Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2023/2024

IL DANNO DA USO DI INTELLIGENZA ARTIFICIALE: STATO DELL'ARTE E PROPOSTE NORMATIVE

Relatore: Prof. Claudio Sarra

Studente: Giacomo Varotto

Matricola n. 2043003

Introduzione

Le ricerche riguardanti l'intelligenza artificiale sono risalenti agli anni '50 del XX secolo, quando venne proposto il tema tra gli altri da Alan Turing nel suo pionieristico *Computing Machinery and Intelligence*[1], e una definizione solo nel 1956 da parte di John McCarthy[2]. Da allora la nozione di IA ha avuto fasi di notorietà accompagnate da grande entusiasmo da parte di addetti ai lavori e pubblico, alternate a fasi di delusione per via delle eccessive aspettative riposte nello strumento: i cosiddetti "*inverni dell'IA*" [3].

L'evoluzione dei sistemi si è vista anche nel raggiungimento di obiettivi tecnico-operativi apparentemente futili, come il programma sviluppato da Arthur Samuel, in cui il sistema sapeva rispondere in autonomia alle mosse di una partita di *dama*. Una funzionalità in realtà di grande rilevanza, in quanto dimostrò l'autonomia in un'attività (il gioco) che presenta degli schemi ripetuti: capacità che può essere adattata ad una grande quantità di applicazioni[4].

Successivamente, con l'affermazione delle tecnologie di *machine learning* prima, già impiegate da Samuel, e di *deep learning* poi, quando lo sviluppo tecnologico delle memorie ha permesso l'efficientamento delle *neural networks*[5], è stato possibile sviluppare delle IA con capacità molto simili alle ipotesi più ottimistiche fatte dagli studiosi di cibernetica negli anni '60.

La tecnologia alla base delle applicazioni che hanno avuto maggior successo commerciale in ambito di intelligenza artificiale negli ultimi dieci anni sono i cosiddetti LLM (*Large Language Model*), i quali elaborano risposte in linguaggio coerente alla domanda, la quale può essere posta tramite testo in linguaggio naturale, contribuendo all'impressione di interagire con una persona. Il risultato è stato raggiunto attraverso il *training,* ovvero l'analisi di dati, di una quantità enorme (decine di *terabyte* di file di testo) di documenti provenienti dal

[1] TURING, 1950
[2] Dartmouth Summer Research Project on Artificial Intelligence, 1956
[3] NILSSON, 2009
[4] SAMUEL, 1959
[5] S. KARTHI, P. KASTJURIRENGAN, 2021

web, i quali hanno fornito la base su cui elaborare le risposte. Gli LLM hanno dato una svolta significativa al panorama dei sistemi di intelligenza artificiale da quando sono stati combinati con le GAN (*Generative Artificial Networks):* dei sistemi di intelligenza artificiale che sono in grado di generare sia testo che immagini o video, e grazie all'integrazione con gli LLM, queste operazioni possono essere compiute facilmente da qualsiasi utente, anche non esperto. A partire dal 2022 è infatti diventato argomento di discussione su tutti i giornali la commercializzazione da parte di *OpenAI* di un sistema complesso ed efficace quanto quello di GPT-3 (e rapide evoluzioni fino a GPT-4o)[6]. La facilità d'uso e la possibile implementazione in qualsiasi operazione digitale, comprendendo ogni strumento di domotica o robotica utilizzato in ambito sia industriale che domestico, ha sollevato preoccupazioni circa gli utilizzi illeciti e la vastità dell'impatto delle operazioni che possono essere così facilmetnte svolte grazie a questa tecnologia.

Oltre al panorama ingegneristico, fin dal principio sono state rilevanti le ricerche e le preoccupazioni in ambito etico-giuridico, seguendo nell'intensità del dibattito l'andamento dei successi e delle promesse provenienti dai ricercatori. Gli stessi inventori di questi sistemi sono stati i primi ad esprimere preoccupazioni per ciò che stavano creando o ciò che si sarebbe potuto creare proseguendo nella traiettoria tracciata da loro, così tentarono di dare riferimenti per la definizione di paradigmi utili a rendere consapevoli gli utilizzatori e la società in generale: sopra tutti il celebre *test* di Turing[7] e il richiamo delle fantascientifiche tre più uno *leggi della robotica* di Asimov[8].

A livello europeo una spinta preliminare alla legislazione in tema di calcolatori, comunicazioni elettroniche e trattamento dei dati si è avuta con la *Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al*

[6]*Hello GPT-4o*, May 13, 2024, OpenAI.com in : https://openai.com/index/hello-gpt-4o/ visitato l'ultima volta il 27/08/2024
[7] TURING, 1950
[8] ASIMOV, 1950

trattamento automatizzato di dati a carattere personale[9] (Convenzione 108), passando poi per la protezione da parte delle Comunità Europee degli acquisti online (Direttiva sul commercio elettronico[10]) e con legislazione specifica anche della *privacy* (Direttiva 95/46/CE[11]) per poi giungere gradualmente a coprire quasi ogni aspetto delle attività eseguibili con un computer: seguendo e supportando l'andamento della digitalizzazione che ha pervaso ogni ambito della vita.

