari di animali selvatici, intrinsecamente pericolosi, si presumono responsabili; mentre i proprietari di animali domestici rispondono solo se consapevoli di una specifica propensione pericolosa dell'animale, secondo la cosiddetta regola del "one bite rule"[273]. Analogamente, i sistemi di IA, privi di una coscienza propria, sono connotati dal pericolo di generare e diffondere responsi errati o discriminatori; peraltro non correlati da alcuna motivazione che gli consenta di riconoscere l'errore. Potrebbero sottostare alla stessa responsabilità differenziata a

[271] Art. 2052 c.c. - Danno cagionato da animali, in Codice Civile commentato a cura di G. Bonilini, M. Confortini, C. Granelli;

[272] Art. 2052 c.c. - Danno cagionato da animali, Op. cit. riporta che una parte della dottrina ritiene «che gli animali selvatici e la selvaggina da qualificare res nullius esulino dall'ambito dell'art. 2052, con la conseguenza che in caso di danno provocato da animali selvatici si deve applicare l'art. 2043 (…). L'orientamento più recente della giurisprudenza, reputa, invece, che i danni cagionati dalla fauna selvatica sono risarcibili dalla P.A. a norma dell'art. 2052, in base al criterio della "proprietà" o, comunque, sull'utilizzazione dell'animale; peraltro, le specie selvatiche protette ai sensi della L. 11.2.1992, n. 157 , rientrano nel patrimonio indisponibile dello Stato e sono affidate alla cura e alla gestione di soggetti pubblici (Regione) in funzione della tutela generale dell'ambiente e dell'ecosistema»;

[273] The doctrine e.g. "one bite rule" «essentially, means that if a dog bites or attacks another person within its owner's enclosed area, the owner may only be held liable if he or she was aware of the dog's aggressive tendencies. If a dog had never attacked or bitten a person prior to the first incident, it can be argued that the owner had no idea that the dog was vicious or aggressive. However, this rule does not apply to all dog bite cases and it may be possible to bring a personal injury claim even when there is no history of a dog being aggressive (https://www.kirshenbaumri.com/library/the-myth-of-dogs-being-allowed-one-bite-free.cfm);

seconda del livello di rischio implicato[274]. Paragonare i sistemi di IA agli animali permetterebbe di differenziarli in base alla pericolosità grazie alle categorie di animale domestico e animale selvatico. Nella prima categoria verrebbero collocati gli algoritmi più semplici, caratterizzati da un processo di funzionamento prevedibile, ovvero nel genere animale selvatico, qualora presentino classi di analisi più complesse. In effetti sistemi di IA e animali presentano entrambi un comportamento autonomo, imprevedibile e soprattutto inesplicabile, alcune IA sono persino progettate per somigliare ad animali, come il Robot Dog di Boston Dynamics. Pertanto, l'applicazione analogica di questa disposizione permetterebbe di accertare la responsabilità del proprietario per danni commessi da un'IA, che sfugga al suo controllo o che diventi pericolosa sotto la sua guida[275]. Pertanto, la soluzione analogica prospettata, anche senza la distinzione nordamericana tra animali selvatici e domestici, consentirebbe di investire la responsabilità del proprietario del software, o di chi lo sta utilizzando e addestrando per perseguire i propri interessi economici *ex* art. 2052 c.c.

Le esaminate fattispecie di responsabilità oggettiva permettono di sollevare importanti considerazioni in merito alle scelte normative proposte nel paragrafo. Partendo dall'analisi degli artt. 2051, 2052 c.c. emerge la centralità dell'elemento del controllo, della custodia e del dovere di predisporre tutte le precauzioni per evitare l'evento lesivo o la perdita di controllo del sistema. Dagli elementi normativi si potrebbe desumere una responsabilità condivisa tra produttore, sviluppatore, utilizzatore e tutti coloro che abbiano un potere di gestione o di controllo su qualsiasi fase del processo di funzionamento dell'algoritmo. Infatti, l'unico elemento che circoscrive la responsabilità del proprietario/utilizzatore è il caso fortuito inteso come fatto imprevedibile[276], che interrompe del tutto il nesso causale tra il sistema di IA ed il danno. Tuttavia, la disamina

[274] A. Lai, *Artificial Intelligence, LLC: Corporate Personhood as Tort Reform*, in Mich. St. L. Rev., 2021, p. 612, Disponibile al link: https://ssrn.com/abstract=3677360;

[275] L. Anat, AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy, in *Mitchell Hamline Law Review*, p. 17, l'autrice che suggerisce l'analogia conclude che: «I believe the animal analogy is supported by different scholars due to the strong connection we tend to cultivate with AI entities, but overlooks the many disanalogies between them. For this reason, the animal analogy is inappropriate when it comes to AI entities causing harms. In its essence, the keeper or owner of the animal is the one strictly liable with regards to the animal's actions, while the latter is judgment-proof. This relationship in the AI context can be reduced to an agency triangle, which will better illustrate the legal connections between the parties involved»; Disponibile al link: https://open.mitchellhamline.edu/mhlr/vol46/iss5/2 ;

[276] Cassazione civile Sez. III sentenza n. 4742 del 30 marzo 2001;

rivela una maggiore attenzione di dottrina e giurisprudenza per la responsabilità per esercizio delle attività pericolose. La fattispecie disciplinata dall'art. 2050 c.c. risulta particolarmente adeguata al caso in esame, considerando il ruolo centrale che l'elemento del rischio riveste quale presupposto fondamentale per la sua applicabilità. Questo inquadramento peraltro ben "amalgamarsi" al risk-based approach inaugurato dall'AI Act. Seguendo questo filone interpretativo si potrebbe così ipotizzare l'applicazione di una responsabilità oggettiva ex art. 2050 c.c. limitatamente ai sistemi di IA ad alto rischio, ed una più lieve responsabilità per negligenza per i danni arrecati da tutti gli altri sistemi.

7) La circolazione dei veicoli self-driving

Le automobili senza conducente sono effettivamente capaci di circolare con una supervisione umana assente o minima in base al loro grado di autonomia[277]. L'invenzione è epocale se si immagina quanto queste macchine possano concretamente incidere nella prevenzione di incidenti e lesioni stradali. I veicoli driverless per alcuni versi sembrano più sicuri, poiché al riparo dall'errore umano dovuti a disattenzione, eccesso di velocità o stanchezza. Tuttavia, la realizzazione concreta e la commercializzazione di questi veicoli autonomi, unitamente alla garanzia che essi raggiungano livelli di sicurezza superiori a quelli di un conducente umano, rappresentano una sfida ancora aperta. Soprattutto se si considera che per molto tempo le strade vedranno interagire contemporaneamente automobili tradizionali e automobili driverless. Ritardare l'introduzione di questa tecnologia, nell'attesa che essa acquisisca una capacità di analisi avanzata (come il riconoscimento dell'età dei pedoni o dei passeggeri), rischierebbe di prolungare indefinitamente il processo di innovazione, introducendo al contempo nuovi margini di errore. Infatti, se il software affronta diverse difficoltà nell'identificare e contare i pedoni, l'idea che un sistema possa determinare età, sesso, e altre caratteristiche personali sarebbe pura fantascienza al momento, distogliendo l'attenzione dalle applicazioni pratiche immediatamente realizzabili[278]. Allo stesso tempo non si può

[277] Vedi Cap. 1 par. 3 di questa tesi;
[278] U. Ruffolo, *Intelligenza Artificiale e diritto - Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, Op. cit. p. 1702;

ignorare le questioni etiche rilevanti che questi automi si troverebbero ad affrontare ad ogni angolo, e che richiedono decisioni tempestive dinnanzi a collisioni inevitabili.

Come osservato nel primo capitolo, il principale difetto dell'IA è la "black box" che caratterizza il funzionamento e rende opache le decisioni algoritmiche, insieme alla possibile presenza di bias nel set di dati di addestramento o il loro autonomo sviluppo nella fase di apprendimento. L'incidente che ha coinvolto un veicolo a guida autonoma di Uber nel 2018, in cui una donna ha perso la vita, costituisce prova della pericolosità di queste macchine già presenti sulle strade. Questa particolare invenzione ha ricevuto subito grande attenzione da parte di tecnici e politici, data la gravità delle conseguenze potenzialmente connesse al malfunzionamento di una driverless car. Infatti, sebbene sia previsto un meccanismo che consenta di recuperare il controllo sulla vettura, il conducente potrebbe non disporre del tempo necessario per valutare ed intervenire nella dinamica degli eventi. Proprio sulla base di queste particolari caratteristiche, la letteratura suggerisce di adottare regimi di responsabilità specifiche per il tipo di tecnologia[279].

Studi recenti suggeriscono che le case automobilistiche inizieranno a commercializzare veicoli autonomi già nei prossimi anni, con la previsione che entro il 2040 questi veicoli rappresenteranno il 25% del mercato globale; senza contare anche la costruzione di traghetti, aerei, autobus e metropolitane dotate di IA. Pertanto, legislatori e tecnici sono chiamati ad individuare e regolare i rischi di questa tecnologia, dall'incolumità fisica di individui e la sicurezza nelle strade, sino alle più complesse ripercussioni sull'ambiente e l'occupazione. D'altro canto, la loro diffusione contribuirà alla riduzione del consumo di energia tradizionale attraverso l'impiego di fonti rinnovabili e ad una diminuzione del traffico, in quanto i servizi di taxi e car sharing autonomi potrebbero comportare una riduzione del numero complessivo del parco auto cittadino, con evidenti benefici per l'ambiente. I veicoli potrebbero inoltre garantire l'effettiva indipendenza per le persone con limitazioni di mobilità, rendendo il trasporto accessibile anche a coloro non in grado di guidare[280].

[279] V. Papadouli, *Artificial Intelligence's Black Box: Posing New Ethical and Legal Challenges on Modern Societies*, Op. cit. p. 54;
[280] M. Tampieri, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, Op. cit. p. 745;

Le stime di Sicurstrada rivelano che nel 2019 il 90% degli incidenti su strade urbane, e l'87,9% su strade extraurbane, sono stati attribuiti ad errori umani. Sebbene la progressiva adozione dei veicoli autonomi sia destinata a ridurre tali incidenti, non li eliminerà completamente, in quanto la maggiore complessità tecnologica comporterebbe un incremento delle probabilità di guasti tecnici. Tali incidenti possono essere determinati da guasti hardware, malfunzionamenti software, ma anche da problemi nelle infrastrutture stradali o guasti alla rete telematica. Ne consegue che i fattori che interferiscono nel funzionamento di questi prodotti possono esulare dal controllo dei fornitori e utilizzatori delle auto e coinvolgere la rete infrastrutturale dei paesi. Infatti, la stessa risoluzione del Parlamento europeo del 2020 aveva sottolineato come gli incidenti causati dall'IA possono essere ricondotti alla loro produzione, ma varia anche in relazione al numero di auto in una determinata località o all'interferenza da parte di individui. Inoltre, bisogna considerare che i veicoli autonomi introducono nuove tipologie di rischi, ad esempio legati ai malfunzionamenti dei loro singoli componenti, quali sensori, mappe ad alta risoluzione e altri strumenti per raccogliere i dati necessari al loro funzionamento.

Le comunicazioni V2V (Vehicle-to-Vehicle) e V2I (Vehicle-to-Infrastructure), pur contribuendo a migliorare la sicurezza stradale, possono esporre i veicoli a rischi di accesso non autorizzato da parte di reti esterne come attacchi hacker. Tali attacchi non minacciano solo la privacy degli utenti, ma anche diritti fondamentali come il diritto alla vita e alla salute, in particolare nel caso in cui i veicoli autonomi siano manipolati per scopi terroristici. Negli Stati Uniti, la National Highway Traffic Safety Administration (NHTSA) ha emesso raccomandazioni per i produttori, basate su standard internazionali di cibersicurezza, tra cui quelli elaborati dal National Institute for Standards and Technology, dalla SAE e dall'Alliance of Automobile Manufacturers. In Europa, sebbene non siano ancora state introdotte normative vincolanti in questo ambito, il Data Protection Working Party dell'UE ha pubblicato pareri volti a sensibilizzare sui rischi legati all'intelligenza artificiale applicata ai veicoli autonomi e alla loro sicurezza.

In breve, come qualsiasi sistema di IA, anche i veicoli autonomi aumenteranno i loro livelli di sicurezza attraverso l'allenamento; pertanto, solo una diffusione su larga scala, consentirà a questi sistemi di accumulare dati sulle strade e sugli ostacoli del mondo reale. Al fine di realizzare l'ambiente adatto, alcuni governi hanno evitato di adottare un approccio normativo restrittivo, creando zone di deregolamentazione dove le aziende

possono testare i loro dispositivi nel contesto reale. In questo modo le aziende e le autorità hanno la possibilità di osservare le driverless car in azione, nei rapporti con cose e persone, facilitando l'identificazione dei rischi associati. Invece, l'Unione Europea ha optato per una soluzione più prudente testando le auto intelligenti in laboratorio[281], pur riconoscendo la necessità di una revisione delle norme internazionali e nazionali e la necessità di strutturare un sistema di responsabilità civile per risarcire le vittime delle macchine intelligenti[282]. Infatti, in questo contesto diverse questioni giuridiche paiono irrisolte, come la disposizione del codice utile ad ottenere un risarcimento in caso di collisione con una vettura driverless, nonché il soggetto da convenire in giudizio nella scelta tra il costruttore o il conducente dell'auto.

La disamina condotta nei paragrafi precedenti suggerisce innanzitutto di indagare l'applicazione analogica delle disposizioni che regolano la circolazione dei veicoli tradizionali. La disposizione di riferimento nel codice civile italiano è l'art. 2054 c.c., essa presume la responsabilità di entrambi i conducenti nel caso di scontro tra veicoli e la responsabilità dell'unico conducente in caso di scontro dell'auto con persone e cose. Inoltre, richiama in solido anche la responsabilità del proprietario (qualora diverso dal conducente), a meno che quest'ultimo non provi «che la circolazione del veicolo è avvenuta contro la sua volontà». La norma è diretta a tutelare i terzi, vittime della strada, assicurando un risarcimento senza l'onere di provare la colpa del conducente. La norma copre tutti i possibili illeciti che coinvolgono una vettura su strada, sia in marcia che durante la sosta. L'evento lesivo deve essere legato alla circolazione della vettura da un nesso di causalità secondo i principi di causalità materiale e causalità adeguata. Infatti, l'attribuzione della responsabilità al conducente richiede che il suo veicolo abbia innescato una sequenza di eventi culminata nel danno. Tale sequenza di eventi deve essere però prevedibile e fondata su una regolarità statistica. Pertanto, anche in assenza di un impatto diretto tra veicoli, il conducente è ritenuto responsabile qualora la sua condotta, o la circolazione del proprio veicolo, abbia contribuito all'evento dannoso, quale antecedente necessario. Il conducente può sottrarsi alla responsabilità solo dimostrando

[281] G. Puleio, *La gestione del rischio emergente da veicoli autonomi in due proposte di regolamento dell'ue e le conseguenze sull'assicurazione degli operatori*, in juscivile, 2021, p. 1084;
[282] Parlamento europeo, Norme di diritto civile sulla robotica, Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=IT ;

che si è verificato un «un avvenimento improvviso ed esorbitante dalla normalità dei comportamenti umani, che non consenta alcuna manovra per evitare il danno», come nel caso fortuito o nella forza maggiore, eventi che sono imprevedibili, inevitabili e straordinari[283].

In determinati casi anche il comportamento della vittima può concorrere ad interrompere il nesso causale[284]. Ulteriore garanzia a tutela dei danneggiati è la solidarietà passiva che imputa al conducente la responsabilità diretta e al proprietario la responsabilità indiretta, per aver concesso al primo l'utilizzo del veicolo[285]. Proprietario e conducente sono inoltre responsabili in solido per vizi di costruzione o difetti di manutenzione dell'auto. La responsabilità, in tal caso, è di tipo oggettivo, il che implica che l'unico modo per il responsabile di esimersi è dimostrare l'assenza di un nesso causale tra i difetti di costruzione o di manutenzione e l'evento dannoso, attribuendo la causa dell'incidente a un fattore esterno. La manutenzione del veicolo richiede un controllo continuo e costante per garantire la sicurezza del veicolo in strada. Questa seconda ipotesi di responsabilità coinvolge anche coloro che collaborano alla costruzione e manutenzione dell'auto[286].

L'attuale regime sulla circolazione dei veicoli indirizza la responsabilità dell'incidente stradale sul conducente, in quanto soggetto responsabile dello stato dell'auto e del controllo del veicolo su strada. Pertanto, la medesima allocazione sarebbe

[283] Cit. massima Cass. civ., Sez. III, sentenza n. 5667 del 18 settembre 1986;

[284] Per quanto concerne il concorso del pedone nella dinamica dell'incidente la massima relativa alla sentenza dell Cass. civ., Sez. III, 07 luglio 1994, n. 6395 precisa che «Poichè la responsabilità presunta del conducente del veicolo può essere esclusa, ai sensi dell'art. 2054 c.c., solo se risulti provato che quest'ultimo ha fatto tutto i possibile per evitare l'incidente e che non avrebbe potuto, quindi, in alcun modo prevenirlo, nel caso di investimento di un pedone, che abbia attraversato la strada senza rispettare il segnale del semaforo, il conducente del veicolo non può limitarsi a provare che il pedone ha attraversato con il semaforo "rosso" mentre il veicolo giungeva da una distanza che non consentiva manovre di emergenza, ma deve anche dimostrare che il pedone, benchè avvistato, non aveva tenuto un comportamento che denunciasse il suo intento di attraversamento della strada nonostante il divieto o, in altri termini, che il pedone ha iniziato l'attraversamento in modo così repentino che anche la dovuta sorveglianza della strada, da parte del conducente del veicolo, non sarebbe servita ad evitare l'incidente, atteso che tale attraversamento non è del tutto imprevedibile essendo astrattamente possibile che il pedone sia disattento o privo di riflessi adeguati»

[285] Infatti, in tal caso l'unica circostanza che libererebbe il proprietario dalla responsabilità consiste nella circolazione della vettura contro la sua volontà, ad esempio in caso di furto;

[286] ad esempio, in caso di danni causati da difetti degli pneumatici, il costruttore, il rivenditore e il rigeneratore sono solidalmente responsabili, insieme al proprietario e al conducente del veicolo, come stabilito dalla sentenza del Tribunale di Massa del primo luglio 1989, per un approfondimento vedi Art. 2054 c.c. - Circolazione di veicoli, in Codice Civile commentato a cura di G. Bonilini, M. Confortini, C. Granelli;

inopportuna qualora l'utente non avesse più il controllo del mezzo, ovvero la capacità di riprendere tempestivamente il controllo del veicolo ed impedire il realizzarsi del pericolo.

Ebbene, il capitolo I aveva circostanziato l'autonomia delle IA con i livelli di autonomia raggiunti dalle macchine dotate di software di guida, ogni livello di autonomia esige una autonoma valutazione per accertare gli elementi di cui all'art. 2054 c.c. Nello specifico, per i veicoli di livello 0 e 1 non si riscontrano cambiamenti significativi in termini di responsabilità e assunzione del rischio, rispetto al sistema attuale. Analogamente, per i veicoli di livello 2 e 3, dove il ruolo dell'individuo nella guida continua ad essere predominante, nonostante emerga un rischio aggiuntivo legato a potenziali malfunzionamenti dei sistemi tecnologici o della connettività. Le vetture semi-autonome possono soggiacere al regime vigente, il quale tuttavia dovrà essere abbastanza elastico da comporre gli incidenti tradizionali, determinati da disattenzione dell'autista o carenze infrastrutturali, da quelli che invece sono stati determinati della maggiore automatizzazione dell'auto.

Malfunzionamenti che possono coinvolgere le nuove auto autonome possono accadere qualora l'utente non disattivi tempestivamente l'assistente di guida per disattenzione, incapacità, o perché non si renda conto della situazione di pericolo e dell'inadeguatezza del sistema di guida automatico[287]. L'accertamento di queste nuove dinamiche dell'incidente stradale richiede la definizione di nuove regole di cautela e un aggiornamento del codice della strada, nonché valutare l'opportunità di varare un principio di affidamento del conducente assistito nel software di guida. Sebbene storicamente, nella circolazione stradale, si sia esitato a dare rilievo a tale principio, imponendo al conducente l'obbligo di prevedere qualsiasi manovra imprevista o situazione pericolosa, oggi si potrebbe considerare la fiducia che l'uomo ripone nel corretto funzionamento della macchina. Queste considerazioni sollevano la questione di come tale affidamento possa incidere su un giudizio di responsabilità penale nei confronti del conducente. In un futuro caratterizzato dall'interazione tra uomo e macchina, potrebbero verificarsi situazioni in cui la colpa è equamente divisa tra l'azione (o

[287] E. Boeri, *Self-driving cars e profili assicurativi,* in Arch. giur. circ. ass. e resp., 2023, p.11;

l'omissione) umana e il malfunzionamento del veicolo autonomo, configurando una nuova forma di responsabilità condivisa, definita come *culpa in interagendo*[288].