Per quanto riguarda le conseguenze specifiche della diffusione delle tecnologie di intelligenza artificiale, l'Unione Europea sta provando a porsi come *leader mondiale nello sviluppo di un'IA sicura, affidabile ed etica*[12] riuscendo ad approvare l'*AI Act*[13] nel 2024, il quale però ha come principale caratteristica la definizione di quattro livelli di rischio in cui categorizzare i sistemi di intelligenza artificiale: tra cui uno di *rischio minimo* per il quale il regolamento stesso non prescrive ulteriori obblighi, e uno di *rischio inaccettabile*, secondo cui dunque i rischi per la sicurezza dei cittadini europei sono troppi per ammettere l'uso di tali sistemi. Da questo regolamento non risulta alcuna indicazione sullo sviluppo di una normativa che definisca la responsabilità civile extracontrattuale da sistemi di intelligenza artificiale[14], lasciando ad una normativa successiva il chiarimento di questo punto fondamentale, e preliminare per una larga adozione della tecnologia in tema, come evidenziato dalla Relazione alla Proposta di direttiva sulla responsabilità da intelligenza artificiale[15].

---

[9] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Consiglio d'Europa del 28 gennaio 1981

[10] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno

[11] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

[12] Consiglio europeo, riunione straordinaria del Consiglio europeo (1 e 2 ottobre 2020) – Conclusioni, EUCO 13/20, 2020

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

[14] D'ALFONSO, 2022

[15] Proposta di direttiva del parlamento europeo e del consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale e modifica alcuni atti legislativi dell'unione COM/2021/206 final

Per comprendere quali sono gli sviluppi normativi che ci attendono riguardo la responsabilità relativa all'utilizzo dell'intelligenza artificiale, sarà necessario comprendere le ipotesi riguardanti gli schemi di responsabilità da intelligenza artificiale della dottrina autorevole, e come l'approccio del legislatore europeo ricalchi e adatti quegli schemi, conformandoli alla recente legislazione in merito a sistemi digitali: Digital Service Act[16], Digital Markets Act[17], e AI Act[18].

[16] Regolamento 2022/2065/UE che modifica la direttiva 2000/31/CE (c.d. regolamento sui servizi digitali)
[17] Regolamento 2022/1925/UE, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive 2019/1937/UE e 2020/1828/UE (c.d. regolamento sui mercati digitali)
[18] Regolamento 2024/1689/UE cit.

1. Schemi di responsabilità per l'Intelligenza Artificiale

Negli ultimi anni diversi Autori hanno affrontato il tema della responsabilità dell'intelligenza artificiale: chi analizzando aspetti particolari dell'applicazione della normativa speciale, per esempio in tema di contratti[19]; responsabilità da prodotto[20]: proprietà intellettuale[21]: e chi con approcci più integrali ha cercato di dare supporto alle teorie per lo sviluppo e l'integrazione della legislazione esistente considerando i dilemmi etici e giuridici derivanti dall'esistenza dei sistemi di IA[22].

Sono stati dunque ipotizzati da una parte scenari in cui i sistemi di IA hanno raggiunto livelli di autonomia totale: tale da poter essere assimilata secondo alcuni ad una persona fisica anche per quanto riguarda la capacità di pensiero, la c.d. Intelligenza Artificiale "forte", e quindi meritare uno status giuridico autonomo, quale la "personalità elettronica"[23], che si presenterà in seguito. Dall'altra scenari in cui la c.d. Intelligenza Artificiale "debole" presenta livelli di autonomia di pensiero che non sembrano comparabili con quelli di una persona, per via delle differenze nei meccanismi di ragionamento (quello biologico e quello meccanico) sottostanti[24] e per le limitazioni agli usi che si possono imporre. Tanto da suggerire solamente un'interpretazione *ad hoc* della legislazione già esistente, o al limite una sua evoluzione tramite legislazione speciale, ma offrendo tutela ai sistemi solamente in quanto cose, come già avviene[25], intervenendo talvolta sulla responsabilità contrattuale e talora sulle categorie della responsabilità aquiliana.

Il Parlamento europeo ha ravvisato l'urgenza di normare in materia di sistemi di intelligenza artificiale fin dal 2017[26], quando il tema non era ancora di

[19] RINALDI, 2020
[20] AMIDEI, 2020
[21] CAPPARELLI, 2020
[22] RUFFOLO, 2020, -c
[23] citata per la prima volta nella Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))
[24] CAROCCIA, 2020
[25] TADDEI ELMI, 1990
[26] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))

così comune dominio come oggi, ma dimostrando un certo ritardo se guardiamo alla risalenza degli avvertimenti in tema[27]. Nella Risoluzione si parla di "robot" e di "Intelligenza Artificiale" facendo riferimento addirittura alla letteratura fantascientifica per sottolineare la potenziale pericolosità dell'evoluzione di questi[28], esponendo i contenuti stessi alla critica che siano ispirati dalla paura verso le nuove tecnologie, piuttosto che da una comprensione tecnica e accurata del fenomeno.

La robotica è ampiamente diffusa nelle industrie da più di un secolo, mentre le applicazioni software di IA sono largamente presenti da oltre 50 anni. Ciò che si vuole normare più precisamente sono una categoria specifica di artefatti: sistemi assimilabili alle citate Intelligenze Artificiali "forti", quando dotate di elevata autonomia e combinate con appendici materiali che permettono di agire direttamente nel mondo, non dunque i soli software, che per quanto impattanti, sono oggetto di riflessioni a parte.