Invece, la circolazione dei veicoli di livello superiore al 3, il sistema di responsabilità richiede un ripensamento radicale, poiché l'interazione umana si riduce progressivamente fino a scomparire del tutto nei casi in cui il veicolo operi senza una persona a bordo in grado di prenderne i comandi. Pertanto, si deve evincere l'insussistenza dei presupposti del controllo e della gestione della vettura nelle self-driving car di livello L4 e L5[289], in grado di condurre la tratta in assoluta autonomia, dispensando il proprietario sia dall'obbligo di condurre l'auto, sia di intervenire in presenza di ostacoli. Ne consegue l'impossibilità di applicare l'art. 2054 c.c. alle vetture totalmente automatizzate per due ordini di considerazioni. In primo luogo, la disposizione configura una responsabilità presunta del conducente, ma implica comunque una valutazione -in astratto- di colpevolezza. Infatti, il conducente può liberarsi dalla responsabilità dimostrando di aver fatto tutto il possibile per evitare il danno. Questa valutazione è tuttavia impossibile per le auto driverless in quanto, come si può desumere dal nome, il ruolo del conducente non è previsto nel sistema di guida. Invece il secondo ordine di riflessione valuta la scelta allocativa alla luce dell'impatto economico che avrebbe sul mercato e la società, valutando la distribuzione degli incentivi e delle esternalità negative derivanti dal prodotto. Dunque, sotto questo profilo l'applicazione dell'art. 2054 c.c. appare inefficace poiché attribuisce il rischio di incidente al conducente che non possiede né gli incentivi né i mezzi necessari per mitigare tale rischio. Infatti, in questo caso il conducente non conduce più, ha perso il controllo della vettura e il potere di influenzare il futuro sviluppo del software che ne controlla la guida automatizzata[290]. Pertanto, in tale contesto, più che di conducente si potrebbe parlare di acquirente di un prodotto oppure, grazie ad una interpretazione molto elastica, utente di un servizio di trasporto.

Quindi, sebbene non sussistano i presupposti giuridici ed economici per ritenere il conducente colpevole, il quarto comma dell'art. 2054 c.c. fornisce una diversa e più utile

[288] L. D'Amico, *intelligenza artificiale e auto a guida autonoma. tra prevenzione primaria, colpa penale e rischio consentito artificial intelligence and self driving cars. between primary prevention, criminal negligence and allowed risk,* in Riv. It. Med. Leg., 2022, p. 608;
[289] Vedi capitolo 1, p. 12;
[290] A. Davola, R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in Danno e Responsabilità, n. 5, 1 settembre 2017, p. 620;

allocazione del danno. Il legislatore del 1942 considera l'ipotesi che la collisione sia stata determinata da un malfunzionamento o difetto dell'auto dando al conducente la possibilità di chiamare in causa, o agire in rivalsa, il produttore per responsabilità del prodotto difettoso, o il meccanico che non abbia svolto diligentemente la riparazione. Si configura a carico di questi ultimi una responsabilità oggettiva basata esclusivamente su un difetto di costruzione o di manutenzione, in linea con quanto stabilito dalla direttiva 85/374/CEE e dal codice del consumo. In tale contesto, il produttore appare l'unico soggetto in grado di monitorare e correggere eventuali difetti del sistema, migliorando così l'affidabilità e la sicurezza dei veicoli, risulta il soggetto più idoneo a rispondere dei danni[291]. Infatti, secondo la normativa vigente, risulta particolarmente complesso per la parte danneggiata dimostrare l'esistenza di un difetto del prodotto e il nesso causale tra tale difetto e il danno subito. Allo stesso modo il consumatore incontra delle difficoltà nel provare che il prodotto non garantisce la sicurezza che ci si può legittimamente attendere dal prodotto, come richiesto dalla direttiva prodotti difettosi. La scelta di attribuire i costi risarcitori al produttore riconoscendogli la responsabilità, anche senza accertare la colpa, sembra efficiente dal punto di vista economico-giuridico. Infatti, questo approccio incentiva la ricerca di sistemi più affidabili e trasparenti, che tengano traccia dei processi funzionali e per dimostrare la sicurezza dei loro programmi e l'assenza di colpa. La prospettiva di responsabilità futura incoraggerebbe una maggiore attenzione alla sicurezza e alla trasparenza già nelle fasi iniziali della progettazione. Tuttavia, come già osservato, un regime di responsabilità senza colpa potrebbe, di fatto, scoraggiare i progettisti e i produttori dall'investire sulla tecnologia IA, a causa delle frequenti condanne di liquidazione del danno. Un effetto deterrente, che allontana le imprese dall'innovazione, il quale potrebbe essere attenuato tramite un'eccezione che esima i produttori dalla responsabilità per i rischi imprevedibili al momento della progettazione del sistema complesso[292].

Questa soluzione, molto simile alla difesa del rischio da sviluppo, riuscirebbe a mantenere l'alea del rischio dei produttori di auto driverless in confini determinati più facili da assicurare. Inoltre, sia qualora si optasse per un a responsabilità per colpa, che

[291] M. Tampieri, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, Op. cit. p. 755;
[292] M. Monot-Fouletie, *Liability for Autonomous Vehicle Accidents*, in
The Cambridge Handbook of Artificial Intelligence Global Perspectives on Law and Ethics, Cambridge University Press, 2022, p. 169;

una responsabilità oggettiva, sarà utile elaborare guide lines e best practice per accertare la negligenza o il difetto del prodotto. Infatti, constatata l'assenza di un autista umano, si deve prendere atto della sostanziale autonomia del driver digitale garantendo la sua capacità di guidare in sicurezza. In questa prospettiva è necessario elaborare un codice di condotta per imprenditori e ingegneri che stabilisca le misure di sicurezza che costituiscano uno standard minimo di diligenza e che stabilisca, al contempo, un margine di tolleranza per gli errori commessi nella ideazione e produzione del sistema.

Il livello di sicurezza imposto a ciascun'automobile varia in base al livello di autonomia del veicolo. Per i veicoli completamente autonomi, si prospettano situazioni in cui il danno è principalmente imputabile alla macchina stessa, rendendo tali eventi penalmente irrilevanti ma perseguibili in sede civile per ottenere una compensazione del danno. Tale scenario richiama una versione moderna del "danno anonimo", tipico di contesti tecnologicamente avanzati dove è estremamente difficile, se non impossibile, individuare con precisione il responsabile di un danno[293]. Il mantenimento dei costi di progettazione e assicurativi è necessario anche per contenere i costi del prodotto sul mercato[294]. D'altronde l'introduzione di ogni innovazione richiede un periodo di assestamento e di dialogo tra tecnica e diritto per comprendere i rischi e tracciare i confini dell'alea ritenuta dalla società accettabile. Il bilanciamento tra il pericolo residuale ed ineliminabile e l'interesse allo sviluppo della tecnologia costituisce la base per la definizione del regime di responsabilità civile e del generale sistema di governance.

8) La RC in crisi tra la ricerca di criteri di imputazione della responsabilità, l'individuazione del rischio consentito e la funzione redistributiva

[293] L. D'Amico, *intelligenza artificiale e auto a guida autonoma. tra prevenzione primaria, colpa penale e rischio consentito artificial intelligence and self driving cars. between primary prevention, criminal negligence and allowed risk*, Op. cit. 610;
[294] A. Albanese, *Mobilità del futuro e funzione preventiva della responsabilità civile*, in Europa e Diritto Privato, 2023, pag. 444;

Dal 1950 ad oggi, le fattispecie di responsabilità civile sono progressivamente aumentate. La causa dell'ampliamento risiede nell'ampiezza delle formule generiche adottate dal codice civile, come le nozioni di "illecito" e "danno ingiusto", che non vincolano l'applicazione della fattispecie a particolari attività o condotte. In questo incremento concorre anche il contesto socio-economico determinato dall'aumento di attività pericolose ammesse nell'ordinamento, ed il conseguente aumento degli incidenti e dei danni risarcibili. La responsabilità civile si è affermata come un mezzo per la tutela dei diritti fondamentali, l'art. 2043 c.c. e la condanna al risarcimento del danno è divenuto con il tempo un utile strumento di affermazione di interessi individuali. Il diritto alla privacy o il diritto alla salute sono spesso citati quali contraltari necessari per imporre l'avanzamento tecnologico ed industriale con i diritti civili e sociali, svolgendo in alcuni anche una funzione punitiva e di deterrenza.

L'elasticità delle disposizioni sulla responsabilità civile l'ha resa un'efficacie strumento per orientare le attività economiche private verso gestioni più virtuose ed attente a fare tutto il possibile per evitare l'evento dannoso. In particolare, questa visione della responsabilità civile è stata sostenuta anche dall'Unione Europea, che ha introdotto la responsabilità del produttore con questo intento. Tuttavia, tale misura ha incontrato l'iniziale opposizione di coloro che consideravano prioritario l'interesse imprenditoriale. Infatti, durante il XIX secolo e gran parte del XX secolo, il progresso industriale e tecnologico è stato agevolato dal mancato risarcimento delle vittime, consentendo ridurre i costi e raccogliere il capitale necessario allo sviluppo economico[295]. Il trend è proseguito fino a quando non è stato invertito da una politica più orientata a tutelare le vittime, spesso a scapito di chi causa il danno. Questo cambiamento ha comportato una maggiore disincentivazione ad assumere rischi o, in alternativa, una gestione o eliminazione di tali rischi attraverso mezzi alternativi, come la stipulazione di polizze assicurative.

Ebbene, il XXI secolo ha portato nuovi ritrovati della tecnica e scoperte nel campo delle scienze, dell'ingegneria e dell'informatica, tra i quali appunto la tecnologia IA. Pertanto, il sistema di responsabilità civile si trova di nuovo al centro del dibattito sull'equilibrio tra interessi tecnico-industriali e rispetto dei diritti civili; tuttavia, gli attuali

[295] M. Franzoni, *La responsabilità civile una lunga storia ancora da scrivere*, in Contratto e Impresa, 2021, p. 1108, che in merito afferma « Il risparmio di spesa dei mancati risarcimenti ha costituito una sorta di accumulazione originaria per lo sviluppo dell'economia capitalistica»;

ordinamenti dovrebbero essere in grado di garantire la pace sociale e non sacrificare i diritti fondamentali sull'altare del capitalismo.

L'IA e l'IoT rappresentano le principali innovazioni di questo secolo e caratterizzano la cd. Quarta Rivoluzione industriale. Questa tecnologia non costituisce soltanto una nuova categoria di prodotti, intelligenti e connessi, ma è una tecnologia in grado di rivoluzionare il processo di produzione dei beni, distribuire servizi, svolgimento di prestazioni e mansioni. La capacità di analizzare una quantità di dati per trovare risposte in tempi brevi è una capacità utile per velocizzare in special modo le prestazioni professionali. Di conseguenza anche il sistema di responsabilità civile si trova ad affrontare le questioni giuridiche sollevate dalla tecnologia a causa del suo utilizzo in tutti i settori economici e sociali. Un esempio è rappresentato dall'impiego dell'IA nel settore sanitario, qualora il medico utilizzi strumenti di *clinical decision support system*, software IA di supporto all'attività diagnostica e terapeutica, la cui efficacia è aumentata grazie a ulteriori tecnologie di supporto come la cartella clinica elettronica. Questi sistemi possono ricoprire autonomamente diverse mansioni: riducono gli errori nella prescrizione di terapie e medicinali, assicurano il rispetto delle linee guida, segnalano la necessità di un follow-up del trattamento, propongono opzioni di farmaci o trattamenti più economici, suggeriscono diagnosi sulla base dei dati del paziente[296]. Di conseguenza l'utilizzo di questi device impatterà sulla responsabilità professionale del medico, infatti si possono delineare tre scenari possibili: (1) il medico attenda un'indicazione algoritmica errata, (2) il medico adempia alle indicazioni corrette del sistema di IA, ma si verifichi comunque un danno, e (3) il medico si discosta da un'indicazione corretta senza addurre giustificazioni. Nonostante l'affidabilità di tali sistemi, persiste una certa percentuale di rischio per gli errori. La responsabilità del medico potrebbe emergere dal mancato rilevamento di errori nella decisione algoritmica, che solo lui potrebbe individuare attraverso l'anamnesi e l'esame fisico del paziente. Nonostante l'elevato grado di automazione, i sistemi di supporto alla diagnosi continuano a richiedere l'intervento del medico, il quale svolge un ruolo cruciale nell'implementazione e nell'interpretazione delle indicazioni algoritmiche.

[296] R. T. Sutton, D. Pincock, D. C. Baumgar, D. C. Sadowski, R. N. Fedorak, and K. I. Kroeker, *An overview of clinical decision support systems: benefits, risks, and strategies for success*, in npj Digital Medicine, 2020, p. 3, disponibile al link: https://www.nature.com/articles/s41746-020-0221-y ;

Naturalmente anche con il livello di personalizzazione raggiunto dalla macchina l'intervento medico rimane indispensabile, quanto meno per l'effettiva attuazione delle terapie indicate dall'IA. Orbene, per la valutazione della responsabilità sanitaria 2.0 possono concorrere diversi fattori ad aver determinato il responso erroneo, come la chiarezza delle istruzioni fornite dal produttore; nella circostanza addotta ad esempio la condotta del medico professionista verrebbe ritenuta di maggiore gravità qualora le istruzioni fossero chiare e quest'ultimo non le avesse rispettate. Al contrario, nel caso in cui l'errore risultasse di minore entità o la tecnologia particolarmente complessa, della responsabilità per negligenza potrebbe essere valutata meno severamente[297].

In sede di giudizio il giudice deve dirimere diverse interpretazioni della collaborazione professionista-macchina. Potrà ancora essere definita la prestazione sanitaria un'attività tecnica di speciale difficoltà? Ai sensi dell'art. 2236 c.c. è esonerato da responsabilità il prestatore che non soddisfi il creditore qualora la mansione richiedesse la risoluzione di problematiche tecniche di speciale difficoltà. La fattispecie menzionata determina la particolare diligenza a cui sono tenuti i prestatori d'opera (professionisti, medici, avvocati, notaci ecc.) che, in quanto prestatori d'opera intellettuale, non sono tenuti al raggiungimento del risultato ma a svolgere la mansione con la diligenza e la perizia richieste dalla particolare prestazione. Questa prerogativa contrassegna le cd. obbligazioni di mezzi che richiedono conoscenze scientifiche e tecniche le quali, tuttavia, potrebbero risultare comunque non sufficienti ad assicurare al creditore il risultato atteso; come, ad esempio, in caso di malattie e terapie sperimentali[298]. Ebbene, in questi contesti, occorre comprendere quale ruolo e quale incidenza possano giocare ora i sistemi di IA nella risoluzione di problemi tecnici: se costituiscano uno strumento risolutivo e decisivo o se, al contrario, sono ancora troppo aleatori, erronei e passibili di censura per essere ritenuto affidabile. Quindi, l'interprete potrebbe concludere non più sussistente la speciale difficoltà grazie all'utilizzo dell'IA; oppure il medico che non abbia rilevato l'errore del software o abbia mancato di interrompere tempestivamente il suo funzionamento potrebbe così configurare una nuova fattispecie di malpractice[299]. Una fattispecie simile

[297] A. G. Grasso, *Diagnosi algoritmica errata e responsabilità medica*, in Rivista di diritto civile, 2023, p. 347; C. Scarpellino, *Responsabilità nell'e-health*, in Comparative Law Review, 2022, p. 189;
[298] *Art. 2236 c.c. – Responsabilità del prestatore d'opera*, in *Codice Civile commentato* a cura di G. Bonilini, M. Confortini, C. Granelli;
[299] A. G. Grasso, *Diagnosi algoritmica errata e responsabilità medica*, op. cit. p. 351 che sul punto circostanzia: « Peraltro, il professionista che, a causa dell'assoluta novità dello strumento, non ne utilizzi

è stata prefigurata nel paragrafo precedente, descrivendo i possibili incidenti automobilistici causati dall'utilizzo di veicoli driverless, e che pone i medesimi dubbi sul confine tra l'azione dell'uomo e il funzionamento della macchina nella dinamica di un incidente[300].

Una volta accertato il ruolo predominante del software, rispetto alle azioni dell'utilizzatore, sia esso consumatore o professionista, nella catena causale degli eventi che ha provocato il danno, è fondamentale identificare i responsabili del malfunzionamento dell'IA, coinvolti nel processo di produzione e sviluppo. L'AI Act tenta un elenco esemplificativo di soggetti obbligati, in particolare menziona: il produttore, l'ideatore del software o dell'algoritmo su cui si basa il software, il programmatore, il collaudatore e il trainer, l'utente finale qualora lo utilizzi per scopi professionali[301]. La scelta della controparte alla quale destinare la propria citazione rappresenta una scelta principalmente di natura giuridica-economica, diretta ad evitare che l'adozione delle tecnologie digitali comporti una riduzione dei livelli di sicurezza e responsabilità, attribuendo il costo dei danni al soggetto più adatto a minimizzarli. Pertanto, il soggetto responsabile dovrà essere individuato tra tutti gli operatori coinvolti nella "catena del valore" dei sistemi intelligenti. Questa definizione non facilita l'individuazione del colpevole a causa della complessità del sistema di IA, dei molteplici soggetti che collaborano per la costruzione di un device e della sovrapposizione dei loro ruoli e competenze nel processo di ideazione e produzione del prodotto. In questo contesto è difficile delineare una precisa progressione causale degli eventi e ancor di più riuscire ad individuare l'errore e il soggetto deputato ad evitarlo attraverso il tradizionale giudizio controfattuale. Infatti, l'elevato numero di soggetti potenzialmente responsabili rappresenta un ulteriore, anche di natura economica, per la parte che intende intraprendere

al meglio le funzioni o non riconosca l'errore in cui è incorso l'algoritmo, potrebbe essere considerato alla stregua di un medico poco esperto, privo di una formazione adeguata ad adoprare un mezzo così` tecnologicamente innovativo: sì che la fattispecie rientrerebbe nel perimetro di applicazione della regola che dottrina, giurisprudenza e Corte costituzionale hanno confinato ai casi di imperizia»;

[300] E. Boeri, *Self-driving cars e profili assicurativi*, op. cit. p. 9 descrive l'interrelazione uomo-macchina «I veicoli autonomi sono sistemi complessi di sensori e hardware controllati da un enorme varietà di sistemi software, alcuni dei quali possono anche essere non deterministici, nel senso che, dato un certo input, il sistema potrebbe restituire danno un output inaspettato e imprevedibile. Oltre a ciò, l'autovettura a guida automatica si troverà a rilevare i problemi e prendere decisioni in una serie di situazioni che potrebbero non essere tutte previste dal produttore del software»

[301] A. D'Adda, *Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo*, in Rivista di diritto civile, 2022, p. 825;

azioni legali per ottenere un risarcimento[302]. Pertanto, è compito del legislatore assicurare che le vittime possano facilmente identificare e raggiungere i responsabili. In generale sia dottrina che policymaker hanno identificato il fornitore quale soggetto responsabile. Tuttavia, diversi attori potrebbero essere identificati quali produttori, ad esempio, per aver prodotto un singolo componente del device individuato quale fonte del malfunzionamento. Si evidenzia inoltre che, qualora venisse usato come criterio di imputazione il controllo dell'AI al momento del danno dovrebbero concorrere altre figure, nella catena di responsabilità, come gli utilizzatori, e professionisti incaricati di monitorare il funzionamento della macchina. Questi professionisti, come evidenziato nelle recenti proposte europee, non sempre coincidono con il produttore[303].

Alla luce del contesto produttivo descritto e della molteplicità di potenziali operatori economici nella catena causale del danno, la dottrina suggerisce un modello di responsabilità solidale che incentivi la riduzione dei rischi a monte e garantisca una giusta ripartizione dei costi di risarcimento a valle. Il fondamento di questa responsabilità condivisa potrebbe essere rintracciato nell'«obiettivo comune, consistente nel progettare, programmare e produrre un'intelligenza artificiale e le sue componenti»[304]. All'atto pratico, il giudice dovrà indagare l'apporto del programmatore, del produttore, dell'esercente del servizio che lo utilizza, e degli eventuali soggetti terzi coinvolti (proprietari, utilizzatori, gestori di rete ed eventuali hacker) nella catena causale che ha determinato il danno. Sebbene l'ideatore dell'algoritmo ricopra un ruolo centrale, la sua responsabilità deve essere condivisa con quella del produttore e dell'utilizzatore/proprietario. Infatti, quest'ultimo non dovrebbe essere esonerato dalla responsabilità, anche se privo delle competenze necessarie per comprendere o correggere l'algoritmo, poiché al momento dell'acquisto e dell'utilizzo del sistema l'utilizzatore accetta i rischi dichiarati dal costruttore. Diversamente, si rischierebbe di ridurre la protezione per la vittima nell'ottenere le informazioni necessarie per intraprendere azioni legali contro l'ideatore o il programmatore dell'algoritmo[305].

---

[302] G. D'Alfonso, *Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules*, in European Journal of Privacy Law & Technologies, 2022, p. 30;
[303] A. D'Adda, *Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo*, Op. cit. p. 827;
[304] G. D'Alfonso, *Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules*, op. cit.
[305] Vedi Supra p. 32;

D’altronde anche la direttiva sulla responsabilità da prodotto aveva optato per un regime di compensazione solidale *ex* art. 2055 c.c., al fine di garantire una protezione più ampia al danneggiato. Questa normativa esclude la responsabilità dei produttori o fornitori di componenti difettosi solo nel caso in cui il difetto sia completamente attribuibile alla progettazione del prodotto, in cui tali componenti sono state integrate (art. 7, lett f)[306]. La *ratio* garantista sembra la più solida, in quanto non vi sono prove che tutti gli imprenditori e professionisti coinvolti siano consapevoli dell’“obiettivo comune”. Peraltro, è più che plausibile che i fornitori di componenti minori non siano a conoscenza del progetto complessivo del software, data l'attenzione particolare rivolta alla protezione del segreto industriale.

In aggiunta alle esposte problematicità relative all’imputazione dei danni da algoritmo si devono tuttavia menzionare anche le opportunità determinate dalle nuove tecnologie, rispetto alla raccolta e trattamento dei dati. Infatti, se da un lato l’IA processa in assoluta autonomia i dati per estrapolarne risposte, permette anche di beneficiare di dispositivi come l'Event Data Recorder installato sui veicoli self-driving. Si tratta di un dispositivo capace di ricostruire la dinamica degli incidenti attraverso la registrazione di ciò che accade nel veicolo, riportando fedelmente sia le azioni del conducente, sia le operazioni compiute dall’auto. Le registrazioni della scatola nera consentirebbero di osservare il comportamento del conducente, accertando eventuali violazioni del codice della strada o delle istruzioni fornite con il veicolo. In questo modo si può valutare ogni comportamento negligente ai fini della distribuzione dei costi risarcitori tra utilizzatore e produttore, ai sensi dell’art. 1227 c.c. . Parimenti, la compagnia assicurativa, chiamata a liquidare il risarcimento, può utilizzare i dati registrati dalla scatola nera sia per ridurre la propria responsabilità verso terzi, provando il concorso colposo del danneggiato (art. 1227 c.c.) o di altri soggetti che abbiano contribuito al danno o ne abbiano aggravato le conseguenze (art. 2055 c.c.), sia per avviare un'azione di rivalsa nei confronti del proprio assicurato, qualora il veicolo non fosse a norma. Quindi, la vendita al pubblico di veicoli dotati di Event Data Recorder (EDR) contribuirebbe ad aumentare la fiducia dei consumatori nei veicoli driverless, che spesso dubitano dell’affidabilità dei sistemi di assistenza di guida. Inoltre, l’EDR incentiva un maggior livello di attenzione nella guida dei conducenti che,

[306] A. D’Adda, *Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo*, Op. cit. p. 829;

consapevoli di essere costantemente registrati, saranno maggiormente indotti a non commettere violazioni del codice della strada[307]. Il maggior flusso di informazioni comporterà anche una riduzione dei premi assicurativi, in quanto l'assicuratore potrà avere accesso ai dati sulle abitudini di guida del cliente, nonché informazioni dirette sulle dinamiche degli incidenti. In sintesi, la nuova tecnologia potrebbe contenere in sé gli strumenti di controllo, gestione e registrazione del rischio algoritmico e dei rischi tradizionali.

Le considerazioni sopra esposte spingono i policymaker a ripensare i due principali modelli utilizzati per l'attribuzione della responsabilità, a causa della inapplicabilità dei tradizionali criteri di imputazione. In particolare, i modelli di responsabilità oggettiva e presunta, fondati per lo più sul presupposto della gestione del rischio, scelgono di imputare la responsabilità al soggetto più vicino al prodotto, l'unico nella posizione di migliorare i dispositivi attraverso misure di sicurezza e monitoraggio. Inoltre, permette di attribuire all'impresa i costi risarcitori, anche qualora abbia adottato tutte le precauzioni necessarie, accollandole l'inevitabile ed intrinseco rischio "residuo" delle nuove tecnologie. Infatti, questo schema normativo attribuisce al fornitore il rischio della mancata prova pagando il risarcimento del danno anche nel caso rimanga incerta la causa effettiva dell'incidente. Il secondo modello di responsabilità, basato sulla colpa e in particolare sulla negligenza, richiede un quadro normativo ben definito e regole tecniche specifiche per valutare la condotta degli imputati[308].

Ad ogni modo nessuno dei due regimi descritti è in grado di colmare il "liability gap" riscontrato nei danni da algoritmo. La questione appare irrisolvibile a causa della matrice culturale antropocentrica che ritiene l'uomo unico possibile soggetto responsabile, in quanto detentore del controllo sulle macchine. Da questo assunto deriva l'inconciliabilità tra gli attuali criteri di imputabilità e il funzionamento delle macchine dotate di deep learning dichiaratamente imprevedibili e incorreggibili. Pertanto, al fine di coniugare l'interesse sociale alla vendita di prodotti sicuri e le istanze dell'imprenditoria privata alla sperimentazione e all'avanzamento tecnologico, il legislatore europeo ha preferito

[307] E. Al Mureden, *Event Data Recorder e advanced driver assistance systems: la "spinta gentile" verso la mobilita 'del futuro*, in Contratto e Impresa, 2022, p. 390;
[308] G. D'Alfonso, *Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance" rules*, op. cit. p. 33;

adottare un sistema di governance e gestione del rischio, rispetto alla definizione di un quadro armonizzato sulla responsabilità civile. Lo schema imposto dall'AI Act ha infatti scelto misure e requisiti per le IA "ad alto rischio", mentre per tutti i sistemi con rischio minimmo, ci si limita ad obblighi di trasparenza, regole “etiche”, codici di condotta e norme di soft law[309]. In sostanza, la piramide disegnata dall’AI Act cerca di standardizzare il rischio in categorie predeterminate, cionondimeno nelle cause di responsabilità deve essere accertato il rischio in concreto, per comprendere se la macchina o un elemento esterno ed imprevedibile (caso fortuito o forza maggiore) abbia determinato il danno.

Il sistema di governance europeo mira a bilanciare i benefici dell'IA, come l'efficienza e la rapidità nella distribuzione dei servizi, con i potenziali rischi per i diritti fondamentali, la salute e la sicurezza. Infatti, il Regolamento individua un esemplificativo elenco di attività che i sistemi di IA non possono svolgere, in quanto comportano rischi troppo elevati rispetto ai benefici. Invece, i sistemi ad alto rischio presentano un rischio socialmente accettabile, a condizione che vengano rispettate le restrizioni ed i controlli imposti dalla norma e atti a ridurre in rischio ad un’alea ritenuta socialmente accettabile. Dalla lettura sistematica del Regolamento, della AILD e della PLD possiamo delineare un quadro normativo abbastanza elastico, che indirizza la responsabilità civile dei sistemi di IA verso il più favorevole regime della responsabilità oggettiva (PLD), qualora il danneggiato abbia acquistato direttamente il software malfunzionante. Invece, in tutti gli altri casi, l’attore avrà a disposizione l’azione della responsabilità per colpa (AILD), agevolata dalla obbligatoria esibizione della documentazione. Questo approccio appare del tutto in linea con quanto previsto per le altre attività socialmente necessarie, ma potenzialmente pericolose[310].

---

[309] F. Caroccia, *Ancora su responsabilità civile e uso delle intelligenze artificiali*, in Contratto e Impresa, 2022, p. 417;

[310] J. Chamberlain, *The Risk-Based Approach of the European Union’s Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, in European Journal of Risk Regulation, 2023, p. 8, l’autrice in merito alle direttive AILD e PLD, ed il loro rapporto con le categorie di rischio, osserva « According to the proposal for a revised directive on product liability, AI products are covered by the directive – meaning that damages may be awarded for material harm (including medically recognised psychological harm) caused by a defective AI-enabled good. Both in this proposal and in the proposed directive on civil liability for AI, a central theme is the alleviation of the plaintiff’s burden of proof in cases where it is challenging to establish the causal link between damages and an AI system»;

Pertanto, l'AI Act avrebbe delimitato i confini del rischio accettabile, e spostato l'accertamento del giudice dalla liability alla accountability. D'altronde la centralità dell'accountability è apparsa una scelta razionale, in considerazione del ruolo che assumono i dati personali e il loro trattamento nel funzionamento dell'IA e del principio di accountability espresso nel GDPR. In questo modo verrebbe superato il tradizionale modello fondato sulla prova dell'illecito e della colpa dell'art. 2043 c.c., che presuppone la colpevolezza o il dolo per trasferire le conseguenze dannose dal patrimonio del danneggiato a quello del danneggiante. Ebbene il principio di accountability impone a colui che svolge il trattamento dati di tenere traccia e dimostrare di aver adottato tutte le misure tecniche e organizzative richieste dalla legge e in grado di rispondere ai rischi implicati dalla loro attività[311]. Il sistema piramidale di governance disposto dall'AI Act si è impegnato a fornire uno schema di requisiti ed obblighi (per ora ancora generali) in grado di conoscere e gestire il più possibile una tecnologia che potrebbe avere risvolti di portata sia individuale che collettiva. Tuttavia, una domanda resta insoluta nel sistema di responsabilità civile disegnato dalla AILD e dalla PLD, ossia su chi grava il rischio della mancata prova. Quale soggetto, tra tutti gli attori coinvolti, sopporterà il costo del danno nel caso in cui non si rinvenga la causa e tutti i soggetti obbligati abbiano effettivamente adempiuto le prescrizioni di legge.

Ebbene, il sistema di responsabilità giuridica per i danni arrecati dall'IA deve tenere conto delle esigenze della nuova tecnologia, della ricerca e della società. In questa prospettiva, il produttore risulta essere il soggetto più adatto a rispondere dei danni causati dai veicoli automatizzati, sia dal punto di vista economico, poiché ne trae i profitti, sia sotto il profilo giuridico, in quanto ha il controllo sul processo di produzione ed è responsabile del suo monitoraggio, durante l'intero ciclo di vita del prodotto. Allo stesso tempo, il regime di responsabilità non deve ridurre gli investimenti sulla ricerca, né causare un eccessivo aumento del prezzo del prodotto, che limiterebbe la diffusione dell'IA ad una fetta privilegiata di persone. Il bilanciamento di queste esigenze in realtà ha contrassegnato il processo di accettazione e regolazione di tutte le innovazioni del passato. I vaccini, ad esempio, sono prodotti altamente innovativi che apportano enormi benefici alla collettività, ma anche che comportano una serie di rischi collaterali alla

[311] M. Scotto di Carlo, *La responsabilità connessa all'utilizzo dei sistemi di intelligenza artificiale*, in Danno e Resp., 2024, p. 424;

salute. Negli Stati Uniti il rischio di danno alla salute è stato ridistribuito tramite l'istituzione di un fondo di compensazione no-fault per i vaccini. Nel caso dei veicoli automatizzati, la sola istituzione di un fondo di garanzia non sarebbe di per sé sufficiente ad arginare il rischio in modo efficiente, poiché potrebbe ridurre gli incentivi per i produttori nello sviluppare tecnologie più sicure. Dunque, si suggerisce una forma di responsabilità oggettiva con un fondo di garanzia a cui attingere per compensare gli incidenti occorsi in assenza di una violazione di legge[312].

Il bene della società non deve essere perseguito a costo di pochi, quei pochi devono essere risarciti, per il pericolo che sfortunatamente li ha coinvolti. Questo principio di solidarietà ha ispirato anche il sistema di responsabilità oltralpe, che ha suggerito un superamento dei comuni criteri di imputazione per garantire il principio di solidarietà tra consociati. Difatti, la legge francese Kouchner del 2002 stabilisce che, in assenza di prove che conducano ad un responsabile, le vittime di malasanità devono comunque essere risarcite in base al principio di solidarietà[313]. Questo modello potrebbe essere applicato anche ai veicoli autonomi, dove la difficoltà di provare la responsabilità e allocare i costi rende necessario un sistema che garantisca risarcimenti equi, mantenendo comunque la responsabilità di progettisti e produttori.

In conclusione, i conflitti derivanti dall'uso del digitale e dell'intelligenza artificiale risultano sempre più complessi da risolvere attraverso il tradizionale concetto di colpa, il cui presupposto si fonda sulla volontà consapevole dell'individuo. L'intelligenza artificiale, pur non sostituendo l'intelligenza umana, si propone di eseguire compiti e prendere decisioni in modo autonomo. Ciò comporta che, in caso di incidente provocato da un veicolo autonomo, il concetto di colpa potrebbe non costituire lo strumento più idoneo per risolvere il conflitto, in quanto manca del tutto l'elemento della volontà. Quindi si devono trovare altri criteri per stabilire la responsabilità, come quello del profitto o della gestione del rischio. Inoltre, anche qualora si stabilisse una responsabilità oggettiva a carico di un solo attore, altri meccanismi potrebbero sopraggiungere per

[312] A. Davola, R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, Op. cit. p. 629;

[313] M. Monot-Fouletie, *Liability for Autonomous Vehicle Accidents*, op. cit. p. 174, l'autrice in relazione a questo specific Sistema di No-Fault per danni arrecati a causa di una prestazione sanitaria specifica che «In such cases, a State public establishment, the Office National d'Indemnisation des Accidents Médicaux (National Office for the Compensation of Medical Accidents), compensates the victims under conditions that guarantee both fair coverage of the harm and effective accountability of the various actors involved»;

ridistribuire i costi, come l'articolo 2055 c.c. o le disposizioni del codice del consumo in materia di prodotti difettosi[314]. Per sfruttare al meglio tutte le funzioni della responsabilità civile la scelta del sistema da adottare dovrebbe contestualizzarsi all'interno dei meccanismi di governance che, come introdotto nel secondo capitolo, contempla quattro necessarie fasi: conformità, comunicazione, sorveglianza e attuazione[315]. La responsabilità può essere vista come l'attuazione concreta della norma, attraverso la verifica, caso per caso, della regolarità della condotta tenuta dai fornitori/distributori/utilizzatori. In questo processo, tali soggetti devono rendere conto alle autorità competenti del loro operato in relazione alla specifica situazione.

Orbene, dato che il sistema di governance deve proporre un insieme equilibrato di diritti e doveri, qualora il regime di responsabilità civile prescelto sia di tipo oggettivo (come quello proposto dalla PLD), sarà necessario rafforzare in modo corrispondente la fase di compliance, attraverso l'emanazione di linee guida, best practice e codici di condotta, elementi fondamentali per rendere effettivamente censurabile il comportamento illecito. Invece, qualora si volesse optare per una responsabilità per colpa, anche presunta (come quella prevista dalla AILD) sarà necessario emanare linee guida, ma anche prevedere procedure interlocutorie tra le amministrazioni competenti e strumenti di sperimentazione normativa, per fornire a produttori e programmatori i dati e le procedure utili per sviluppare l'IA più sicura possibile.

[314] M. Franzoni, *La responsabilità civile e gli ottant'anni del codice civile*, in Responsabilità Civile e Previdenza, 2022, p.1453;
[315] C. Novelli, M. Taddeo, L. Floridi, *Accountability in Artificial Intelligence: What It Is and How It Works*, op. cit.;

Capitolo IV
Nuove soluzioni alla risarcibilità del danno da algoritmo: tra personalità giuridica, fondi di compensazione e sistema di no-fault

1) La responsabilità civile per i sistemi di IA: tra vecchie e nuove soluzioni

I capitoli precedenti hanno illustrato cause e caratteristiche del liability gap generato dai sistemi di IA negli ordinamenti globali. In particolare, è stato evidenziato il peso che la questione assume soprattutto per i sistemi di IA ad alto rischio. Per questi sistemi il legislatore europeo ha predisposto un preciso schema di governance e suggerito tutele minime per coloro che sono stati danneggiati da sistemi di IA non conformi alle disposizioni di legge. D'altro canto, le direttive AILD e PLD avanzate dalla Commissione, innescherebbero un sistema di presunzioni qualora il fornitore convenuto non produca la documentazione obbligatoria o non dimostri la sicurezza del dispositivo. Come precedentemente illustrato, la violazione delle disposizioni dell'AI Act configura la colpa del convenuto ai sensi della AILD, mentre costituisce un difetto del sistema ai sensi della PLD. Pertanto, il quadro normativo proposto sembrerebbe declinare una responsabilità oggettiva a carico dei fornitori di sistemi di IA ad alto rischio che violino il quadro di governance europeo, poiché individuati quali soggetti più idonei a gestire il rischio da algoritmo, assieme al custode, al proprietario ed al provider.

Ebbene, come più volte evidenziato, la responsabilità oggettiva non promuove l'innovazione tecnologica né il suo sviluppo. Questo regime attribuisce al produttore la responsabilità di qualsiasi danno, senza però considerare gli eventuali sforzi e investimenti per garantire la messa in sicurezza del dispositivo. Pertanto, questa soluzione non rappresenta la scelta più efficiente per una tecnologia in continua evoluzione. D'altro canto, la ripartizione dei costi tra tutti i soggetti coinvolti nella

filiera produttiva, demandata all'azione di rivalsa tra fornitore e utilizzatore, *ex* art. 2055 c.c., «nella misura determinata dalla gravità della rispettiva colpa e dall'entità delle conseguenze che ne sono derivate»[316], garantisce un incentivo per lo sviluppo di dispositivi sicuri.

Senonché, il quadro delle criticità strutturali del sistema di responsabilità civile si rivela ancora più complesso. In primo luogo, i costi legali e amministrativi risultano considerevoli, con procedimenti lunghi e gravosi che comportano oneri economici rilevanti, sia per le parti interessate, che per il sistema giudiziario nel suo complesso. Generalmente, i risarcimenti vengono corrisposti in un'unica soluzione, il che spesso conduce a valutazioni poco precise delle spese effettivamente necessarie per affrontare e riparare le lesioni, con una conseguente sottostima dei danni effettivi. Inoltre, l'efficacia deterrente di tali misure risulta limitata, poiché progettisti e produttori non sono sufficientemente scoraggiati dalle sanzioni; a ciò si aggiunge l'intervento assicurativo, che ne diluisce ulteriormente il peso economico, riducendo pertanto l'impatto finanziario delle eventuali responsabilità[317]. Tuttavia, nonostante le limitazioni nell'efficacia deterrente delle sanzioni, la responsabilità civile continua a svolgere un ruolo cruciale nel promuovere comportamenti virtuosi tra gli individui, fungendo da incentivo per l'adozione di pratiche responsabili. In presenza di un regime di responsabilità oggettiva, le imprese sono incentivate a implementare rigorose misure di prevenzione del rischio, al fine di minimizzare il pericolo di incidenti e le conseguenti sanzioni. Tuttavia, imprese con risorse limitate si trovano spesso a dover equilibrare gli investimenti tra sicurezza e produzione, tendendo a privilegiare quest'ultima riducendo le misure di sicurezza preventive, specialmente in mercati altamente competitivi con una molteplicità di attori. La pressione concorrenziale, infatti, può indurre le imprese a comprimere i costi legati alla prevenzione, anche in presenza di un regime di responsabilità oggettiva, per favorire invece la vendita ad un prezzo più competitivo. Si rileva infatti che «strict liability and competition may involve higher risk when resources are scarce and must be

[316] Cit art. 2055 c.c., questa ricostruzione è stata suggerita da U. Salanitro, *Intelligenza Artificiale e responsabilità: la strategia della Commissione Europea*, in Rivista di diritto civile, 2020, p. 1272;
[317] J. Yoshikawa, *Sharing the Costs of Artificial Intelligence: Universal No-Fault Social Insurance for Personal Injuries*, in Vanderbilt Journal of Entertainment and Technology Law, 2020, p. 1172; Disponibile al: https://scholarship.law.vanderbilt.edu/jetlaw/vol21/iss4/8 ;

shared between production and safety. When hazard is abnormal and threaten both society and the firms viability due to excess potential repairs, capped strict liability associated with ex-ante control appears as a good regulatory instrument»[318]. Di conseguenza la letteratura ha rilevato che in presenza di attività d'impresa o commercio di prodotti ad alto rischio, sia per la società che per le imprese, l'emanazione di un regime di responsabilità oggettiva non spingerebbe le aziende ad accrescere la sicurezza dei propri prodotti, poiché esse troverebbero più conveniente concentrarsi sulla riduzione del prezzo del proprio prodotto. Pertanto, sarebbero necessari dei correttivi, come la previsione di un tetto massimo sull'ammontare dei risarcimenti e frequenti controlli preventivi. Tale sistema incentiverebbe le imprese a destinare maggiori risorse alla prevenzione, seppur possa comportare un incremento dei prezzi di mercato e una conseguente riduzione dell'offerta di beni.