Il legislatore è per definizione destinato ad inseguire le evoluzioni tecnologiche, e sta proprio in questo secondo alcuni[29] la chiave per dare risposte durature, seguendo un approccio di neutralità tecnologica: una legislazione che dia principi applicabili di volta in volta alle nuove tecnologie, fornendo obiettivi da raggiungere e non limiti basati sulla singola applicazione tecnologica. Approccio questo prevalente a livello internazionale, come dimostrato nella *Model law on electronics* dell'UNCITRAL[30] e nel Regolamento e-IDAS[31].

Ad esempio l'ondata che ha investito la nostra società dal 2022, quando le prime applicazioni di IA di facile utilizzo per qualsiasi utente hanno iniziato a diffondersi[32], ha reso palese la potenza di questi sistemi, e l'inadeguatezza degli

[27] da CAROCCIA, cit. Una prospettiva che considera le potenzialità della robotica moderna sulla massificazione, profeticamente S. RODOTÀ *Elaborati elettronici e controllo sociale,* Bologna, 1973
[28] Considerando A, Risoluzione 16 febbraio 2017, cit.
[29] G. FINOCCHIARO, 2022; D'ALFONSO, 2022
[30] UNCITRAL, Model Law on Electronic Commerce, 1996
[31] Regolamento 2014/910/UE del parlamento europeo e del consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
[32] DALL-E software per la generazione di immagini a partire da testo; e ChatGPT software per la creazione di testo ottimizzato per risultare più accuratamente possibile linguaggio umano, sono stati rilasciati con grande successo nel 2022 dall'azienda OpenAI

strumenti normativi per affrontare il problema. Fin da subito sono stati chiari i rischi legati all'affidabilità delle informazioni; al diritto d'autore; al trattamento dei dati personali. Temi che erano già stati evidenziati negli anni ad esempio dal Comitato Economico e Sociale Europeo[33], e che hanno reso più urgenti le riflessioni sugli interventi normativi da operare, in particolare a livello comunitario.

1.1 Personalità elettronica

Dalla già citata Risoluzione del Parlamento del 2017[34], sono emerse alcune necessità per normare il fenomeno dell'Intelligenza Artificiale compatibilmente con il rispetto dei diritti dei cittadini europei, e la necessità di garantire la tutela dell'innovazione. Tra i punti che hanno fatto discutere, quello maggiormente attenzionato è la possibilità di introduzione, per quanto indicata come proposta di lungo periodo, della c.d. "personalità elettronica" citata al punto §59 f), come conclusione di una serie di iniziative che possono essere valutate per affrontare il problema delle macchine dotate di autonomia.

Alcune di queste proposte riguardano l'introduzione di un regime assicurativo obbligatorio simile a quella per la limitazione della responsabilità civile per le automobili §59 a); l'istituzione di fondi comuni, generali o per categoria di robot, per i produttori e i proprietari, per far fronte agli eventuali danni cagionati dalle macchine §59 d).

Al punto §59 f) infine è proprio citata la possibilità dell'"*istituzione di uno status giuridico specifico per i robot*"[35], facendo sorgere quesiti in merito alla fondatezza di una tale novità. Sarà da definire in cosa consista la "personalità elettronica": si potrà far derivare dal modello delle persone fisiche, o da quello per le persone giuridiche, ma in risposta a tale ipotesi la dottrina ha anche elaborato personalità intermedie, ridotte o parziali, come l'ipotesi di una

[33] Parere del Comitato economico e sociale europeo su «L'intelligenza artificiale — Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società», 31 maggio 2017
[34] Risoluzione 16 febbraio 2017, cit.
[35] *Ibidem*

soggettività parziale dei flussi comunicativi in quanto attori collettivi[36]. Entrambe le esistenti personalità sono vettori di diritti e doveri: secondo Ruffolo[37] i problemi legati ai doveri nel caso dell'introduzione di una simile innovazione sono stati ampiamente dibattuti, e di relativamente facile soluzione, mentre la discussione dei diritti che dovrebbero derivare alle macchine e delle tutele da accordare a queste sarebbe molto più complessa e innovativa.

Si dovrebbe definire in che misura le macchine autonome siano libere di agire, e come le loro azioni si pongano in relazione con le scelte di proprietari e custodi. Come individuare la volontà, ammesso che la si possa chiamare tale, all'interno di un algoritmo che autoapprende e si modifica in base ad input e ambiente?

1.1.1 Trasparenza

La risposta a questo quesito si inserisce nel tentativo di risolvere il problema della c.d. *black box.* Secondo alcuni[38] ci sarebbero le capacità tecniche per risalire al processo che ha portato ad ognuna delle azioni compiute da un robot: ammesso che sia tecnicamente fattibile, bisogna poi scontrarsi con la tutela degli algoritmi accordata dalla proprietà intellettuale[39], strumento che supporta l'innovazione alla base della creazione di queste macchine complesse.