A tali osservazioni si aggiunge l'impossibilità di allocare la responsabilità per i danni imprevedibili ed inevitabili, o per i danni arrecati dai sistemi di IA conformi alle norme e alle best practices. In questi casi non si rinverrebbe il presupposto del difetto, o della colpevolezza ai sensi della AILD, che permette l'accertamento della responsabilità. Pertanto, è stata proposta l'introduzione di un meccanismo di socializzazione dei costi attraverso la creazione di fondi finanziati da tutti gli attori di mercato, basati su un criterio di ripartizione equa dei costi; tuttavia, tale proposta non è stata recepita nei documenti ufficiali[319]. Infatti, la Risoluzione del Parlamento UE del 2017 evidenzia che «una possibile soluzione al problema della complessità dell'attribuzione della responsabilità per il danno causato da robot sempre più autonomi potrebbe essere un regime di assicurazione obbligatorio, come già avviene, per esempio, con le automobili»[320]. La Risoluzione inoltre continua suggerendo di adottare una soluzione analoga al «caso dell'assicurazione dei veicoli a motore, [dove]

[318] Cit. G. Mondello, *Strict liability, scarce generic input and duopoly competition*, in European Journal of Law and Economics (2022) 54:369–404, disponibile al link: https://doi.org/10.1007/s10657-022-09738-5;

[319] U. Salanitro, *Intelligenza Artificiale e responsabilità: la strategia della Commissione Europea*, Op. cit. p. 1272 che in merito alla proposta di fondi sponsorizzati afferma «L'idea, pur prospettata nella Risoluzione del Parlamento Europeo, non è stata valorizzata nel Report dell'Expert Group e non ha trovato spazio nel documento della Commissione»;

[320] Parlamento europeo, Norme di Diritto Civile sulla robotica - Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=IT ;

tale regime assicurativo [è stato] integrato da un fondo per garantire la possibilità di risarcire i danni in caso di assenza di copertura assicurativa»[321]. In effetti, come spiegherà meglio la Risoluzione del 2020, l'assicurazione fungerebbe da cuscinetto qualora il sistema di IA, non classificato ad alto rischio e quindi non ancora assicurato, dovesse arrecare danni. A mo' di ulteriore inconveniente, la Commissione UE ha evidenziato un insurance gap in presenza di un evento dove si materializzino danni collettivi superiori ai massimali risarcibili[322].

Pertanto, l'assicurazione non può assorbire qualsiasi conseguenza arrecata da un sistema di IA, o per mancanza di una condotta colposa a cui attribuire il danno, oppure per insufficiente copertura del rischio. In caso di danno senza illecito, l'ordinamento soccorre con l'istituto dell'indennizzo; ne sono un esempio gli indennizzi per danni da calamità naturali[323], per danni da balck-out[324] e per infortuni sul lavoro. Questi emolumenti sono garantiti da fondi sovvenzionati interamente dal settore pubblico o, come nell'ultimo caso, dal settore pubblico e dai privati datori di lavoro. La letteratura inoltre sottolinea la fungibilità di questo strumento di compensazione "sociale", già utilizzato in Italia per risarcire le vittime della strada, danneggiate da un conducente o un veicolo non identificati; ovvero da guidatori identificati ma sforniti di un'assicurazione e/o di un patrimonio sufficiente. La liquidazione e la valutazione del

[321] Parlamento europeo, Norme di Diritto Civile sulla robotica, cit. par. 58;
[322] Parlamento europeo, Civil liability regime for artificial intelligence - European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) sul punto « However, a "one-size-fits-all" solution is difficult to envisage and the insurance market will need time to adapt. The Commission should work closely with the insurance market to develop innovative insurance products that could close the insurance gap. In exceptional cases, such as an event incurring collective damages, in which the compensation significantly exceeds the maximum amounts set out in this Regulation, Member States should be encouraged to set up a special compensation fund, for a limited period of time, that addresses the specific needs of those cases» ;
[323] disposto dal DECRETO 11 agosto 2023, Criteri e modalita' per la concessione di aiuti a sostegno delle microimprese e piccole e medie imprese del settore agricolo colpite da calamita' naturali, Gazzetta ufficiale Serie Generale n.243 del 17-10-2023, disponibile al link: https://www.gazzettaufficiale.it/eli/id/2023/10/17/23A05685/sg ;
[324] Sono garantiti dall'ARERA, maggiori informazioni sono disponibili al link: https://www.arera.it/atlante-per-il-consumatore/elettricita/la-fornitura/interruzioni-del-servizio/che-cosa-sono-le-interruzioni-senza-preavviso-di-vasta-estensione#:~:text=In%20caso%20di%20interruzioni%20di,durata%20massima%20di%20interruzione%20pari ;

danno viene disposta dalle imprese assicurative incaricate da IVASS, autorità di settore[325].

Alla luce del sistema di indennizzo così strutturato, si propone l'istituzione di un sistema nominato Market Enterprise Responsibility (MER) per il risarcimento delle vittime di veicoli delf-driving. Tale fattispecie potrebbe essere facilmente inquadrata come danno senza illecito e senza colpevoli, qualora non si rinvengano difetti nell'automa. Questo fondo, finanziato direttamente dai produttori di auto driverless, garantirebbe la copertura dei danni causati dagli incidenti, assicurando un indennizzo ai soggetti coinvolti, inclusi passeggeri, pedoni e terzi, e promuovendo una ripartizione più equa dei costi associati agli incidenti provocati dai veicoli autonomi. In sostanza, il cd sistema MER consentirebbe una distribuzione economicamente sostenibile dei costi sociali e individuali scaturiti dai sistemi di IA, integrando i principi compensativi della responsabilità civile con il principio della market share liability. Questo meccanismo permetterebbe di coinvolgere direttamente i produttori nel bilanciamento tra vantaggi e svantaggi delle nuove tecnologie, imponendo un contributo obbligatorio ex ante. L'ammontare di tale contributo verrebbe stabilito in proporzione alla loro quota di mercato; ad esempio, imponendo a ogni produttore di contribuire in proporzione alla quota di veicoli commercializzati, e quindi in base al grado di rischio che ciascuna azienda introduce nella società[326]. Il contributo potrebbe essere imposto quale condizione di accesso al mercato, quale requisito di liceità dei prodotti venduti dal fornitore oppure sotto forma di imposta. Inoltre, la scelta di un criterio economico per ripartire le spese tra i produttori non aggraverebbe eccessivamente le barriere all'accesso del mercato per le PMI e start-up.

Bisogna inoltre considerare che l'adozione di un sistema no-fault con annesso fondo di compensazione risolverebbe le sopraccitate criticità del sistema di

[325] Il Fondo di Garanzia per le Vittime della Strada è stato istituito con legge n. 990 del 1969 (abrogata con l'entrata in vigore del Codice delle Assicurazioni Private) ed è operativo dal 12 giugno 1971. È amministrato, sotto la vigilanza del Ministero delle Imprese e del Made in Italy, dalla Consap con l'assistenza di un apposito Comitato presieduto dal Presidente della Società o, in sua vece, dall'Amministratore Delegato ed è composto da rappresentanti del Ministero delle Imprese e del Made in Italy, del Ministero dell'Economia e delle Finanze, di Consap, dell'Ivass, delle imprese di assicurazione e dei consumatori. Maggiori informazioni sulla procedura per la richiesta di risarcimento al link: https://www.consap.it/fondo-di-garanzia-per-le-vittime-della-strada/ ;

[326] E. Al Mureden, *Event data recorder e advanced driver assistance systems: la "spinta gentile" verso la mobilita` del futuro,* Op. cit. p. 405;

responsabilità civile. Infatti, in un sistema di no-fault si eradica alla base la necessità di un processo per accertare colpevole, colpa e nesso causale, riducendo significativamente i costi amministrativi e giudiziali. La procedura compensativa implicherebbe unicamente la dimostrazione del danno e la provenienza del prodotto, sollevando in questo modo il consumatore dalle preoccupazioni inerenti malfunzionamenti e garanzie relative ai sistemi di IA.

Tuttavia, questo approccio non considera alcuni profili delle dinamiche di mercato. Infatti, una siffatta modalità di ristoro non aumenterebbe la fiducia degli utenti nell'affidabilità di questa tecnologia. Al contrario, l'istituzione di un fondo di garanzia per danni costituirebbe un ulteriore sintomo della pericolosità dell'IA e dell'elevata frequenza di incidenti prevista durante l'uso di questi software. Di fatto, i fondi per le emergenze sopraelencati sono stati istituiti anche in ragione della frequenza degli eventi lesivi (es. terremoti, incidenti stradali e incidenti sul lavoro), oltre che in considerazione della volontà dello Stato di assicurare una compensazione. Sotto questo profilo un'ammissione di colpa dei fornitori per le prestazioni delle loro invenzioni potrebbe risultare più persuasiva della socializzazione del danno[327], che al contrario potrebbe essere percepita dal pubblico come una de-responsabilizzazione delle aziende tech. Inoltre, il criterio economico della quota di mercato non incentiva il miglioramento dei prodotti intelligenti e potrebbe invece favorire scelte imprenditoriali diverse.

Per questo motivo, il criterio di contribuzione economico dovrebbe essere integrato con un fattore aggiuntivo in grado di premiare gli investimenti destinati dall'azienda allo sviluppo di misure di sicurezza. Ad esempio, il contributo economico di ogni produttore al fondo di compensazione per le vittime di incidenti dovrebbe essere calcolato indicizzandolo rispetto ad un cd. "coefficiente di sicurezza" dei veicoli venduti[328]. Questo parametro fungerebbe da incentivo per produrre auto con migliori capacità di prevenire incidenti e di ridurre i danni.

[327] A. Albanese, *Mobilità del futuro e funzione preventiva della responsabilità civile*, Op. cit. p.
[328] E. Al Mureden, *Event data recorder e advanced driver assistance systems: la "spinta gentile" verso la mobilita` del futuro*, Op. cit. p. 406;

Tuttavia, stabilire concretamente la misura del 'coefficiente di sicurezza' presenta le stesse difficoltà incontrate nel tentativo di stabilire parametri tecnici di riferimento per identificare software difettosi e nel determinare le migliori pratiche tecnologiche per ciascuna categoria di essi[329]. Soltanto attraverso un costante aggiornamento delle best practices verrebbe assicurata la rivalutazione della sicurezza dei software in commercio, in funzione dei progressi tecnologici e della loro evoluzione nel tempo. Inoltre, l'elaborazione degli standard di valutazione dovrebbe necessariamente ottenere un consenso internazionale per garantire un'analisi uniforme e condivisa dei dati e delle misure relative al funzionamento dei sistemi.

2) La responsabilità civile e il suo impatto sul sistema assicurativo: il caso statunitense.

Una delle soluzioni ipotizzate dalla dottrina e dal Parlamento europeo nelle menzionate risoluzioni riguarda il trasferimento del rischio dai vari attori di mercato, quali fornitori, distributori, importatori e utilizzatori, alle compagne assicurative. Ciò avverrebbe tramite polizze assicurative che li manlevino dai danni arrecati a terzi a causa della loro attività. In alcune fattispecie il trasferimento del rischio è stato raggiunto attraverso uno schema di ridistribuzione dei costi, già adottato per altre fattispecie di attività pericolose, come pratiche mediche e circolazione dei veicoli. Lo stesso AI Act ha obbligato gli organismi di valutazione della conformità a stipulare a loro volta «un'adeguata assicurazione di responsabilità per le loro attività di valutazione della conformità»[330]. Pertanto, è stata ipotizzata anche per i fornitori di sistemi di IA, un'assicurazione obbligatoria per traslare il costo dei danni eventualmente addebitati.

Per valutare l'opportunità di ricorrere a questo strumento nel sistema di governance dell'IA e nella regolazione del mercato, sarebbe opportuno ripercorrere la storia della sua applicazione, al fine di anticipare e governare alcune delle possibili

[329] Descritta nel Cap. III, par. 3 di questa tesi;
[330] Cit. Art. 31, par 9, Regolamento UE n. 2024/1689;

conseguenze economico-sociali del ricorso alle assicurazioni della responsabilità civile verso terzi. Negli Stati Uniti, ad esempio, tra il 1984 e il 1986 il settore assicurativo subí un forte aumento dei premi e una riduzione della disponibilità a coprire i danni civili verso terzi derivanti da attività d'impresa. La crisi economica aveva determinato incrementi del prezzo delle polizze di centinaia di punti percentuali, nonché riduzioni drastiche dell'alea di rischio assicurata. Questo periodo storico è stato caratterizzato da significative fluttuazioni tra soft e hard market, alternando fasi di prezzi medi bassi a fasi di prezzi medi elevati, con una conseguente variazione nella disponibilità delle assicurazioni a coprire aree di rischio più ampie. Alcuni studiosi ritengono che l'hard market riscontrato nel 1986 fosse dovuto a delle iniziative legislative che avrebbero irrigidito il mercato attraverso la regolazione "flex-rate", adottata per contenere gli aumenti dei premi e limitare la possibilità delle assicurazioni di cancellare o non rinnovare le polizze[331]. Ebbene, le fluttuazioni del mercato assicurativo possono essere addebitate a diversi fattori, come un potenziale calo dei rendimenti degli investimenti per le compagnie assicurative, ovvero un aumento della frequenza e gravità delle perdite. L'effetto combinato di questi fattori potrebbe rappresentare una minaccia significativa per la stabilità economica del settore. Inoltre, l'introduzione di normative sfavorevoli, che limitano le prerogative delle assicurazioni o modificano il quadro regolatorio in modo restrittivo, metterebbe ulteriormente sotto pressione il modello di business tradizionale delle assicurazioni, aumentandone l'esposizione a rischi non calcolabili efficacemente[332].

Secondo la critica, un'altra plausibile causa della crisi statunitense '84-'86 può essere rinvenuta nella politica adottata per ridistribuire le esternalità negative delle attività pericolose esercitate nel mercato. Il legislatore è intervenuto, da un lato irrigidendo il contenuto dei contratti assicurativi, ad esempio imponendo un preavviso per il recesso dalla polizza, e, dall'altro, ampliando le fattispecie di responsabilità oggettiva connesse ad attività pericolose. Benché questa politica abbia cercato di non trasferire il costo di queste attività sui consumatori, risparmiatori e società, il risultato

[331] R. A. Winter, *The Liability Crisis and the Dynamics of Competitive Insurance Markets,* in *Yale Journal on Regulation*, 1988, p. 455;
[332] J. Rake, The hard market: Challenges and opportunities, in SwisseRe Corporation Solutions, disponibile al link: https://corporatesolutions.swissre.com/insights/knowledge/the-hard-market-challenges-and-opportunities.html ;

principale è stata una riduzione del numero di polizze disponibili sul mercato e un incremento del loro prezzo. In particolare, nella fase di hard market nel settore delle assicurazioni sulla responsabilità civile, le riforme legislative sulla materia hanno esasperato le criticità (fino a indurre le compagnie a ritirarsi da molti settori economici). Questi dati rivelano come un quadro normativo incerto sulla responsabilità civile incida direttamente sul livello di rischio che le assicurazioni sono chiamate a garantire. La letteratura dell'epoca evidenzia che «in the area of product liability, for example, there was a shift from traditional notions of fault-based liability to strict liability. Thus, as far back as 1963, sellers of unreasonably dangerous defective products were subjected to a theory of strict liability in *Greenman v. Yuba Power Products Inc*»[333]. Queste premesse avrebbero determinato negli anni '85-'86 un aumento del 70% dei premi delle polizze assicurative sul rischio imprenditoriale. Per di più l'hard market non solo potrebbe ridurre l'esposizione delle imprese assicurative, ma potrebbe innescare il rifiuto di assicurare determinati rischi[334]. La riduzione dell'alea del rischio è stata promossa anche da clausole di tipo "claims made", che impediscono a terzi ed assicurati di riscuotere il premio per danni occorsi dopo il periodo di validità della polizza.

Un'altra corrente della dottrina americana sostiene che la crisi sia emersa per effetto della scelta di politica del diritto, orientata a includere nello strumento risarcitorio la funzione compensativa e garantista delle situazioni sostanziali vietate, piuttosto che perseguire il solo effetto deterrente. Infatti, in quegli anni, si è assistito anche ad un incremento di condanne di liquidazione dei danni emesse nei confronti di più convenuti responsabili in solido per il danno arrecato. La responsabilità in solido risponde alla necessità di assicurare un risarcimento ai danneggiati, facendo appello alla logica del "deep pocket defendant". Questa tendenza ha comportato che «new classes of protected plaintiffs have been created in the tort law arena, increasing

[333] Cit. F. Achampong, *The Liability Insurance Capacity Crunch and Tort Liability Reform*, in Capital University Law Review 16, p. 622;
[334] R. A. Winter, *The Liability Crisis and the Dynamics of Competitive Insurance Markets*, Op. cit. p. 459 che menziona quali soggetti sono rimasti esclusi dal mercato assicurativo: «Many municipalities were unable to obtain insurance at prices they were willing to pay; about forty percent of day-care centers had their policies cancelled»;

the potential liability of insurers for damage awards against insured defendants»[335] . Allo stesso tempo è stato ampliato il novero di danni risarcibili, come ad esempio quello da perdita del rapporto parentale in caso di morte ingiusta[336]. Questo diverso e più "sociale" approccio delle cause di responsabilità civile avrebbe determinato una maggiore incertezza nell'ammontare dei risarcimenti che le compagnie assicurative avrebbero dovuto garantire, comportando quindi un aumento del rischio[337].

Oltre al quadro normativo e giurisprudenziale instabile, ulteriori elementi di crisi potrebbero essere addebitati alle perdite registrate dalle assicurazioni nel settore immobiliare nel 1970, che hanno spinto le imprese a prediligere categorie di rischio più redditizie, riducendo pertanto la disponibilità di polizza assicurative in alcuni settori economici.

Un ulteriore fattore di irrigidimento del mercato è stato riscontrato nella indisponibilità di servizi di riassicurazione, indispensabili per garantirne la stabilità. Il contratto di riassicurazione funge da elemento di flessibilità per il mercato assicurativo, permettendo alle compagnie di trasferire il rischio in eccesso al servizio di riassicurazione, riducendo così la loro esposizione complessiva.

Il collasso del sistema assicurativo nel settore della responsabilità civile verso terzi costituisce un problema di vera e propria politica pubblica, specialmente nel caso in cui venga meno la disponibilità di servizi assistenziali fondamentali come quelli offerti dal servizio sanitario nazionale. Infatti, si è rilevato come i medici avrebbero presto smesso di operare qualora non avessero potuto traslare il rischio professionale su un soggetto terzo, come l'assicurazione. Diversamente, il personale medico sarebbe costretto a esercitare la professione sotto la costante minaccia di azioni legali dirette al loro patrimonio personale. La crisi assicurativa degli anni '80 ha così investito anche il settore sanitario, che faticava a trovare compagnie che assicurassero professionisti e ospedali. Per tamponare il problema, sorsero compagnie assicurative

[335] Cit. F. Achampong, *The Liability Insurance Capacity Crunch and Tort Liability Reform*, Op. cit. p. 624 che inoltre riporta come i tribunali civili hanno indirizzato le loro condanne nei processi di risarcimento lo Stato per i danni lungo latenti derivati da test effettuati su dispositivi atomici oppure sono stati convenuti revisori legali dei conti per le erronee certificazioni di bilancio.
[336] Bullard v. Barne;
[337] M. J. Trebilcock, The Social Insurance-Deterrence Dilemma of Modern North American Tort Law: A Canadian Perspective on the Liability Insurance Crisis, 24 San Diego L. Rev., 1987, 929;

avallate o sponsorizzate da gruppi ospedalieri. Questa soluzione offriva diversi vantaggi rispetto ai contratti di assicurazione individuali, tra cui una migliore comunicazione tra le parti coinvolte. Infatti, gli assicuratori mantenevano un contatto diretto con i clienti principalmente durante le fasi di negoziazione e le revisioni periodiche dei premi. Questo tipo di rapporto assicurativo garantiva non solo una maggiore trasparenza e collaborazione tra le parti, ma anche una gestione del rischio più efficace. Grazie alla distribuzione del rischio su un ampio numero di assicurati, l'esposizione finanziaria per singolo partecipante veniva notevolmente ridotta. Inoltre, la possibilità di negoziare direttamente con organizzazioni di grandi dimensioni permetteva agli assicuratori di acquisire informazioni dettagliate sul cliente, sui suoi servizi e sui livelli di rischio associati a ciascun reparto. Questa conoscenza approfondita favoriva lo sviluppo di soluzioni assicurative più mirate e personalizzate, migliorando significativamente l'efficacia delle coperture[338].

Infine, un altro fattore che influisce sull'andamento del mercato assicurativo è rappresentato dalla sfortunata occorrenza di eventi naturali catastrofici, fallimenti aziendali o atti terroristici. Tali eventi hanno colpito il continente nordamericano in due occasioni significative nel 2001: l'11 settembre con l'attacco al World Trade Center di New York e il 2 dicembre con il crack di Enron. Ben prima del 2001 il settore delle assicurazioni aveva registrato perdite nel mercato immobiliare a causa di eventi naturali. Questo ha comportato un aumento del sessanta e ottanta per cento per le assicurazioni di immobili che si trovavano in regioni costiere (perché più soggette ad eventi metereologici avversi ed estremi), oppure edifici vicini ad obiettivi terroristici. Inoltre, in generale, è stata ridotta la disponibilità e il tasso di rischio coperto per danni arrecati da attacchi terroristici dopo l'11 settembre. Invece lo scandalo Enron ha avuto un impatto significativo sul mercato assicurativo nel settore delle operazioni finanziarie aziendali, determinando un innalzamento delle polizze

[338] M. Kendall, J. Haldi, Appendix: Report of the Secretary's Commission on Medical Malpractice, Washington, U.S. Dept. of Health, Education, and Welfare, p. 549 che si trova a rispondere proprio sulla disponibilità di copertura assicurativa per negligenza medica «concern of this study is whether the insurance industry will continue to make malpractice insurance available to qualified institutions and practitioners, i.e., is the malpractice insurance market collapsing, or is it likely to collapse? To summarize the conclusion of this study, for the foreseeable future insurance will almost certainly be available on a competitive basis from the private insurance industry, but the available sources and channels may undergo significant consolidation and change»;

D&O (direttori e dirigenti) ed E&O (errori e omissioni). La Enron, infatti, si era resa colpevole di pesanti falsi in bilancio, debitamente certificati dalla società di revisione Arthur Andersen. La bancarotta dichiarata dalla società ha sollevato il dubbio sulla regolare gestione della contabilità delle società quotate, e sull'effettivo pericolo di "cattura" tra controllore e controllati[339]. Pertanto, da allora, gli assicuratori sono obbligati a valutare attentamente la solidità finanziaria delle aziende che richiedono i loro servizi. Infine, si menziona anche una maggiore preoccupazione delle assicurazioni per i tassi di Technology Errors & Omission, che sono rapidamente aumentate a causa delle preoccupazioni sull'affidabilità delle nuove tecnologie quali oggetto di finanziamento; in particolare si temono malfunzionamenti totali o parziali degli algoritmi[340].

L'analisi storico-economica del contratto di assicurazione per la responsabilità civile ha evidenziato come il mercato delle assicurazioni si irrigidisca in un contesto di alto rischio di lesioni e istanze di risarcimento. L'alto rischio connesso ad un settore di mercato può essere determinato da diverse cause: l'offerta dell'assicurato di prestazioni connotate da maggior pericolo, come nel caso di una terapia particolarmente rischiosa; il sopraggiungere dell'evento imprevedibile e incerto con effetti particolarmente estesi, come un attacco terroristico o calamità naturale; infine, il commercio di prodotti pericolosi, come quelli finanziari o frutto di una tecnologia particolarmente innovativa. Oltre all'alea intrinseca del rischio assicurato, l'assicurazione per la responsabilità civile è inevitabilmente investita da qualsiasi riforma concerna il settore o gli standard e best practice utilizzate per valutare la condotta dell'assicurato. Pertanto, sebbene lo strumento dell'assicurazione per la responsabilità civile sposti agevolmente l'alea del rischio

[339] M. Novarini, *La truffa che sconvolse Wall Street (e non la cambiò per niente): i 20 anni del crac della Enron*, in Forbes, 2 dicembre 2021, disponibile al link: https://forbes.it/2021/12/02/enron-20-anni-truffa-rivelo-lato-oscuro-wall-street/ ;

[340] ALI-ABA Course of Study Materials: United States and International Litigation and Dispute Resolution: Current Developments and Their Impact on U.S. and European Companies, Insurers, and Lawyers, April 10-12, 2002, London, England. Philadelphia, American Law Institute - American Bar Association Committee on Continuing Professional Education, lo studio ha inoltre rilevato come ad aggravare la posizione dei società quotate e degli imprenditori in generale « A major problem for big businesses is the lack of available capacity in the surety market. At least one major recent bankruptcy has been attributed to the inability of the bankrupt to obtain surety. Brokers are finding it increasingly difficult to find surety and this fact in litigation. Chubb and other insurers have denied payment. They allege that bonds were obtained by misrepresentation. That performance had never been intended.»

dal fornitore/distributore/utilizzatore, essa deve essere ben bilanciata per evitare un'eccessiva estensione del rischio che porterebbe al collasso del mercato digitale e di quello assicurativo. Nel caso dei prodotti facenti uso di intelligenza artificiale, le compagnie assicurative potrebbero rifiutarsi di assicurare i sistemi ad alto rischio qualora il sistema di governance non abbia elaborato linee guida e standard per valutarne la sicurezza, né vi siano altri strumenti o procedure per valutare la condotta del fornitore. Infine, anche l'interpretazione dei tribunali incide direttamente sull'ammontare e sulla frequenza delle condanne di risarcimento; pertanto, la distribuzione dell'onere probatorio e la sua concreta applicazione impatteranno nella valutazione del rischio condotta dalle assicurazioni.

3) Caratteristiche principali dei sistemi di no-fault nelle diverse giurisdizioni

Stabilito che l'assicurazione non possa costituire il salvagente di ogni commercio di prodotti o attività pericolose, la distribuzione del rischio dovrà essere operata utilizzando diversi strumenti. L'istituto del fondo di compensazione, già ampiamente conosciuto in Italia, è stato sfruttato anche in altre giurisdizioni allo scopo di superare i difetti e le procedure di accertamento della responsabilità civile in determinati settori. L'analisi comparata dei fondi di compensazione adottati all'estero potrebbe suggerire modalità non tradizionali di gestione del rischio da algoritmo.

Ebbene, il primo caso di studio prende in esame il sistema di compensazione adottato in Danimarca ed oggi regolato dal Danish Patient Compensation Act per i danni scaturiti in particolari fattispecie di malpractice sanitaria[341]. La norma prevede

[341] Le quali sono previste nella Section 20 dello stesso atto, e impongono il risarcimento in quattro principali circostanze: quando uno specialista esperto, date le circostanze, avrebbe agito diversamente e la lesione sarebbe stata evitata; quando la lesione è causata da un guasto o malfunzionamento di attrezzature o strumenti utilizzati durante l'esame o il trattamento; quando una diversa tecnica o metodo di trattamento disponibile avrebbe potuto prevenire la lesione con la stessa efficacia nel trattamento della malattia; e quando il paziente contrae un'infezione o complicazioni più gravi di quanto normalmente previsto, considerando la gravità della lesione, la malattia e lo stato di salute del paziente. Per maggiori informazioni consultare il Consolidated Act of 28 august 2017, No. 1022, as last amended by the Act of 25 April 2018, No. 314 (Danish Patient Act) disponibile al link: https://eng.patienterstatningen.dk/entitled-to-compensation/laws-and-

che le vittime di malpractice sanitaria debbano presentare il loro reclamo al Danish Patient Compensation, un'associazione indipendente che decide in merito al diritto al risarcimento del paziente istante, in base al Danish Comepnsation Act. Il sistema di no-fault per la responsabilità sanitaria associato ad un fondo di garanzia pubblico per la liquidazione del danno è stato adottato nel 1992 con il Patient Insurance Act. In quegli anni il legislatore era stato chiamato a risolvere un gap di tutela registrato proprio in materia di responsabilità per danno alla salute, arrecato all'interno di strutture ospedaliere. In generale, i percettori dei servizi sanitari lamentavano una grave disparità tra la posizione giuridica del paziente e quella della struttura sanitaria, direttamente sovvenzionata dallo Stato. Tale disparità era ampiamente riscontrata dalle statistiche che, nei primi anni '90, registravano circa 38.000 incidenti, ma solo una minima parte si traduceva in azioni legali, dalle quali solo il 50% dei casi riusciva ad ottenere un risarcimento effettivo[342]. Pertanto, con tale riforma, il governo danese intendeva garantire un risarcimento alle vittime della prestazione sanitaria senza dover sostenere i ritardi e i costi del sistema processuale. Inoltre, eliminava l'onere del paziente di dimostrare la negligenza medica e il nesso causale, ulteriore fattore che spesso scoraggiava i pazienti dall'agire nei confronti della struttura sanitaria.

Il fondamento legale che stabilisce la responsabilità indiretta dell'ospedale applica il principio del *respondeat superior*, ossia l'istituto alla responsabilità dei padroni e committenti *ex* art. 2049 c.c. Questo principio identifica i soggetti potenzialmente responsabili nei proprietari e dirigenti degli ospedali per i danni causati dal personale medico operante presso la struttura. Tuttavia, l'ospedale non può esercitare il diritto di rivalsa nei confronti del dipendente responsabile, salvo il caso in cui la lesione sia stata provocata intenzionalmente. In questo modo, il PIA estende la responsabilità indiretta non solo agli atti negligenti, ma anche a quelli intenzionali, pur prevedendo la possibilità di rivalsa da parte dell'ospedale per i danni derivanti da condotte intenzionali del dipendente[343].

---

regulations#:~:text=The%20Danish%20Patient%20Compensation%20evaluates,or%20side%20effects%20to%20drugs. ;

[342] Per quanto concerne i dati attuali i report pubblici riportano soltanto l'ammontare totale delle liquidazioni il Danish Patient Compensation tra le statistiche dichiara che «In 2023 885 million Danish kroner was given as compensation to patients and their relatives»;

[343] Ann Ulrich, *An Evalution of the Danish No-Fault System for Compensating Medical Injuries*, in Annals of Health Law 3 (1994): 243-282

Il secondo caso di studio riguarda la gestione delle controversie relative ai sinistri stradali. Puerto Rico, insieme ad altri 12 Stati americani[344], ha optato per l'adozione di un no-fault system per liquidare i danni delle vittime della strada. Nei primi anni '70 Puerto Rico aveva una popolazione di quasi tre milioni di abitanti, distribuiti su un territorio, prevalentemente montuoso, di circa 3.000 miglia quadrate. All'epoca la situazione economica sull'isola era precaria, tuttavia si era verificato un aumento degli standard di vita della popolazione, sebbene il reddito pro-capite fosse inferiore alla media salariale degli Stati Uniti e un tasso di disoccupazione sei volte più elevato rispetto al continente.

In tale contesto gli incidenti automobilistici, e più in generale tutti i danni patiti dai veicoli sulla strada, divennero un problema di rilevanza pubblica a causa della loro frequenza. Il crescente utilizzo dell'automobile sull'isola, le infrastrutture stradali inadeguate a sostenere l'aumento del traffico, e l'alto costo dei veicoli avevano reso gravoso l'acquisto ed il mantenimento dell'auto[345]. Dall'altro lato, la popolazione non aveva scelta, doveva sopportare i costi complessivi della circolazione a causa della mancanza di mezzi pubblici alternativi all'auto. Pertanto, nonostante gli aumenti la domanda di auto non diminuiva e con esse gli incidenti. Quindi, con un tasso di disoccupazione che raggiungeva il 20% della forza lavoro e livelli di reddito piuttosto bassi, molti conducenti coinvolti in incidenti non erano in grado di adempiere le sentenze di condanna al pagamento dei danni. Le compagnie assicurative offrivano polizze estremamente costose a causa dell'elevato rischio di incidenti e danni ai veicoli; di conseguenza, la maggior parte delle auto in circolazione non erano assicurate. Il governo fu quindi chiamato a intervenire per correggere le criticità del sistema di responsabilità civile nella circolazione dei veicoli, il cui squilibrio minacciava anche la sostenibilità delle attività commerciali legate al trasporto di persone, come i servizi taxi.

[344] Florida, Hawaii, Kansas, Kentucky, Massachusetts, Michigan, Minnesota, New Jersey, New York, North, Dakota, Pennsylvania e Utah;

[345] H. B. Nachman, *Puerto Rico and Its No Fault System*, in International Society of Barristers Quarterly 5, 1970, p. 52-62 che sul punto riporta uno degli effetti di quest aumento dei prezzi «There is, to accomplish that end, an euphemistically-termed excise tax (in reality, an import duty) graduated both by the size and year of the vehicle. A new car, regardless of size, costs at least 50% more in Puerto Rico than in the States. Used smaller cars cost about a third more»;

Le soluzioni che si proponevano erano due: l'istituzione di un'assicurazione RCA obbligatoria oppure di un fondo di compensazione no-fault. All'esito delle valutazioni condotte nel 1968 venne emanato il "Social Protection Plan", per garantire il risarcimento di almeno di una parte degli incidenti che si verificavano nell'isola[346]. Oggi i risarcimenti vengono gestiti dall'Automobile Accident Compensation Administration, che in conformità con le disposizioni della Legge n. 138 del 26 giugno 1968, elargisce compensazioni per prestazioni medico-ospedaliere alle vittime di incidenti automobilistici.

In New Jersey, invece, il sistema di risoluzione giudiziale dei sinistri stradali affrontava una degenerazione diversa in quanto determinata dall'elevato costo raggiunto dalle polizze assicurative. Per riequilibrare un mercato fortemente sbilanciato, il governo è intervenuto istituendo un sistema di compensazione senza colpa. All'iniziativa si opponevano i legali e le imprese di assicurazione, contrari all'adozione di un sistema di responsabilità civile "no-fault", in quanto un simile modello avrebbe comportato una riduzione delle garanzie assicurative e un aumento dei costi delle polizze. Inoltre, si riteneva preminente l'interesse a preservare il legame tra responsabilità civile e individuo, piuttosto che la sicurezza di poter compensare la vittima. Tuttavia, la Corte Suprema ritenne che gli alti costi assicurativi stessero compromettendo il mercato, ed il legislatore intervenne con norme per monitorare e controllare gli importi delle polizze e con l'istituzione del Claim and Judgment Fund Law (UCJF). Questo fondo avrebbe riparato tutti i danni non compensati a causa della mancata identificazione del danneggiante o della sua insolvenza. L'istituto era finanziato in parte dallo Stato, in parte dai privati al momento dell'immatricolazione dell'auto; inoltre, lo Stato si riservava in ogni caso il diritto di rivalsa nei confronti dei danneggianti.

Tuttavia, nonostante il descritto meccanismo di regresso, l'onere economico risultava insostenibile per le casse dello Stato, per cui sono state chiamate le assicurazioni ad assorbire il rischio; offrendo polizze che assicuravano gli automobilisti dal danno, anche in assenza di un colpevole o di un patrimonio sul quale rivalersi. La stipulazione di questa polizza è stata successivamente resa obbligatoria

[346] Vedi Supra;

in New Jersey[347]. Oggi il sistema no-fault in New Jersey è regolato dall'Automobile Insurance Cost Reduction Act[348], in forza del quale i proprietari di veicoli sono obbligati a sottoscrivere una polizza assicurativa prima di procedere con la registrazione del veicolo. Il sistema assicurativo "no-fault" in New Jersey prevede tre tipologie di polizze obbligatorie: la protezione contro lesioni personali "PIP", che garantisce il rimborso delle spese mediche sostenute a causa di un incidente, un'assicurazione RCA per la copertura di danni patrimoniali ed infine un'assicurazione che garantisca ai conducenti il risarcimento anche qualora la controparte non sia assicurata o solvibile. Oltre a queste polizze sono offerti anche contratti standard di assicurazione sulla responsabilità civile, che implicano il diritto degli assicurati di agire nei confronti del soggetto responsabile[349]. Il cambiamento di rotta rispetto all'inziale Claim and Judgment Fund Law sembra essere stato motivato dall'insostenibilità economica dell'iniziativa che, nonostante sia sostenuta anche da tutti i proprietari di auto, non è riuscita a rispondere al carico risarcitorio richiesto. A parere della letteratura, il tasso di incidenti non sarebbe diminuito, in quanto l'«automobile insurance may create a moral hazard by diminishing the motivation for drivers to exercise due care»[350].

Il sistema di no-fault è stato adottato anche dalla Nuova Zelanda e dalla Svezia. Queste due legislazioni hanno istituito un sistema pubblico di risarcimento per danni da malpractice. In Svezia la riforma voleva rispondere alla complessità del sistema di responsabilità civile tradizionale, che rendeva difficile per i pazienti ottenere il risarcimento adeguato. Mentre in Nuova Zelanda il sistema di risarcimento era stato previsto per la liquidazione dei danni derivanti da infortuni sul lavoro[351]. Il sistema di compensazione previsto da questi ordinamenti è regolato dall'apparato statale amministrativo e dalle compagnie assicurative ed impone agli operatori sanitari

[347] M. K. Gajewski, *Automobile Insurance Reform in New Jersey: Could a Pure No-Fault System Provide a Final Solution*, Seton Hall Law Review 25, 1995): 1219-1255;
[348] Senate, No. 3, State Of New Jersey - 208th Legislature, The Automobile Insurance Cost Reduction Act, disponibile al link: https://pub.njleg.gov/bills/9899/s0500/3_i1.htm ;
[349] Law Office of Jeffrey S. and Hasson P. C., Understanding New Jersey No-Fault Laws, disponibile al link: https://www.hassonlawoffices.com/understanding-new-jersey-no-fault-laws/ ;
[350] M. K. Gajewski, *Automobile Insurance Reform in New Jersey: Could a Pure No-Fault System Provide a Final Solution*, Op. cit. p. 1254;
[351] T. Vandersteegen, W. Marneffe, I. Cleemput, L. Vereeck, *The impact of no-fault compensation on health care expenditures: An empirical study of OECD countries,*in Health Policy,2015, P. 368, ISSN 0168-8510, disponibile al link: https://doi.org/10.1016/j.healthpol.2014.09.010.

l'obbligo di stipulare una polizza per coprire i danni causati dalla loro attività. Il Patient Injury Act ha deferito il compito di valutare le richieste di risarcimento dei pazienti ad una commissione composta da medici consulenti. Le istanze dei pazienti lesi vengono sottoposte alla commissione, la quale assume una decisione sulla risarcibilità della lesione prendendo in considerazione il danno subito, il nesso di causa tra trattamento e danno, e la prevedibilità o evitabilità del pregiudizio. La commissione indaga anche la qualità dell'attività terapeutica espletata dal medico, valutandola secondo il criterio dello "specialista esperto". La valutazione pone a confronto le scelte cliniche adottate dal professionista nel caso di specie, con la condotta del miglior professionista sul campo. Dunque, il criterio dello "specialista più esperto" richiede al medico un più alto grado di expertise e diligenza nell'esecuzione della prestazione, che innalza per il professionista l'onere della prova sul proprio corretto adempimento. Infine, la richiesta può essere accolta anche se si dimostra che un trattamento alternativo avrebbe evitato il danno o che le lesioni siano risultate più gravi del previsto[352].