Si è già potuto vedere infatti come la potenziale indagine del processo decisionale della macchina possa essere ostacolato. Celebre è il caso del software COMPAS: utilizzato dalle corti di diversi stati statunitensi in diverse fasi del

[36] TADDEI ELMI, 2021

[37] Cfr. RUFFOLO, 2020, "*Il problema della "personalità elettronica"" -a*

[38] Nel 2018 un gruppo di esperti (tecnici, filosofi, imprenditori) dell'intelligenza artificiale ha scritto una lettera aperta alla Commissione Europea in seguito alla Risoluzione del 16 febbraio 2017 del Parlamento Europeo, "*Open Letter To The European Commission - Artificial Intelligence And Robotics*". Il gruppo ha criticato la proposta dell'introduzione di una personalità elettronica, sostenendo che fosse basata su assunti errati, dettata da una erronea comprensione del fenomeno, e che sarebbe stato un errore sia dal punto di vista etico-filosofico che legale. TADDEI ELMI, 2021, *cit.* sostiene l'infondatezza delle ragioni del gruppo, considerando che il PE non intendesse certamente dotare di personalità ontologica i robot, si trattava piuttosto di una personalità ascrittricia come quella delle società.

[39] D'AMBROSIO, 2020

processo penale, come la definizione della pena in base al fattore dato dal rischio di recidiva. Nonostante gli evidenti pregiudizi razziali, chiari dai risultati di analisi indipendenti, la corte d'appello non ha reso accessibile l'algoritmo sottostante all'imputato che ha fatto ricorso, tutelando invece il segreto industriale[40].

Questo fenomeno rientra nel problema della *explainability* delle decisioni algoritmiche. Secondo autorevole dottrina nel GDPR[41] ci sarebbe il tentativo di introdurre un diritto alla spiegazione delle decisioni prese in modo automatizzato che hanno impatto significativo sulle persone[42] all'articolo 22, quando combinato con l'art 15 e trovando fondamento nel considerando 71. L'effettivo impatto di una tale previsione è stato ampiamente dibattuto[43], considerando sia le eccezioni previste all'art 22, che il fatto che un simil dettato era già presente all'articolo 15 nella Direttiva 46/95/CE[44], ma in quell'occasione aveva trovato una quasi nulla applicazione. Ancora, come verrà analizzato *infra 3*, l'Unione Europea ha ribadito il principio della spiegazione delle decisioni algoritmiche nell'AI Act, con effetti non del tutto convincenti.[45]

1.1.2 Patrimonio

Una delle preoccupazioni che hanno portato all'elaborazione della Risoluzione del Parlamento del 2017[46] è certamente la ricerca di una limitazione della responsabilità in capo a produttori e utilizzatori di sistemi di intelligenza artificiale che operano in modo particolarmente difficile da prevedere: questa limitazione costituisce un passaggio necessario per poter commercializzare tali prodotti, esponendo altrimenti ad un rischio che sarebbe difficilmente sopportato

[40] ANGWIN, 2022
[41] Regolamento 2016/679/UE del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
[42] GOODMAN, FLEXMAN, 2017
[43] SARRA, 2019, WATCHER, et al., 2017
[44] Formulazione che era stata interpretata e recepita in modo differente dai vari stati membri
[45] D'AMBROSIO, 2020
[46] Risoluzione 16 febbraio 2017, cit.

dagli operatori del settore se esposti al modello della responsabilità oggettiva per come è oggi definito.

Una delle soluzioni proposte è la destinazione di un patrimonio nella disponibilità degli enti robotici: questo sarebbe utilizzato per far fronte al risarcimento dei danni che possono essere provocati da questi sistemi. Tale soluzione però può essere implementata indipendentemente dalla costituzione di una soggettività giuridica come quella suggerita dal modello della "personalità elettronica". Ad esempio tali riserve economiche potrebbero essere finanziate da produttori e utilizzatori, andando a costituire fondi comuni o individuali, ed essere quindi ugualmente funzionali per rispondere alle pretese risarcitorie, senza necessità di introdurre novità rivoluzionarie nel sistema normativo[47].

Il patrimonio eventualmente a disposizione permetterebbe di avere uno strumento riconoscibile dai terzi, che potrebbero contare su una somma che saprebbero essere dedicata a far fronte ad eventuali danni, e quindi li potrebbe rassicurare e invogliare ad interagire con i robot.

La più grossa preoccupazione legata ad una tale soluzione è però l'abuso della limitazione di responsabilità. Nel modello delle persone giuridiche in ultima istanza ci sono sempre una o più persone fisiche individuabili, mentre con il riconoscimento di una soggettività piena non si avrebbe più questa possibilità; inoltre la responsabilità per danni non è limitata al valore dell'ente o di un patrimonio definito, come avverrebbe in questo caso. È ravvisabile da più parti uno scenario preoccupante, aggravato dalla potenzialità tipica dei sistemi automatizzati di agire nei confronti di una pluralità molto ampia di soggetti contemporaneamente, ponendo interrogativi in merito alla definizione di questo tipo di rapporti[48].

[47] FINOCCHIARO, 2022
[48] RUFFOLO, 2020, -c

1.1.3 Conclusioni

La proposta di introduzione della personalità elettronica ha perso supporto anche all'interno dello stesso Parlamento Europeo, primo a formalizzare la proposta nell'iter normativo nel 2017. Come verrà presentato *infra,* per affrontare la legislazione delle macchine autonome ci sono state altre proposte che valorizzano istituti già esistenti, come la responsabilità per danno da prodotto. Apparentemente approcci diversi hanno prevalso, intervenendo con soluzioni che valorizzano maggiormente la coerenza sistemica, come evidente dalla combinazione delle più recenti proposte normative europee in tema: Proposta di Direttiva sulla responsabilità per danno da prodotti difettosi[49] e Proposta di direttiva sulla responsabilità da intelligenza artificiale[50].

Il riconoscimento della personalità elettronica ha ricadute che riguardano questioni etico-filosofiche ancora molto dibattute, le quali dovranno necessariamente trovare risposta nei prossimi anni, dal momento che il progresso tecnologico è inarrestabile e le interazioni uomo-macchina saranno sempre più difficili da separare nettamente. Nonostante questo la soluzione proposta non risulta convincente, poiché andrebbe ad aumentare complessità e incertezza sia riguardo l'applicazione sia per via delle ricadute sul sistema, obiettivi opposti rispetto a quelli che si vorrebbero raggiungere normando un fenomeno così impattante[51].

La nuova direzione intrapresa dal legislatore europeo è stata influenzata dalla dottrina, e da pareri provenienti da gruppi di esperti che volontariamente o interpellati dalle istituzioni europee hanno dato pareri tendenzialmente uniformi e contrari all'introduzione della soggettività per i robot, come dalla Lettera Aperta *in nota 38*, dal Parere del Comitato economico e sociale europeo del

[49] Proposta di direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi COM/2022/495 final
[50] Proposta COM/2021/206 final, cit.
[51] CAROCCIA, 2020

maggio 2017[52], dal Rapporto degli Esperti del novembre 2019[53] e dalla Relazione della Commissione del febbraio 2020[54].

1.2 Responsabilità "per difetto di sorveglianza"

Nei sistemi normativi a forte codificazione come quelli dell'Europa continentale è riscontrabile nella legislazione un'impronta proveniente da millenni di esperienza: dalla tradizione romanistica sono discesi attraverso le mediazioni della pandettistica i principi poi impressi nei codici civili ottocenteschi: primo su tutti il *Code Napoleon,* spesso ripreso in massima parte nei paesi francofoni[55] e fonte chiave tanto del codice civile tedesco (BGB)[56] quanto di quello italiano[57].

Tale evoluzione ha dimostrato come nonostante le variazioni delle tecnologie, dei mercati e della sensibilità sociale, attraverso l'interpretazione e residualmente l'analogia, i principi legislativi sono stati declinati in modo sufficientemente ampio da essere applicabili anche in scenari non immaginabili da chi ha scritto il dettato codicistico. Fatto non casuale, dal momento che detti sistemi ad alta codificazione hanno in sé proprio la pretesa di poter mantenere un nucleo stabile di norme a cui far riferimento, lasciando alla normazione speciale la disciplina di tecnicismi e dettagli che necessariamente non possono essere modulabili. La spinta ad aggiornare il codice dunque deve essere una tendenza limitata ai casi strettamente necessari, per via degli imprevedibili effetti sistemici che possono essere provocati da ogni novità[58].

---

[52] Parere del Comitato economico e sociale europeo su «L'intelligenza artificiale - Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società» (2017/C 288/01)

[53] European Commission, Liability for Artificial Intelligence and other Emerging Digital Technologies, November 2019

[54] Commissione europea, Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità, COM/2020/64

[55] ZIMMERMANN, 2006

[56] Bürgerliches Gesetzbuch, 1900

[57] Il primo codice civile italiano risale al 1865, mentre quello attualmente in vigore, del 1942, ne ricalca i contenuti in larga parte. Si evidenzieranno più avanti alcune delle novità introdotte negli artt 2049-2054

[58] RUFFOLO, 2020 -c

Per rispondere ai fenomeni delle nuove tecnologie e della digitalizzazione è stato necessario nell'ultimo quarto di secolo un grande sforzo di aggiornamento degli strumenti normativi, in particolare come adattamento necessario alle spinte comunitarie[59]. Per quanto riguarda il riparto della responsabilità in seguito alla diffusione di sistemi di IA è stata proposta la rivisitazione degli artt 2047-2052 c.c. in alternativa, ma più spesso in combinazione, con la normativa in tema di *product liability.*

Tali articoli disciplinano situazioni riguardanti cose, persone, animali, accomunati da un certo grado di imprevedibilità: dovuto all'intelligenza umana, talvolta all'intelligenza animale, e talvolta alla riconosciuta pericolosità intrinseca in una certa attività.

Gli artt 2047,48, e 2051,52 c.c., disciplinano la responsabilità per il fatto compiuto dall'incapace, mentre i secondi la responsabilità da danni per custodi di cose e proprietari di animali. Diventa così più ardito applicare gli artt 2047,48 c.c. in casi di utilizzo dei sistemi di IA, in quanto manca il richiamo al rapporto strumentale tra chi compie l'azione e chi ne è responsabile. Ulteriore dubbio nell'applicazione di tali articoli ai sistemi in esame, è che il presupposto della responsabilità rimane comunque la colpa, dimostrato dall'esimente accordata dal non aver potuto evitare il danno, e quindi poco affine a soddisfare contemporaneamente le esigenze di produttori ed utilizzatori .