Il processo di valutazione e indagine sopraccitato mira a selezionare gli episodi di malpractice da risarcire, al fine di contenere la spesa pubblica e di evitare l'emergere di comportamenti opportunistici del personale sanitario, che, consapevole della tasca profonda e sicura del fondo, potrebbe esercitare minore cura nell'esecuzione della prestazione. Un filtro di diversa natura è invece stato adottato dal sistema no-fault svedese, che tramite il Patient Insurance Compensation Fund, modula la tutela offerta ai pazienti. Questo sistema prevede delle soglie minime di infortunio, ossia un livello minimo di gravità di una lesione necessario per presentare richiesta di risarcimento. Tale livello è stabilito specificando l'importo minimo di denaro richiesto per la compensazione[353], escludendo così le lesioni bagatellari dal risarcimento. Parallelamente è fissato un massimale per ciascuna istanza di risarcimento, proporzionato al numero di individui coinvolti nell'incidente. Infine, un altro criterio usato per delimitare l'esposizione del fondo è la regola dell'evitabilità, che riconosce

[352] C. Scarpellino, Responsabilità nell'e-health, Op. cit. p. 197;

[353] che all'epoca D. M. Studdert; E. J. Thomas; B. I.W. Zbar; J.P. Newhouse, *Can the United States Afford a No-Fault System of Compensation for Medical Injury*, in Law and Contemporary Problems, 1997,p. 1-34 precisa che «In 1997, the base sum was 36,300 SEK ($US 5,220), hence a deductible of approximately 1,820 SEK ($US 238) was levied upon every injury compensated by the Fund in that year, effectively removing minor injuries from the ambit of the scheme»;

diritto al risarcimento se il danno subito avrebbe potuto essere evitato utilizzando la normale diligenza e disponendo di adeguati attrezzi e infrastrutture[354]. Dall'altro lato, la liberazione del personale sanitario dalla minaccia di cause civili - si auspica - inneschi un atteggiamento virtuoso dei medici, incentivandoli a dichiarare i propri errori e a collaborare attivamente con i pazienti per completare i moduli di reclamo per malpractice.

I sistemi di no-fault o i fondi di compensazione pubblici per il risarcimento dei danni arrecati da un colpevole non identificabile sono stati strutturati, dalle giurisdizioni menzionate, con caratteristiche e modalità diverse a seconda del particolare scopo perseguito. Tuttavia, il profilo comune di tutte queste esperienze consiste proprio in un gap di tutela del sistema di responsabilità civile che non riusciva fisiologicamente a raggiungere la propria *raison d'etre*, compensando del pregiudizio patito tutti gli aventi diritto. Come diffusamente illustrato in questo paragrafo, in Danimarca i pazienti difficilmente ottenevano il risarcimento per danni da malpractice. Puerto Rico affrontava la carenza strutturale delle strade, il numero di automobili in circolazione, e soprattutto, il livello di povertà della popolazione; condizioni che avevano determinato un alto tasso di incidenti automobilistici e danni ai veicoli. Invece, in New Jersey il costo dell'assicurazione RCA aveva raggiunto costi troppo elevati. Infine, nei paesi scandinavi il sistema no fault è stato adottato per superare le criticità del tradizionale sistema di responsabilità civile.

Ebbene, ciascuna esperienza mostra strumenti diversi per modulare l'istituto in base alle esigenze del caso. Il fondo di compensazione pubblico potrebbe essere finanziato dal solo soggetto pubblico o da soggetti pubblici e privati. Il rischio da garantire potrebbe essere delimitato ponendo una soglia di gravità per le lesioni oggetto della richiesta e imponendo massimali. Inoltre, con l'applicazione del principio di evitabilità si può limitare la validità delle istanze ai pregiudizi che il sistema sanitario avrebbe concretamente potuto scongiurare, coincidendo quindi con la fattispecie di malpractice. Un fondo di compensazione costruito predisponendo

[354] T. Vandersteegen, W. Marneffe, I. Cleemput, L. Vereeck, *The impact of no-fault compensation on health care expenditures: An empirical study of OECD countries*, Op. cit. ;

queste condizioni potrebbe non aggravare eccessivamente le casse di uno stato[355]. Il sistema è stato spesso utilizzato anche in Italia per la compensazione di danni arrecati nell'esercizio di determinate attività pericolose, ritenute indispensabili al vivere sociale, come nel caso dell'indennizzo per danni risultanti dalla somministrazione di un vaccino[356] oppure il Fondo di Garanzia per le vittime della strada (FGVS)[357]. La *ratio* di questi fondi pubblici risiede nella accettazione del rischio implicato da una attività a fronte dei benefici che ne trae, e nella consapevolezza di non poter lasciare che una percentuale della popolazione ne paghi lo scotto. In ragione di questa valutazione, lo Stato si assume dunque l'onere di risarcire il danno da questi patito, collettivizzando la perdita.

Alla luce dell'analisi esposta, la prospettiva di utilizzare un fondo di compensazione per rispondere alle istanze di risarcimento per danni da algoritmo, potrebbe costituire la soluzione totale o parziale del liability gap causato dai sistemi di IA. Il sistema costituirebbe una risposta parziale qualora accogliesse solo in casi in cui non è stato possibile individuare un colpevole. Invece un sistema di no-fault puro raggiungerebbe qualsiasi fattispecie di danno, gestendo tutte le istanze a livello amministrativo privato per eliminare le esigenze processuali della responsabilità extracontrattuale, riducendo così i costi connessi all'utilizzo dei sistemi di IA. Questa soluzione potrebbe raccogliere anche il favore degli stakeholders del settore, che si libererebbero dell'incertezza legata alla liquidazione dei danni e spese legali in cambio di una forma di compensazione privata al fondo di garanzia. Questa soluzione eviterebbe un eccessivo innalzamento del prezzo di questi prodotti, che invece scaturirebbe qualora si applicasse un regime di responsabilità tradizionale a carico dei produttori imponendo al contempo un'assicurazione obbligatoria: opzione capace di

[355] Questa affermazione è stata rivolta in particolare al caso degli Stati Uniti da C. Vincent, *Compensation as a duty of care: the case for "no fault"*, in *BMJ Quality & Safety*, 2003, pp .240-241 che al riguardo sostiene «Studies by Brennan and colleagues suggest that implementing the Swedish system of compensation, which employs a criterion of avoidability of injury as grounds for compensation, would not lead to greatly increased overall costs in the United States» ;

[356] Ministero della Salute, Indennizzi per i danneggiati in modo irreversibile da vaccinazioni, trasfusioni e somministrazione di emoderivati infetti (Legge 210/92), dove fa riferimento alla «Legge 25 febbraio 1992 , n. 210, riconosce un indennizzo ai soggetti danneggiati in modo irreversibile da vaccinazioni, trasfusioni e somministrazione di emoderivati infetti, normativa disponibile sul sito: https://www.salute.gov.it/portale/indennizzo/dettaglioContenutiIndennizzo.jsp?lingua=italiano&id=921&area=indennizzo&menu=vuoto ;

[357] Leggi inerenti la sua istituzione e organizzazione disponibili al link: https://www.consap.it/fondo-di-garanzia-per-le-vittime-della-strada/normativa/ ;

determinare un crollo del mercato assicurativo, come già avvenuto sul finire degli anni ’90 negli Stati Uniti.

Le compagnie assicurative non sono i soggetti più adatti per bilanciare l'interesse pubblico nel garantire il risarcimento degli interessi sociali. Il rischio troppo alto è dovuto all’incalcolabilità *ex ante* dei danni di scala che potrebbero scaturire da un algoritmo ad alto rischio, o a rischio minimo ma operante in settori sensibili. Pertanto, l’innalzamento del costo delle polizze determinerebbe un diretto e proporzionato aumento del prezzo dei software, aumento peraltro circoscritto al solo mercato europeo. In conclusione, dall’analisi esposta emerge chiaramente che la tutela dei diritti rappresenta un aspetto cruciale nella governance dell’IA. Tuttavia, è necessario trovare un equilibrio che contemperi l’interesse economico e competitivo del mercato europeo, il quale attualmente sembra aver perso terreno nella corsa all’IA; come rivela il numero di brevetti rilasciati per invenzioni europee negli ultimi 10 anni.

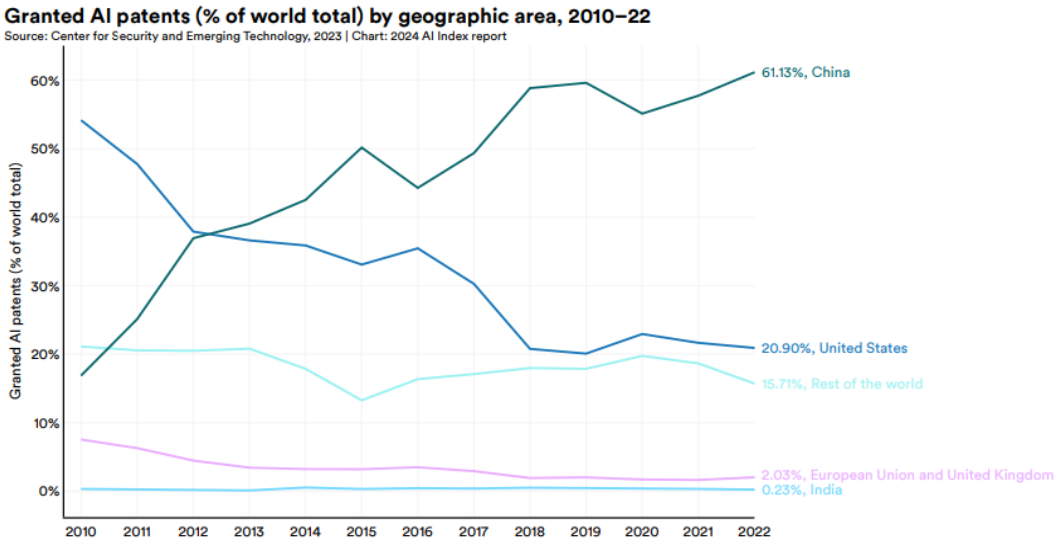

Figura 6. Artificial Intelligence Index Report 2024

A mo' di conclusione

Il sistema di governance dell'Intelligenza Artificiale proposto dall'AI Act si articola in un insieme di obblighi e requisiti che, nel loro complesso, garantiscono un equilibrio tra i potenziali rischi e i benefici del singolo software. Il bilanciamento viene assicurato da obbligazioni e requisiti di gravità crescente, parametrate al rischio implicato da ciascun sistema di IA. Il quadro di contabilizzazione e controllo contempla strumenti di compliance *ex ante,* quali misure di sicurezza e valutazione di impatto sui diritti fondamentali; mentre altri intervengono *ex-post*, quindi soltanto dopo che il pericolo si sia verificato. Ebbene, in questo quadro il regime di responsabilità rappresenta solo uno degli strumenti giuridici atti a compensare il danno da algoritmo; infatti, la letteratura propone l'adozione di vari sistemi di compensazione, sia indipendenti sia combinati tra loro.

Ad ogni modo, la responsabilità civile e l'allocazione dei danni hanno un impatto politico e sociale[358], che supera la dimensione bilaterale della controversia, influenzando le dinamiche di mercato e i suoi equilibri. Nel caso di studio, il rischio legato allo sviluppo, produzione e commercio dell'IA è determinato dal prodotto, a causa del suo meccanismo di funzionamento opaco, autonomo e delicato. Nonostante questo, i software di IA si propongono, nella maggior parte dei casi, quali utili assistenti in qualsiasi attività di lavoro o di studio; sono infatti in grado di moltiplicare la produttività di un lavoratore[359]. Le statistiche rivelano, quindi, che le imprese sarebbero intenzionate a sperimentare la nuova tecnologia ma appaiono ancora titubanti a causa dalle conseguenze legali incerte e di un quadro normativo non ancora chiaro.

---

[358] N. Muftic, *Understanding the Risks of Artificial Intelligence as a Precondition for Sound Liability Regulation,* Op. cit. p. 102;

[359] S. Arcudi, *AI utile per aumentare la produttività, ma non tutti i dipendenti sono pronti alla trasformazione*, in Sole 24 ore, 11 marzo 2024, il quale riporta che «secondo gli intervistati [oltre 12.000 business executive] il rapido sviluppo delle capacità dell'Ai generativa fa sperare un aumento della produttività della forza lavoro e il 40% degli executive prevede incrementi di produttività di oltre il 30% grazie all'Ai. Tuttavia, tre intervistati su cinque (58%) ritengono che la tecnologia stia avanzando a un ritmo più rapido rispetto alla capacità stessa dell'azienda di riqualificare il personale e meno della metà (47%) pensa che l'azienda sarà in grado di far fronte alla domanda quest'anno basandosi sul talent model esistente.» ;

Un'altra caratteristica che rende incerto l'utilizzo del tradizionale regime di responsabilità civile è la molteplicità di potenziali convenuti. La catena del valore dell'IA, molto più che per qualsiasi altro prodotto, coinvolge imprenditori, professionisti e accademici di diverse regioni e giurisdizioni. Peraltro, anche le infrastrutture (centri per la connettività della rete, per la conservazione dei dati, server con capacità di elaborazione) necessarie per ciascuna fase di produzione potrebbero essere collocate in giurisdizioni differenti. Pertanto, il coinvolgimento di tutti questi attori costituirebbe ragione di ulteriori ritardi e spese processuali.

In questa ottica va commentato il pacchetto IA composto oggi dal recente Regolamento UE 1689/2024 e dalle proposte direttive PLD e AILD. Le due direttive costituiscono la risposta dell'Unione Europea al gap di responsabilità che si verifica nell'imputazione dei danni da algoritmo. La soluzione adottata sembra quella di offrire ai consumatori entrambi le voci di responsabilità: oggettiva e per colpa. La PLD, come l'attuale Dir. 85/374/CEE, prevede la responsabilità oggettiva del produttore che abbia messo in commercio un prodotto difettoso. La AILD, invece, definisce la fattispecie sulla colpa del fornitore facendola coincidere con «la non conformità a un obbligo di diligenza, a norma del diritto dell'Unione o nazionale»[360]. Questo passaggio evidenzia il legame tra la responsabilità civile e il sistema di governance: infatti la prima costituisce uno degli strumenti di enforcement delle obbligazioni e dei requisiti previsti dall'AI Act. Nello specifico il giudice dovrà obbligatoriamente presumere la non conformità del software ai requisiti europei, qualora il convenuto non abbia prodotto la documentazione prescritta ai sensi dell'AI Act. Tuttavia, in pratica il meccanismo presuntivo prestabilito potrebbe non facilitare l'attore danneggiato, in quanto al fornitore basterebbe esibire una documentazione che attesti il rispetto di requisiti tecnici (come l'allenamento su un set di dati correttamente addestrati, gli obblighi di trasparenza, un sistema di supervisione umana etc..) per evitare l'attivazione delle presunzioni previste. Ecco che allora la combinazione di strumenti dell'AILD e della PLD potrebbe concludersi in un nulla di fatto, ed impedire la liquidazione del danno perché risultano rispettati i requisiti di forma;

[360] Cit. Commissione EU, Proposta di Direttiva Del Parlamento Europeo E Del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale), disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52022PC0496 ;

circostanza che peraltro impedirebbe ulteriori indagini, salvo che l'attore non riesca a provare l'inadeguatezza delle misure adottate.

Qualora si affermi una prassi di questo tipo, la PLD risulterebbe più efficacie della AILD nel garantire un risarcimento alla parte lesa. La direttiva contempla infatti più elementi per stabilire il difetto del prodotto, sganciandosi in questo modo dall'AI Act e dal suo puntuale quadro di governance. L'onere della prova è più elastico nella PLD, che considera il prodotto difettoso qualora «non offra la sicurezza che il grande pubblico può legittimamente attendersi»[361].

Da queste considerazioni consegue un risultato per certi versi paradossale, dove il consumatore danneggiato da un prodotto acquistato riceve una tutela maggiore rispetto a un individuo cui siano stati negati i diritti fondamentali. Quanto dire che il danno arrecato a piatti e bicchieri da una lavastoviglie intelligente implicherà la responsabilità oggettiva del fornitore, mentre, nel caso in cui la medesima persona venisse discriminata durante lo screening dei curriculum per una posizione lavorativa a causa di un bias razziale, o ricevesse condizioni per un mutuo particolarmente gravose, a causa di un debito universitario o del ritardo nel pagamento di due rate del computer, la responsabilità passerebbe per il più arduo sentiero della prova di una qualche imputabilità colposa[362]. Quindi, l'applicazione delle due direttive, così strutturate, potrebbe non comporre il vuoto di tutela evidenziato. Tanto più che si dovrebbe anche provare l'ingiustizia del danno patito per una decisione automatizzata; circostanza che potrebbe essere dimostrata soltanto provando il bias di funzionamento, reso oscuro dalla black-box, oppure argomentando che un individuo deputato alla stessa mansione avrebbe preso una decisione differente, basandosi sugli stessi dati.

Il timore che la AILD si dimostri inefficacie appare ancora più plausibile se si considera che, le concrete modalità di adempimento degli obblighi e dei requisiti dell'AI Act sono lasciate alla libera determinazione dell'obbligato. Di fatto, il Regolamento 1689/2024 fa appello nuovamente al middle-out approach per regolare le nuove tecnologie. Questa strategia normativa, basata sul principio di accountability e di

[361] Cit. Art. 6, par. 1., Proposta di Direttiva Del Parlamento Europeo E Del Consiglio sulla responsabilità per danno da prodotti difettosi, Bruxelles, 28.9.2022 COM(2022) 495 final;
[362] M. Malcheva, *Liability and Artificial Intelligence*, 2022, www.lex.bg, Available at SSRN: https://ssrn.com/abstract=4400410 or http://dx.doi.org/10.2139/ssrn.4400410;

"compliance"[363] by design e by default, impone al produttore finale del sistema di IA di gestire e monitorare la propria tecnologia, nonché di identificare i rischi e le possibili responsabilità connesse al suo funzionamento. Il fornitore dovrebbe dare conto di tali valutazioni, e dell'adeguatezza delle sue misure, in una valutazione di impatto. Tuttavia, è ben possibile che alcuni rischi del software non possano essere individuati nella fase di ideazione e sviluppo, ma soltanto in una successiva fase applicativa. Il contesto di utilizzo infatti è indispensabile per testare la tecnologia, osservando se istruzioni e informativa predisposte siano sufficienti a garantirne un funzionamento sicuro. Inoltre, è importante rilevare la relazione con gli ambienti circostanti per valutare la reazione dell'automa alle circostanze di vita reale. Oltre all'adozione di misure di sicurezza per rispettare requisiti e obbligazioni (es. algoritmi capaci di individuare il rischio di pregiudizi discriminatori e strumenti open-source progettati per garantire equità e accuratezza nei risultati prodotti dai sistemi automatizzati, software per migliorare la trasparenza del device), il produttore potrà mettere in campo protocolli e procedure per garantire lo sviluppo di sistemi sicuri (come guide lines, best practices, sistemi di gestione dei progetti per tenere traccia delle attività espletate da programmatori e ingegneri nello sviluppo del sistema e predisporre appositi codici di condotta per queste figure[364]) e strumenti educativi diretti alla formazione continua del proprio personale e ad informare il pubblico sui pericoli del sistema di IA e sulle precauzioni necessarie.

Allo stesso tempo l'apparato pubblico deve essere pronto a valutare i sistemi per ammetterli al mercato europeo. Spetterà alle autorità di vigilanza del mercato e agli organismi di valutazione accreditati emettere le certificazioni di conformità per attestare la liceità e sicurezza del sistema. Entrambi le categorie di enti devono possedere le competenze necessarie per valutare il software ed accertarne la conformità alle norme, avuto riguardo alle specificità presentate dal sistema e dal suo contesto di applicazione. Inoltre, per incentivare la costruzione di un ambiente AI friendly, l'intero sistema amministrativo e burocratico, composto da funzionari, giudici, avvocati, dovranno essere

[363] Sostituzione della parola "privacy" del principio disposto dal GDPR "privacy by design and by default" con "compliance";
[364] OCSE, Tools for trustworthy ai a framework to compare implementation tools for trustworthy ai systems OECD digital economy papers, giugno 2021, disponibile al link: https://www.oecd-ilibrary.org/fr/science-and-technology/tools-for-trustworthy-ai_008232ec-en ;

preparati sulle opportunità della nuova tecnologia, per essere pronti a gestire documenti, istanze e procedure svolte tramite l'assistenza di un'IA[365].

Infatti, l'acquisizione delle più moderne tecnologie è inutile se il contesto di riferimento non ha gli strumenti per sfruttarne l'operato. Sovente, tuttavia, le risorse a disposizione non permettono di raggiungere questo risultato, si registra una fame insoddisfatta di informazioni sugli algoritmi, sulle logiche di funzionamento e sui data base usati per allenarli; specialmente nel campo dell'IA generativa e dei foundation models. L'asimmetria informativa tra governi e big tech è uno dei nodi critici nella definizione di un quadro di governance soprattutto in Europa, che subisce passivamente la concorrenza di Stati Uniti e Cina nella corsa all'IA. Questa condizione è aggravata dalla distanza tra i maggiori operatori del settore e le pubbliche amministrazioni europee, che vede le maggiori Big Tech stabilite in una diversa giurisdizione. In questa prospettiva, gli obblighi relativi alla documentazione tecnica e alla valutazione di impatto, previsti nell'AI Act, dovrebbero più correttamente essere interpretati come un'effettiva richiesta di dati da parte delle istituzioni europee.