Invece nella seconda coppia è ravvisabile il principio etico del *cuius commoda eius incommoda*: chi gode dei vantaggi di un certo bene, vivente o meno, risponde anche degli svantaggi che questo comporta. Tale normativa appare quindi più accurata per l'estensione ai casi di utilizzo commerciale o personale dei sistemi di AI. La responsabilità qui definita, considerata oggi come oggettiva, per lungo tempo si è basata comunque sul dogma della colpa, che veniva un tempo inquadrata come colpa presunta.

[59]Ne sono un esempio la Direttiva 95/46/CE relativa al trattamento dei dati personali e la Direttiva 2000/31/CE relativa al commercio elettronico nel mercato interno

Ciò che ha permesso l'evoluzione in merito all'interpretazione di tale colpa sono le esigenze derivanti dai nuovi scenari produttivi manifestanti fin dalla prima rivoluzione industriale, ma assecondate solo più tardi. In questo modo il riparto delle responsabilità risulta più equo, e si può fare carico del rischio connesso all'utilizzo di strumentazioni complesse chi effettivamente ha gli strumenti per gestirlo.

Il ricorso agli articoli riguardanti la responsabilità per la condotta altrui artt 2047,48,49 c.c., confluirebbe comunque nel dilemma conseguente l'attribuzione di soggettività "umana" all'IA, con tutte le ricadute non solo sui doveri, ma anche sugli eventuali diritti da accordare ad una tale soggettività, rimandando alle problematiche sollevate dalle ipotesi legate all'introduzione della personalità elettronica[60].

Bisogna quindi capire dove volgere l'attenzione in questa dicotomia, se a norme che riguardano l'autonomia di intelligenze umane, o l'autonomia di intelligenze non umane, tutelate per il loro valore strumentale e non per la loro essenza umana.

Per completare bisogna aggiungere che nei confronti di tutti gli animali, dotati quindi di c.d. "intelligenza animale" la mutata sensibilità è arrivata a superare alcuni limiti antropocentrici, riconoscendo loro diritti per la loro stessa natura di esseri senzienti[61]. Nei confronti invece degli animali da affezione oggi la tutela valorizza anche il legame affettivo che si stabilisce con la persona che ne condivide insieme un pezzo di vita[62]. Quindi anche la trasposizione ai sistemi di IA delle categorie che sono alla base della creazione della legislazione dedicata agli animali, richiede una speciale cautela.

Mancando quindi un riconoscimento generale del grado di "intelligenza" dei sistemi di IA allo stato attuale, ancora (non si sa per quanto) sembrerebbe più appropriato allora volgere lo sguardo alle norme relative allo svolgimento di

[60] cfr. RUFFOLO, 2020 -b
[61] Convenzione europea per la protezione degli animali da compagnia, Consiglio d'Europa, 13 novembre 1987
[62] CAROCCIA, 2022

attività pericolose, disciplinate all'art 2050 c.c., in combinazione con la normativa da *product liability*.

1.3 Responsabilità "da attività pericolosa"

Sviluppo, commercializzazione e utilizzo di sistemi di IA dotati di elevata autonomia configurano secondo alcuni una situazione ascrivibile all'ipotesi di responsabilità da attività pericolosa come normato all'art 2050 c.c..

Così come si è riscontrato nell'autonomia di azione dei sistemi di IA una analogia con l'autonomia di animali e cose che per loro natura sono seagenti, tale assunzione è stata estesa a cose inerti, le quali in relazione alle circostanze in cui sono utilizzate possono configurare la moderna figura dell'attività pericolosa[63].

Tale orientamento è sopravvenuto anch'esso, come quello che ha guidato l'elaborazione dell'art 2051 c.c., per far fronte alla moderne dimensioni dei fenomeni produttivi in un periodo in cui la normativa in merito alla responsabilità da prodotto difettoso era ancora assente: solo con la Direttiva 85/374/CEE[64] c'è stato un adeguamento in materia. Le attività rientranti nel dettato dell'art 2050 c.c. devono come detto configurarsi come pericolose: possono essere tipizzate, ma è sufficiente che le circostanze in cui avviene l'attività la rendano pericolosa.

Quando si tratta di attività produttive, queste norme producono in capo ai produttori l'obbligo di verificare tutte le misure da adottare per contrastare il rischio intrinseco di cagionare danni derivante dalle proprie attività: se il difetto rimane non conoscibile allo stato delle conoscenze al momento della messa in commercio del prodotto, o le circostanze in cui questo viene utilizzato rimangono imprevedibili, la disciplina rientra nel c.d. rischio da sviluppo. Teorizzazione che secondo alcuni deroga all'ampiamente applicato in sede

[63] RUFFOLO, 2020 -c

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

europea principio di precauzione[65], che verrà visto più in dettaglio in merito alla normativa propriamente da *product liability*.

Già dall'assetto definito nel Codice del 1942 è stato possibile giungere al superamento della presunzione di colpa come da tradizione in capo al produttore, a favore invece della presunzione di responsabilità in capo allo stesso, riconoscendo l'oggettività della responsabilità che ne dovrebbe scaturire in caso di danno .

L'onere della prova in capo al danneggiato divenne decisamente più agevole, dovendo questo dimostrare solamente il danno, e lasciando al danneggiante l'onere di provare di aver adottato tutte le misure necessarie ad evitare il danno.[66]

Se è vero che appare necessario per il mercato digitale un aggiornamento della normativa in merito a tale onere della prova, per via delle difficoltà date dalla complessità degli strumenti, tanto più risulta non del tutto adeguato per sistemi di IA in cui potrebbe non essere mai possibile conoscere il meccanismo che ha portato ad una certa scelta.

Secondo alcuni dunque l'utilizzo di taluni sistemi di IA potrebbe rientrare in questa disciplina, e sarebbe parzialmente adeguata per rispondere alle pretese risarcitorie di coloro che subiscono i danni derivanti dall'uso di tali sistemi.

[65] AMIDEI, 2020 -b
[66] RUFFOLO, 2020 -c

2. Responsabilità "da prodotto difettoso": Proposta di direttiva per la responsabilità extracontrattuale dell'IA

Per far fronte alle moderne dimensioni produttive la legislazione si è evoluta nella direzione che permettesse di superare la responsabilità soggettiva, la quale si basa su una concezione etica, in cui l'elemento della colpa viene bilanciato con sanzioni che hanno sia funzione dissuasiva che retributiva; a favore di una responsabilità oggettiva, in cui lo scopo perseguito è il riparto del costo economico-sociale dei danni derivanti dai prodotti stessi, o a volte dalla produzione dei beni, tra coloro che hanno la miglior capacità di risponderne: i produttori stessi.

Partendo da tale chiara impostazione, nel caso della commercializzazione di sistemi di IA, o che integrano tecnologie di intelligenza artificiale l'imputazione della responsabilità in caso di danni è più complicata: le difficoltà stanno nel determinare l'elemento da considerare "difettoso", il nesso causale con il danno, e dunque chi nella catena dei soggetti responsabili debba rispondere di tali danni in sede risarcitoria.

2.1 Responsabilità "da prodotto difettoso"

La normativa più definita in tema di responsabilità da prodotto difettoso è stata introdotta nel sistema normativo italiano come adeguamento alla Direttiva 85/374/CEE[67] con norme che sono poi confluite nel Codice del consumo del 2005[68].

Le misure riguardano ogni bene mobile, e la difettosità consiste come da art. 6 nel "non offrire la sicurezza che ci si può legittimamente attendere tenuto conto di tutte le circostanze". La definizione di tali circostanze sarà oggetto di maggior approfondimento relativamente alla Proposta di aggiornamento della Direttiva da prodotto difettoso[69].

[67] Direttiva sulla responsabilità per danno da prodotti difettosi, cit
[68] Decreto Legislativo 6 settembre 2005, n. 206 - Codice del consumo
[69] Proposta COM/2022/495 final, cit

La Direttiva del 1985 ha svolto un'ottima funzione nel rispondere alle esigenze di responsabilità da prodotto sorte in fase di armonizzazione delle normative nazionali, arrivando a definire un perimetro entro cui gli attori commerciali potevano confidare in una certa uniformità legislativa.

Per comprendere come lo strumento della Direttiva lasci comunque spazio ai singoli Stati membri di differenziarsi all'interno dell'ordinamento nazionale, si può notare come "il nostro Paese abbia introdotto il "rischio da sviluppo" tra le esimenti della responsabilità oggettiva, oggetto questo di ampia dottrina e giurisprudenza[70]. In questa scelta il legislatore ha seguito altri Stati per esigenze di politica del diritto, in modo da non creare uno svantaggio competitivo alle aziende italiane"[71].

La Direttiva ha introdotto un alleggerimento dell'onere della prova in capo al danneggiato, dovendo questo solamente dimostrare il danno, il difetto da cui il danno è derivato, e il nesso causale tra il difetto e il danno[72], senza dover dimostrare la colpa in capo al produttore. Tale impostazione ha permesso una grande evoluzione nella tutela del consumatore.

Fin dall'inizio del XXI secolo però la Direttiva è stata messa alla prova dall'insorgenza dei servizi digitali, diventati poi sempre più presenti nella quotidianità di tutti, e progressivamente anche in ogni processo aziendale.

Per sopperire ai quesiti che sono sorti nel corso degli anni, per esempio riguardo la loro categorizzazione come "prodotti", o come si potesse individuare la difettosità, l'Unione Europea ha finalmente colmato le lacune attraverso una strategia di ampio raggio: l'UE vuole essere leader mondiale nella definizione degli approcci normativi nei confronti delle nuove tecnologie, costruendo un

[70] si menzionano come riportate in D'AMBROSIO, 2022, p.59, le questioni di sovrapposizione o alterità delle tutele tra quelle derivanti dalla Direttiva sui prodotti difettosi, e quelle derivanti invece dalle attività pericolose (art. 2050 c.c.). La Corte di Giustizia europea sostiene la preminenza della legislazione europea nel confronto tra la legge di recepimento della Direttiva e altra legislazione nazionale mentre la giurisprudenza italiana ha riconosciuto il cumulo tra azione extracontrattuale, ai sensi del Codice del consumo, e l'azione contrattuale, nei casi in cui tra produttore e danneggiato esista anche un rapporto contrattuale. In aggiunta la previsione del rischio da sviluppo è stata ridotta in via giurisprudenziale alle sole ipotesi di caso fortuito, a causa della severità dell'onere della prova richiesto al produttore in fase processuale, andando comunque secondo alcuni ad intaccare il principio di precauzione perseguito in sede unionale.