Dunque, alla luce dello stato dell'arte, la ricerca si presenta con un quadro di governance incompleto e ancora incerto, in attesa dell'implementazione di standard, la cui emanazione è attesa nei prossimi anni grazie ad una procedura attivata su istanza della Commissione europea e rivolta agli European Standardisation Organisations (ESO). L'obiettivo è rappresentato dall'elaborazione di standard tecnici che permettano di adempiere correttamente agli obblighi e requisiti dell'AI Act, in questo modo gli operatori potranno disporre di linee guida da seguire, mentre le autorità potranno usarli come parametri di giudizio per stabilire la sicurezza del software. Un corredo di standard tecnici adeguati costituisce presupposto indispensabile per una governance effettiva, in quanto l'assenza di parametri di valutazione non rende l'attività del provider effettivamente accountable/liable.

[365] Microsoft, *Governing AI: A Blueprint for the Future*, 2023, in merito riporta l'esempio «judges needed to decide cases that started to turn, in part, on evidence about or involving PC software and hardware» disponibile al link: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw ;

Dunque, proprio perché il quadro di governance per l'IA è in costante evoluzione che appare urgente fornire un sistema di responsabilità civile che risarcisca i danni, senza pregiudicare lo sviluppo e il commercio nel mercato digitale. Quindi, il sistema proposto dalla Commissione europea non elimina il gap di responsabilità oggetto del presente studio. Il vuoto di tutela persiste a causa della prospettiva antropocentrica che informa il cd. "pacchetto IA", riflettendo l'idea che soltanto l'individuo è soggetto capace di commettere, prevenire, ripristinare, riparare. Questo approccio determina inevitabilmente il gap, poiché legittima soltanto le richieste di risarcimento danni causati dalla negligenza che si determina con la violazione delle prescrizioni dell'AI Act. Pertanto, acclarata la possibilità che il danno da algoritmo si verifichi anche in assenza di colpa o di un effettivo illecito, urge adottare un sistema di responsabilità civile senza colpa, che in modo indipendente o combinato con altri strumenti soccorra a risarcire i danni arrecati dai sistemi di IA.

A tal fine questo studio suggerisce tre ipotetici regimi:

- Responsabilità presunta: il primo sistema suggerisce l'applicazione dell'art. 2050 c.c. sulla responsabilità per attività pericolose, beneficiando della disclosure of evidence e delle presunzioni previste nella proposta AILD. L'onere probatorio determinato dalla presunzione dell'art. 2050 c.c. permette di spostare il rischio della mancata prova sul produttore; cosicché, nel caso in cui rimanga ignota la causa del danno, essa venga comunque imputata al convenuto;
- Responsabilità oggettiva: questo strumento permette di allocare la responsabilità sul soggetto ritenuto dall'ordinamento più vicino allo sviluppo del prodotto pericoloso, e che pertanto potrebbe meglio rispondere all'effetto deterrente della minaccia risarcitoria;
- Sistema di no-fault: questo istituto permette di collettivizzare i costi della tecnologia. Il sistema si avvale di un fondo di garanzia che può essere finanziato congiuntamente dagli operatori di mercato e dal settore pubblico.

Sebbene tutte e tre le proposte soddisfino lo scopo di questa ricerca nel delineare soluzioni legali per eliminare il gap di responsabilità, è bene considerare il differente impatto economico-sociale di ciascuna ipotesi. Dunque, sintetizzando all'estremo i rilievi di analisi economica disseminati nel lavoro, è dato opinare che il regime di responsabilità presunta, integrato dalla disclosure of evidence della AILD, sia in grado di rispondere all'asimmetria informativa tra le parti e di allocare il rischio di danno arrecato senza colpa. L'ulteriore vantaggio di questa traiettoria consiste nella preclusione dell'eccezione del rischio da sviluppo. Tuttavia, essa rimette all'attore la non facile problematica di individuare il convenuto responsabile (tra programmatore, addestratore, fornitore, distributore e utilizzatore).

Il regime di responsabilità oggettiva, invece, garantisce la copertura totale di tutti i danni da algoritmo; tuttavia, per non gravare eccessivamente sul produttore, è normalmente assistito da un regime di assicurazione obbligatoria. Questa soluzione appare, però, poco efficiente sotto due punti vista: *in primis,* non incentiva i fornitori ad investire sulla sicurezza dei prodotti, e poi innesca preoccupazioni in ordine al collasso del sistema assicurativo sotto la pressione delle cause risarcitorie e della difficile determinazione dell'alea del rischio implicato da questi sistemi.

Infine, il sistema no-fault costituisce uno strumento di diretto intervento pubblico, poiché un organo amministrativo si occupa di recepire le istanze e di accertare e liquidare il danno. L'efficienza di questa soluzione è legata alla struttura del fondo di garanzia che, poggiando su un sistema di contribuzione obbligatoria degli operatori di IA, può attivare un meccanismo di tassazione e incentivi atto a rendere il contributo economico proporzionale al coefficiente di sicurezza e agli investimenti in ricerca e sviluppo.

In conclusione, il ruolo della responsabilità civile nel sistema di governance dell'IA può essere sfruttato per raggiungere un equilibrio virtuoso tra regolazione e tecnologia. Tutte le soluzioni proposte possono essere modulate con strumenti tecnici, procedurali ed informativi al fine di massimizzare i benefici connessi all'IA, sia per l'individuo che per la collettività.

Bibliografia

Articoli

Achampong Francis. *The Liability Insurance Capacity Crunch and Tort Liability Reform*. Capital University Law Review 16, 1991, p. 622.

Al Mureden Enrico, *Event Data Recorder e advanced driver assistance systems: la "spinta gentile" verso la mobilita 'del futuro*, in Contratto e Impresa, 2022, p. 390;

Albanese Antonio. *Mobilità del Futuro e Funzione Preventiva della Responsabilità Civile*. Europa e Diritto Privato, 2023, pag. 444.

Allen J. Hilary. *Sandbox Boundaries.* Vanderbilt Journal of Entertainment & Technology Law, 2020, p. 300.
https://scholarship.law.vanderbilt.edu/jetlaw/vol22/iss2/3/

Arezzo Emenuela. *Protezione del Segreto e Tutela del Software: Convergenze, Sovrapposizioni, Conflitti*. Il Diritto Industriale, 2018, 145.
https://research.unite.it/handle/11575/103463

Arnaudo Luca, Pardolesi Roberto, *Ecce robot. Sulla responsabilità dei sistemi adulti di intelligenza artificiale*. Danno e Responsabilità, 2023, p. 409.

Astone Antonia. *Autodeterminazione nei Dati e Sistemi A.I.*. In Comitato e Impresa, 2022 p. 434.

Atlante per il Consumatore. *Interruzioni di Servizio*. 2023.
https://www.arera.it/atlante-per-il-consumatore/elettricita/la-fornitura/interruzioni-del-servizio/che-cosa-sono-le-interruzioni-senza-preavviso-di-vasta-estensione

Banca d'Italia. *Regulatory Sandbox*. 2023.
https://www.bancaditalia.it/focus/sandbox/index.html?com.dotmarketing.htmlpage.language=1&dotcache=refresh&dotcache=refresh

Bank of Englad. *Digital Securities Sandbox.* 2024.
https://www.bankofengland.co.uk/paper/2024/cp/digital-securities-sandbox-joint-bank-of-england-and-fca-consultation-paper

Beckers Anna, Teubner Gunther. *Three Liability Regimes for Artificial Intelligence*. Bloomsbury Publishing, 2022, p. 139. https://www.bloomsbury.com/us/three-liability-regimes-for-artificial-intelligence-9781509949335/

Bellisario Elena. *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle Proposte della Commissione*. Danno e responsabilità, 2023, p. 153. https://www.altalex.com/documents/2023/05/25/pacchetto-europeo-responsabilita-danni-da-prodotti-intelligenza-artificiale-riflessioni-proposte-commissione

Bertolini Andrea. *Artificial Intelligence Does Not Exist! Defying the Technology-Neutrality Narrative in the Regulation of Civili Liability for Advanced Technologies.* Europa e Diritto Privato, 2022, p. 384.

Bieber Christy, Ramirez Adam. *What Is Respondeat Superior?* Forbes Advisor. 2023. https://www.forbes.com/advisor/legal/personal-injury/respondeat-superior/

Boeri Elisa, *Self-driving cars e profili assicurativi,* in Arch. giur. circ. ass. e resp., 2023, p.11;

Bruyne Jan & Gool, Elias & Gils Thomas. *Tort Law and Damage Caused by AI Systems*. 2021. 10.1017/9781839701047.015. https://www.researchgate.net/publication/351875982_Tort_Law_and_Damage_Caused_by_AI_Systems

Buiten Miriam. *Product Liability for Defective AI*. SSRN Scholarly Paper. Rochester, NY, 2023, p. 255. https://papers.ssrn.com/abstract=4515202.

Butz Martin V. *Towards Strong AI*. KI - Künstliche Intelligenz 35, fasc. 1, 2021, p. 91–101. https://doi.org/10.1007/s13218-021-00705-x

Cabral Tiego Sergio. *The Proposed AI Libability Directive, Another Pieco of the Puzzle for AI Regulation in the EU.* Consumer, Health & Environment - Data, Tech & IP - Justice & Litigation 2022. https://eulawlive.com/op-ed-the-proposed-ai-liability-directive-another-piece-of-the-puzzle-for-ai-regulation-in-the-eu-by-tiago-sergio-cabral/

Carroccia Francesca. *Ancora su responsabilita` civile e uso delle intelligenze artificiali.* Contratto e Impresa, 2022, p. 418.

Cath Corinne, Wachter Sandra, Mittelstadt Brent, Taddeo Mariarosaria, Floridi Luciano. *Artificial Intelligence and the "Good Society": The US, EU, and UK Approach*. Scholarly Paper. Rochester, NY, 2016. https://doi.org/10.2139/ssrn.2906249

Čerka Paulius, Grigienė Jurgita, Sirbikytė Gintarė. *Liability for Damages Caused by Artificial Intelligence*. Computer Law & Security Review 31, fasc. 3, 2015, p.376–89. https://doi.org/10.1016/j.clsr.2015.03.008

Chamberlain Johanna. *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*. European Journal of Risk Regulation, 2023, p. 8. https://shorturl.at/tsEKg

Chesterman Simon. *Artificial Intelligence and the Problem of Autonomy*. SSRN Scholarly Paper. Rochester, NY, 2020. https://doi.org/10.2139/ssrn.3450540

Cioni Andra. *Nuovi Pregi e Vecchi Difetti della Proposta di Direttiva sulla Responsabilità da Prodotto Difettoso, con Particolare Riferimento all'Onere della Prova*.Responsabilità Civile e Previdenza, 2023, pag. 661.

Commissione Europea. *Orientamenti Etici per un'IA Affidabile | Plasmare il Futuro Digitale dell'Europa*. https://digital-strategy.ec.europa.eu/it/library/ethics-guidelines-trustworthy-ai

Commissione Europea. *Q&As on the Revision of the Product Liability Directive*. 2022. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5791.

Commissione UE. *What does Data Protection 'by design' and 'by default' Mean?*. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

CONSAP. *Fondo di Garanzia per le Vittime della Strada.* 2024. https://www.consap.it/fondo-di-garanzia-per-le-vittime-della-strada/

Cuatrecasas Carlota. *Legal Challenges of Artificial Intelligence (AI)*. Global Privacy Law Review 1, fasc. 1, 2020. https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2020003.pdf

Curran William J. *Report of the Secretary's Commission on Medical Malpractice.* New England Journal of Medicine, vol. 289, fasc. 5, pp. 252–253, ago. 1973. https://www.nejm.org/doi/abs/10.1056/NEJM197308022890507

D'Adda Alessandro. *Danni «da Robot» (Specie in Ambito Sanitario) e Pluralità di Responsabili tra Sistema della Responsabilità Civile ed Iniziative di Diritto Europeo*.

Rivista di diritto civile, 2022, p. 825. https://publires.unicatt.it/en/publications/danni-da-robot-specie-in-ambito-sanitario-e-pluralit%C3%A0-di-responsa

D'Alfonso Giovanna. *Danni Algoritmici e Sviluppi Normativi Europei tra "Liability" e "Permittance" Rules.* European Journal of Privacy Law & Technologies, 2022, p. 30. https://doaj.org/article/71ef0464df5b4315b63b94917732892b

D'Alfonso Giovanna. *The Regime of Liability from Things in Custody between Traditional Issues and 'Algorithm Liability.* European Journal of Privacy Law & Technologies, 2022, p. 104. https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1627/1094

D'Amico Laura. *Intelligenza Artificiale e Auto a Guida Autonoma. tra Prevenzione Primaria, Colpa Penale e Rischio Consentito.* Riv. It. Med. Leg., 2022, p. 608.

Davola Antonio, Pardolesi Roberto. *In Viaggio col Robot: Verso Nuovi Orizzonti della R.C. Auto ('Driverless')?* Danno e Responsabilità, n. 5, 1 settembre 2017, p. 620;

Di Ciommo Francesco, *Minore maleducato e responsabilità dei genitori*, in Danno e Resp, 1998, p. 1090

Di Ciommo Francesco, Scarpellino Camilla. *Le Priorità della Presidenza Italiana del G7 sull'Intelligenza Artificiale*. LUISS Policy Observatory, 03/2024. https://sog.luiss.it/sites/sog.luiss.it/files/Le%20priorita%CC%80%20del%20G7%20per%20l'Intelligenza%20Artificiale_REV.pdf

Degli-Esposti Sara, Ferrándiz Ester. *After the GDPR: Cybersecurity is the Elephant in the Artificial Intelligence Room.* European Business Law Review 32, 2021, p. 1–24. https://doi.org/10.54648/EULR2021001

Embi Peter J. *Algorithmovigilance-Advancing Methods to Analyze and Monitor Artificial Intelligence-Driven Health Care for Effectiveness and Equity*. JAMA Network Open 4, fasc. 4, 2021. https://doi.org/10.1001/jamanetworkopen.2021.4622

Faccioli Mirco. *La responsabilità civile per danni cagionati da sistemi di intelligenza artificiale nel prisma dell'onere della prova*. Responsabilità Civile e Previdenza, 2024, p. 950.

Fernandes Márcia Santana, Goldim José Roberto. *Artificial Intelligence and Decision Making in Health: Risks and Opportunities*. Multidisciplinary Perspectives on Artificial Intelligence and the Law, Cham: Springer International Publishing, 2024, p. 187–205. https://doi.org/10.1007/978-3-031-41264-6_10

Ferrari Maurizio, *Predizione Algoritmica, Intelligenza Artificiale Generativa e Rischi di Cristallizzazione dell'Ermeneutica Giurisprudenziale*. Il Foro Italiano, 2023, p. 2.

Figone Alberto. *Responsabilità Civile dei Genitori, dei Tutori, degli Insegnanti e dei Maestri d'Arte o Mestiere*. Illecito e Responsabilità Civile, G. Giappichelli Editore – Torino, 2005. https://www.ambientediritto.it/dottrina/Dottrina_2005/responsabilita_genitori_figone.htm.

Finocchiaro Gisella. *La Disciplina dell'Esibizione delle Prove Risarcitori per Violazione delle Norme Antitrust in Attuazione della Dir. 2014/104/UE*. Nuove Leggi Civili Commentate, 2018, p. 415.

Floridi Luciano, Cowls Josh. *A Unified Framework of Five Principles for AI in Society*. Harvard Data Science Review 1, fasc. 1, 2019. https://doi.org/10.1162/99608f92.8cd550d1

Floridi Luciano. *AI as Agency Without Intelligence: On ChatGPT, Large Language Models, and Other Generative Models*. Philosophy & Technology 36, fasc. 1, 2023. https://doi.org/10.1007/s13347-023-00621-y

Floridi Luciano. *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford, New York: Oxford University Press, 2023. https://global.oup.com/academic/product/the-ethics-of-artificial-intelligence-9780198883098?cc=us&lang=en&

Floridi Luciano. *Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical*. Philosophy & Technology 32, fasc. 2, 2019, p. 185–93. https://doi.org/10.1007/s13347-019-00354-x

Frattari Niccolò Filippo. *Robotica e Responsabilità da Algoritmo. il Processo di Produzione dell'Intelligenza Artificiale.* Contratto e Impresa - Saggi, 2020.

Franzoni Massimo. *Dei Fatti Illeciti*. Comm. Scialoja, Branca, sub artt. 2043-2059, Bologna-Roma, 1993, p. 521.

Franzoni Massimo. *La responsabilità civile una lunga storia ancora da scrivere.* Contratto e Impresa, 2021, p. 1108

Franzoni Massimo. La Responsabilità Civile e gli Ottant'anni del Codice Civile. in Responsabilità Civile e Previdenza, 2022, p.1453.

https://www.rivistaresponsabilitamedica.it/la-responsabilita-civile-e-gli-ottantanni-del-codice-civile/

Fredrikson Matthew, Lantz Eric, Jha Somesh, Lin Simon, Page David, Ristenpart Thomas. *Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing*. Proceedings of the USENIX Security Symposium 2014, p. 17–32. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4827719/

Future of Life Institute*. Pause Giant AI Experiments: An Open Letter. https://futureoflife.org/open-letter/pause-giant-ai-experiments/*

Future of Life Institute. *Asilomar AI Principles*. https://futureoflife.org/open-letter/ai-principles/

Gajewski Megan K. *Automobile Insurance Reform in New Jersey: Could a Pure No-Fault System Provide a Final Solution?.* Seton Hall Law Review, vol. 25, fasc. 3, 1995. https://scholarship.shu.edu/shlr/vol25/iss3/13

Grasso Alfio Guido. *Diagnosi Algoritmica Errata e Responsabilità Medica.* Rivista di diritto civile, n. 2/2023, 2023. https://www.researchgate.net/publication/371167135_Diagnosi_algoritmica_errata_e_responsabilita_medica_in_Rivista_di_diritto_civile_n_22023

Gonçalves-Sá Joana, Pinheiro Flávio. *Societal Implications of Recommendation Systems: A Technical Perspective*, Springer International Publishing AG, 2023, p. 47–63. https://doi.org/10.1007/978-3-031-41264-6_3

Higgins Andrew. *Open Door Disclosure in Civil Litigation*. The International Journal of evidence & proof, 2012, p. 298. *https://journals.sagepub.com/doi/abs/10.1350/ijep.2012.16.3.406*

IEEE Standards Association. *The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems*. 2024. https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/

Hacker Philip. *The European AI liability directives – Critique of a half-hearted approach and lessons for the future*. Computer Law and Security Review, 2023, p. 1. https://www.sciencedirect.com/science/article/pii/S026736492300081X.

Khosravi,Mohsen, Zare Zahra, Morteza Mojtabaeian Seyyed, Izadi Reyhane. *Artificial Intelligence and Decision-Making in Healthcare: A Thematic Analysis of a Systematic*

Review of Reviews. Health Services Research and Managerial Epidemiology 11, 2024. https://doi.org/10.1177/23333928241234863

Kornilakis Angelos, Nouskalis Georgios, Pergantis Vassilis, Tzimas Themistoklis. *Artificial Intelligence and Normative Challenges*. Springer Nature Switzerland AG, 2023, p. 198. https://www.springerprofessional.de/en/artificial-intelligence-and-normative-challenges/26334384

Lai Alicia. *Artificial Intelligence, LLC: Corporate Personhood as Tort Reform*. SSRN Scholarly Paper. Rochester, NY, 2020. https://doi.org/10.2139/ssrn.3677360

Law Offices of Jeffrey S. Hasson, P.C. *What to know about NJ No-Fault Laws | Free Case Review.* https://www.hassonlawoffices.com/understanding-new-jersey-no-fault-laws/

Lima Pedro, Paiva Ana. *Autonomous and Intelligent Robots: Social, Legal and Ethical Issues.* 127–40, 2023. https://doi.org/10.1007/978-3-031-41264-6_7

Lior Anat. *AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy*. Mitchell Hamline Law Review 46, fasc. 5, 2020. https://open.mitchellhamline.edu/mhlr/vol46/iss5/2

Liverani Marco. *Algoritmi di Ordinamento.* Università Roma Tre, 2005. https://www.researchgate.net/publication/265349837_Algoritmi_di_ordinamento

Lucarelli Tonini Lorenzo Maria. *L'IA tra Trasparenza e Nuovi Profili di Responsabilità: La Nuova Proposta di "Ai Liability Directive".* Diritto dell'Informazione e dell'Informatica, 2023, p. 343.

Maglio Gabriele. *Bilanciare Regolamentazione e Innovazione: le Sfide del Mercato Digitale Europeo.* LUISS Policy Observatory, 02/2024.https://sog.luiss.it/sites/sog.luiss.it/files/Policy%20Brief_2-2024_Bilanciare%20regolamentazione%20e%20innovazione.pdf

Mantovani Rebecca. *La lingua segreta dei bot di Facebook.* Focus Tecnologia e Innovazione. 2017 https://www.focus.it/tecnologia/innovazione/la-lingua-segreta-dei-bot-di-facebook-intelligenza-artificiale-robot

Masucci Alfonso. *Procedimento Amministrativo e Nuove Tecnologie. Il Procedimento Amministrativo Elettronico ad Istanza di Parte*, Giappichelli Editore, Torino, 2011.

Mazzini Gabriele, Scalzo Salvatore. *The Proposal for the Artificial Intelligence Act: Considerations Around Some Key Concepts*. SSRN Scholarly Paper. Rochester, NY, 2022. https://doi.org/10.2139/ssrn.4098809.

Mc Kinsey & Company. *Leveraging Generative AI in Europe: The Opportunities and Challenges*. 2023. https://www.mckinsey.com/featured-insights/lifting-europes-ambition/leveraging-generative-ai-in-europe-the-opportunities-and-challenges.

Mondello Gérard. *Strict Liability, Scarce Generic Input and Duopoly Competition.* European Journal of Law and Economics, 2022 54:369–404. https://doi.org/10.1007/s10657-022-09738-5;

Monot-Fouletier Marjolaine. *Liability for Autonomous Vehicle Accidents.* The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, 163–78. Cambridge Law Handbooks. Cambridge University Press, 2022. https://doi.org/10.1017/9781009072168.018

Moral Machine. *Moral Machine*. 2024. http://moralmachine.mit.edu

Moretti Alessandro. *Algoritmi e Diritti Fondamentali della Persona. Il Contributo del Regolamento (UE) 2016/679*. Università Roma Tre, 2018.

Muftic Nasir. *Understanding the Risks of Artificial Intelligence as a Precondition for Sound Liability Regulation.*, Artificial Intelligence and Normative Challenges International and Comparative Legal Perspectives, in Law, Governance and Technology Series, Springer Nature Switzerland AG, 2023, p. 86. https://www.springerprofessional.de/en/understanding-the-risks-of-artificial-intelligence-as-a-precondi/26334420

Nabil Ryan. *Artificial Intelligence Regulatory Sandboxes.* Journal of Law, Economics & Policy, 2024, p. 295. https://static1.squarespace.com/static/6233d0b9d24b954d519e5d62/t/6631bb5099f1225c6c01dfa8/1714535248948/Nabil+Final+for+PDF.pdf

Nachman Harvey B., *Puerto Rico and Its No Fault System*, in International Society of Barristers Quarterly 5, 1970, p. 52-62

Neri Arianna. *Uso di un Algoritmo Discriminatorio nella Contrattazione Privata.* La Nuova Giurisprudenza Civile Commentata, a.37 n.4, 2021, p.983-990.

Novarini Matteo. *La Truffa che Sconvolse Wall Street (e non la Cambiò per Niente): I 20 Anni del Crac della Enron.* Forbes Business, 2021. https://forbes.it/2021/12/02/enron-20-anni-truffa-rivelo-lato-oscuro-wall-street/

Novelli Claudio, Casolari Federico, Hacker Philipp, Spedicato Giorgio, Floridi Luciano. *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. SSRN Scholarly Paper. Rochester, NY, 2024. https://doi.org/10.2139/ssrn.4694565

Novelli Claudio, Taddeo Mariarosaria, Floridi Luciano. *Accountability in Artificial Intelligence: What it Is and How it Works*. SSRN Scholarly Paper. Rochester, NY, 2022. https://doi.org/10.2139/ssrn.4180366.

OECD AI, Policy Observatory. *AI Principles Overview*. 2019 https://oecd.ai/en/principles

OpenGov Asia. *Empowering SMEs: Singapore's GenAI Sandbox Initiative.* 2024. https://opengovasia.com/2024/02/09/empowering-smes-singapores-genai-sandbox-initiative/.

OECD. *G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI*. Paris Organisation for Economic Co-operation and Development, 2023. https://www.oecd-ilibrary.org/science-and-technology/g7-hiroshima-process-on-generative-artificial-intelligence-ai_bf3c0c60-en

Pasceri Giovanni. *Intelligenza Artificiale,Algoritmo e Machine Learning: la Responsabilità del Medico e dell'Amministrazione Sanitaria*. Temi di Diritto Privato e di Diritto Pubblico, Giuffrè Francis Lefebvre, 2021. https://shop.giuffre.it/024211978-intelligenza-artificiale-algoritmo-e-machine-learning

Pagallo Ugo. *Intelligenza Aritificiale e Diritto. Linee Guiga per un Oculato Intervento Normativo*. Sistemi Intelligenti, Il Mulino, 2017, p. 618. https://www.rivisteweb.it/doi/10.1422/88512

Pagallo Ugo, Casanovas Pompeu, Madelin Robert. *The Middle-Out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data*.
The Theory and Practice of Legislation 7, fasc. 1, 2019, p. 1–25.https://doi.org/10.1080/20508840.2019.1664543

Pagallo Ugo. *The Laws of Robots - Crimes, Contracts, and Torts*. Springer, 2023, p. 121.. https://www.scribd.com/document/495319057/PAGALLO-The-Laws-of-Robots-Crimes-Contracts-and-Torts.

Papadouli Vasiliki. *Artificial Intelligence's Black Box: Posing New Ethical and Legal Challenges on Modern Societies.* Springer Nature Switzerland AG, 2023, p. 47 https://www.springerprofessional.de/en/artificial-intelligence-s-black-box-posing-new-ethical-and-legal/26334410

Pardolesi Roberto, *Danni cagionati dai minori: pagano sempre i genitori?*, in Fam. e dir., 1997, p. 227

Paxton AI Legal Drafting. *Straight-Forward Legal Document*. Drafting. 2024. https://www.paxton.ai/drafting?utm_term=legal%20document%20automation&utm_campaign=Contract+Review&utm_source=adwords&utm_medium=ppc&gad_source=1

Poole David, Mackworth Alan, *Artificial Intelligence: Foundations of Computational Agents.* Cambridge University Press, 2010. https://nlp.jbnu.ac.kr/AI2019/Cambridge_ArtificialIntelligence.pdf

Proietti Giuseppe, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*. Contratto e Impresa, n. 3/2022, p. 880-895.

Prospetti Eugenio. *Accesso al Software e al Relative Algoritmo nei Procedimenti Amministrativi e Giudiziali. Un'Analisi a Partire da Due Pronounce del Tar Lazio.* 2019

Puleo Giulia. *La Gestione del Rischio Emergente da Veicoli Autonomi in due Proposte di Regolamento dell'Ue e le Conseguenze sull'Assicurazione degli Operatori.* Juscivile, 2021, p.1048. http://www.juscivile.it/Article/Archive/index_html?ida=288&idn=41&idi=-1&idu=-1

Rake Jonathan*. The hard market: Challenges and Opportunities.* SwisseRe Corporation Solutions, 2021. https://corporatesolutions.swissre.com/insights/knowledge/the-hard-market-challenges-and-opportunities.html

Ranchordas Sofia, Vinci Valeria. *Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture*. SSRN Scholarly Paper. Rochester, NY, 2024. https://doi.org/10.2139/ssrn.4696442.

Resta Giorgio. *Cosa c'è di "Europeo" nel Diritto Privato Europeo?* Diritto dell'Informazione e dell'Informatica, 2022, p. 327.

Ricci Annarita*. I Diritti dell'Interessato*. In Aa. Vv. Finocchiaro Gisella (a cura di), Il Nuovo Regolamento Europeo sulla Privacy e sulla Protezione dei Dati Personali, 2017,

p. 243. https://www.zanichelli.it/ricerca/prodotti/il-nuovo-regolamento-europeo-sulla-privacy-e-sulla-protezione-dei-dati-personali

Ruffolo Ugo. *Intelligenza artificiale, machine learning e responsabilità da algoritmo*. Giurispondenza Italiana, 2019, p. 1689. https://www.altalex.com/documents/2019/11/07/intelligenza-artificiale-machine-learning-e-responsabilita-da-algoritmo.

Russo Christopher. *The Myth of Dogs Being Allowed One Bite Free.* Kirshenbaum & Kirshenbaum https://www.kirshenbaumri.com/library/the-myth-of-dogs-being-allowed-one-bite-free.cfm

Sag Matthew. *Fairness and Fair Use in Generative AI*. Fordham Law Review 92, fasc. 5, 2024, p. 1887. https://ir.lawnet.fordham.edu/flr/vol92/iss5/7/

Salanitro Ugo. *Intelligenza Artificiale e responsabilità: la strategia della Commissione Europea*. Rivista di Diritto Civile, 2020, p. 1272. https://www.academia.edu/44905831/Intelligenza_artificiale_e_responsabilit%C3%A0_la_strategia_della_Commissione_Europea

Scarpellino Camilla. *Responsabilità nell'E-Health*. Comparative Law Review 13, fasc. 14/2, 2023. http://www.comparativelawreview.unipg.it/index.php/comparative/article/view/271.

Sconcamiglio Maria Luisa. *Intelligenza Artificiale e Responsabilità Civile: L'approccio Dell'Unione Europea – 1) Il Quadro Generale*. Il Foro Italianp. 2023. https://www.foroitaliano.it/news/2653/intelligenza-artificiale-e-responsabilita-civile-l-approccio-dell-unione-europea-1-il-quadro-generale/

Scotto di Carlo Marco, *La responsabilità connessa all'utilizzo dei sistemi di intelligenza artificiale*, in Danno e Resp., 2024, p. 424;

Simonini Gianfranco. *La Responsabilità del Fabbricante nei Prodotti con Sistemi di Intelligenza Artificiale.* Danno e Responsabilità, 2023, p. 442.

Sutton Reed T., Pincok David, Baumgart Daniel C., Sadowsky Daniel C., Fedorak Richard N., Kroeker Karen I. *An overview of clinical decision support systems: benefits, risks, and strategies for success.* Nature Digital Medicine, 2020, p.3. https://www.nature.com/articles/s41746-020-0221-y

Studdert David, Thomas Eric J., Zbar Brett I. W., Newhouse Joseph P., Weiler Paul C., Jonathon Bayuk, Brennan Troyen A. *Can the United States Afford a "No-Fault" System of Compensation for Medical Injury?* Law and Contemporary Problems, vol. 60, fasc. 2, 1997, p. 1–36.
https://scholarship.law.duke.edu/lcp/vol60/iss2/1/

Tampieri Maura. *L'Intelligenza Artificiale: Una Nuova Sfida Anche per le Automobili*. Contratto e Impresa 36, fasc. 2, 2020, p.732–59.
https://cris.unibo.it/handle/11585/766085

Taramundi Dolores Morondo. *Le Sfide della Discriminazione Algoritmica.* GenIUS, 2022, p.26.
https://www.geniusreview.eu/wpcontent/uploads/2022/10/Taramundi_focus_1.pdf

The Economist. *The World's Most Valuable Resource is No Longer Oil, But Data. 2017*.
https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The GFIN. *The Global Financial Innovation Network*. https://www.thegfin.com.

The Toronto Declaration. https://www.torontodeclaration.org/declaration-text/english/

Trebilcock Micheal J. *The Social Insurance-Deterrence Dilemma of Modern North American Tort Law: A Canadian Perspective on the Liability Insurance Crisis*. 24 San Diego Law Review, 1987, p. 929. https://digital.sandiego.edu/sdlr/vol24/iss4/9/

Torne Helen. *What Are Generative AI, Large Language Models, and Foundation Models?*. Center of Security and Emerging Technology (CSET), 2023.
https://cset.georgetown.edu/
article/what-are-generative-ai-large-language-models-and-foundation-models/

Trimarchi Pietro. *Rischio e Responsabilità Oggettiva*. Giuffrè, Milano, 1961, p. 48.
https://www.libreriantiquaria.com/it/catalogo/diritto/diritto-e-procedura-civile/4116-rischio-e-responsabilita-oggettiva.html

UNESCO. *Raccomandazione UNESCO su l'Etica dell'IA: Modellare il Futuro delle Nostre Società.* 2023. https://www.unesco.it/wp-content/uploads/2023/11/Brochure-su-Raccomandazione-UNESCO-sullIntelligenza-Artificiale-1.pdf

Vandersteegen Tom, Marneffe Wim, Cleemput Irina, Vereeck Lode. *The impact of no-fault compensation on health care expenditures: An empirical study of OECD countries*.

ScienceDirect, Health Policy, 2015, p. 368. https://www.sciencedirect.com/science/article/pii/S0168851014002401?via%3Dihub

Vincent Charles. *Compensation as a duty of care: the case for "no fault"*. BMJ Quality & Safety, 2003, pp .240-241. https://colab.ws/articles/10.1136%2Fqhc.12.4.240

Wachter Sandra, Mittelstadt Brent, Floridi Luciano. *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. International Data Privacy Law 7, fasc. 2, 2017, p. 76–99. https://doi.org/10.1093/idpl/ipx005

Winter Ralph. *The Liability Crisis and the Dynamics of Competitive Insurance Markets.* Yale Journal on Regulation, 1988, p. 455. https://openyls.law.yale.edu/handle/20.500.13051/8382

Wrigley Sam. *Taming Artificial Intelligence: "Bots," the GDPR and Regulatory Approaches*.
In M. Corales et al, Robotics, AI and the Future of Law, Springer, 2018, p. 183–208. https://doi.org/10.1007/978-981-13-2874-9_8

Wulf Alexander J., Seizov Ognyan. *Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU*. SSRN Scholarly Paper. Rochester, NY, 2020. https://papers.ssrn.com/abstract=3906460

Yoshikawa Jin. *Sharing the Costs of Artificial Intelligence: Universal No-Fault Social Insurance for Personal Injuries*. Vanderbilt Journal of Entertainment and Technology Law, 2020, p. 1172;
https://scholarship.law.vanderbilt.edu/jetlaw/vol21/iss4/8

Atti e Giurisprudenza

Annals of Health Law Ulrich An Evalution of the Danish No-Fault System for Compensating Medical Injuries. 3 Annals Health L. 243 (1994). https://lawecommons.luc.edu/annals/vol3/iss1/17

Carta di Nizza, 2007. https://fra.europa.eu/it/eu-charter/article/21-non-discriminazione

Codice Civile. Regio Decreto 16 marzo 1942, n. 262 aggiornato alla L. 8 agosto 2024, n. 112. https://www.normattiva.it/

Codice di Procedura Civile. Regio Decreto 28 ottobre 1940, n. 1443 aggiornato alla L. 29 aprile 2024, n. 56. https://www.normattiva.it/

Cassazione Civile, Sezione III, Sentenza n. 4742 del 30 marzo 2001.

Cassazione Civile., Sezione III, Sentenza n. 5667 del 18 settembre 1986.

Cassazione Civile, Sezione III, Sentenza n. 6395 del 07 luglio 1994.

Commissione UE. Better Regulation: Guidelines and Toolbox. 2023.https://commission.europa .eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_en.

Commissione UE. Evaluation of Council Directive 85/374/EEC. 2018. https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52018SC0157.

Commissione UE. Inception Impact Assessment. Ref. Ares, 2021. https://competition-policy.ec.europa.eu/system/files/2021-06/HBERs_inception_impact_assessment.pdf

Commissione UE. Libro Bianco sull'Intelligenza Artificiale - Un Approccio Europeo all'Eccellenza e alla Fiducia. COM 2020 65, p. 1. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0065

Commissione UE. L'Intelligenza Artificiale per l'Europa. COM (2018) 237 final, Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. 2018. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM%3A2018%3A237%3AFIN

Commissione UE. Proposal for a Directive of the European Parliament and of the Council on adapting non-Contractual Civil Liability Rules to Artificial Intelligence.

COM (2022) 496 Final 2022/0303 (COD). 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0496.

Commissione UE. Proposta di Direttiva Del Parlamento Europeo e Del Consiglio sulla Responsabilità per Danno da Prodotti Difettosi (PLD). COM (2022) 495 Final. 2022. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52022PC0495

Convenzione Europea dei Diritti dell'uomo (CEDU). 1997. https://presidenza.governo.it/CONTENZIOSO/contenzioso_europeo/documentazione/Convention_ITA.pdf

Corte di Giustizia Europea. Causa C-621/15: Sentenza della Corte (Seconda Sezione) del 21 giugno 2017. Domanda di pronuncia pregiudiziale Proposta dalla Cour de Cassation, e a. Contro N. W, L. W, C. W/Sanofi Pasteur MSD SNC**.** https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62015CA0621

Costituzione della Repubblica Italiana, 1948. https://www.governo.it/it/costituzione-italiana/principi-fondamentali/2839

Denmark Ministry of Health. Danish Patient Act. 2018. https://eng.patienterstatningen.dk/entitled-to-compensation/laws-and-regulations

Dichiarazione di Montreal Sullo Sviluppo Responsabile Dell'Intelligenza Artificiale, 2021. https://declarationmontreal-iaresponsable.com/wp-content/uploads/2023/01/VF_UdeM_Decl_IA_Resp_LA_Declaration_Ital_26oct2021.pdf

Dichiarazione Universale dei Diritti Umani, 1948. https://www.senato.it/application/xmanager/projects/leg18/file/DICHIARAZIONE_diritti_umani_4lingue.pdf

Executive Office of the President National Science and Technology Council Committee on Technology. Preparing for the Future of Artificial Intelligence. Washington, DC, USA, p. 32. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

GPDP. Intelligenza Artificiale: il Garante Blocca ChatGPT. Raccolta Illecita di Dati Personali. Assenza di Sistemi per la Verifica dell'Età dei Minori. 2023. https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9870832.

Ministero della Salute. Indennizzi per i Danneggiati in Modo Irreversibile da Vaccinazioni, Trasfusioni e Somministrazione di Emoderivati Infetti. Legge 210/92, 1992. https://www.salute.gov.it/portale/indennizzo/dettaglioContenutiIndennizzo.jsp?lingua=italiano&id=921&area=indennizzo&menu=vuoto

Ministero dell'Agrigolutra, della Sovranita' Alimentare e delle Foreste. DL 11 agosto 2023. https://www.gazzettaufficiale.it/eli/id/2023/10/17/23A05685/sg

Parlamento Europeo. Artificial Intelligence Liability Directive. 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf

Parlamento Europeo. Direttiva 2014/104/UE. 2014. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv%3AOJ.L_.2014.349.01.0001.01.ITA

Paralmento Europeo. Direttiva 85/36/CEE. 1985. https://eur-lex.europa.eu/legal-content/MT/HIS/?uri=CELEX:51985PC0572

Parlamento Europeo. Direttiva 93/42/CEE. 1993. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:it:PDF

Parlamento Europeo. EU AI Act: First Regulation on Artificial Intelligence. Regolamento EU 2024/1689. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Parlamento Europeo. Legislative Train for a Europe Fit for a Digital Age. Procedura 2021/0106. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence

Parlamento Europeo. Norme di Diritto Civile sulla Robotica. Risoluzione del Parlamento Europeo, 2015/2103 (INL). 2017. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=IT

Parlamento Europeo. Civil Liability Regime for Artificial Intelligence. 2024/2014 INL. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020IP0276

Parlamento Europeo. Regolamento UE 2016/679. 2016 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679

Parlamento Europeo. Regolamento UE 2017/745. 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017R0745

Parlamento Europeo. Regolamento UE 2017/746. 2017. https://eur-lex.europa.eu/eli/reg/2017/746/oj

Parlamento Europeo. Texts Adopted - Civil Liability Regime for Artificial Intelligence. 2020 https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

Patto Internazione sui Diritti Civili e Politici, 1996. https://unipdcentrodirittiumani.it/it/schede/Articolo-26-LOnda-ha-il-suo-diritto/30

Senate No. 3, State of New Jersey, 208th Legislature. The Automobile Insurance Cost Reduction Act. 1998. https://pub.njleg.gov/bills/9899/s0500/3_i1.htm ;

Supreme Court of Illinois. Case Law 102 Ill. 2d 505. 1984. https://law.justia.com/cases/illinois/supreme-court/1984/58203-6.html

United Nations. United Nations Convention on the Use of Electronic Communications in International Contracts. 2005. https://treaties.un.org/doc/source/RecentTexts/X-18_english.pdf.

The Government of Japan. The Hiroshima AI Process: Leading the Global Challenge to Shape Inclusive Governance for Generative AI. https://www.japan.go.jp/kizuna/2024/02/hiroshima_ai_process.html