[71] D'AMBROSIO, 2022, p. 56

[72] Direttiva 85/374/CEE, art. 4

framework che rispetti i principi etici, democratici, di garanzia dei diritti dei cittadini europei, come ribadito da Parlamento e Consiglio[73].

Gli elementi di tale strategia sono il *Digital Services Act*, il *Digital Markets Act* e l'*AI Act*, in combinazione con le proposte di aggiornamento della Direttiva sulla responsabilità da prodotti difettosi, in cui troviamo previsioni specifiche per i prodotti digitali, la quale va integrata anche dalla c.d. *AI liability directive*[74], in cui si disciplina la responsabilità nel caso di danni esclusi dalla Direttiva generale ma derivanti dai prodotti di intelligenza artificiale o che integrano algoritmi di intelligenza artificiale.

2.2 Revisione della direttiva sulla responsabilità per danni da prodotto difettoso

La proposta di revisione della direttiva sulla responsabilità da prodotto difettoso arriva dopo la constatazione da più parti che dopo quasi 40 anni di Direttiva 85/374/CEE sia necessario un aggiornamento, in particolare in merito alle esigenze sorte riguardo i prodotti digitali e i nuovi modelli produttivi legati all'economia circolare. Tali rilevazioni sono state riaffermate nella Relazione[75] alla proposta di revisione della direttiva, focalizzandosi sulle problematiche relative all'estensione della tutela risarcitoria; sulle categorie definitorie da adeguare per i prodotti digitali; e sull'ulteriore alleggerimento dell'onere della prova.

Come detto *supra* le novità portate da questa direttiva si inseriscono in uno schema più ampio che mira ad un maggiore allineamento nella legislazione in merito alla sicurezza dei prodotti: tra i regolamenti in fase di approvazione o già

[73] Consiglio europeo, riunione straordinaria del Consiglio europeo (1 e 2 ottobre 2020) – Conclusioni, EUCO 13/20, 2020; Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL))

[74] Proposta COM/2021/206 final, cit.

[75] Relazione alla Proposta di direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danni da prodotto difettoso COM/2022/495 final, pp. 1-2

approvati troviamo la c.d. Legge sull'Intelligenza Artificiale[76], il regolamento sui prodotti macchina[77] e il regolamento sulla sicurezza generale dei prodotti[78].

Ognuna di queste iniziative va a colmare quel divario che si è creato negli anni con l'evoluzione da prodotti "tradizionali" in prodotti e mercati digitali. Vengono così definiti nuovi standard di sicurezza e *cyber-security*, nuovi obblighi in capo a produttori e venditori, nuove verifiche di compatibilità con le leggi europee per prodotti che provengono dall'esterno dei confini dell'UE.

Tra le definizioni che troviamo aggiornate nella proposta di direttiva emergono le tre principali: la nozione di prodotto, quella di danno e infine di prodotto difettoso.

Per quanto concerne la definizione di prodotto, ora include esplicitamente tutti i *software*, tra cui i prodotti che fanno uso di intelligenza artificiale, anche se integrati in altri prodotti. Interessante rilevare come dalla consultazione dei portatori di interesse fosse emersa sì la necessità di riconoscere il *software* come prodotto, ma di farlo attraverso "orientamenti non vincolanti anziché mediante una revisione legislativa della direttiva sulla responsabilità per danno da prodotti difettosi"[79].

La definizione di "danno" invece risulta ampliata in modo sensibile: oltre alle perdite materiali derivanti dalla distruzione della proprietà, dalla morte e da lesioni personali, vengono compresi innovativamente da una parte i danni psicologici, dall'altra la perdita o corruzione di dati non usati esclusivamente a fini professionali[80]. Si capisce come il cambiamento nella sensibilità sociale, non solo le evoluzioni tecnologiche, abbiano influenzato un tale aggiornamento. Per quanto concerne le misure riguardo i dati c'è da rilevare ancora una volta come gli operatori economici fossero contrari ad una tale previsione, in quanto

[76] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, cit.
[77] Proposta di regolamento del Parlamento europeo e del Consiglio sui prodotti macchina, COM(2021) 202 final
[78] Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla sicurezza generale dei prodotti, COM(2021) 346 final
[79] Relazione alla Proposta di direttiva del Parlamento europeo e del Consiglio sulla responsabilità per danni da prodotto difettoso COM/2022/495 final, p. 9
[80] Proposta COM/2022/495 final, cit. art. 4, comma 1°, n.6

valutarono come sufficiente il ricorso alle misure previste dal GDPR[81], mentre il resto di portatori di interessi come ONG e amministrazioni pubbliche hanno visto favorevolmente tale novità.

Per definire un prodotto difettoso fin dalla Direttiva del 1985 erano stati definiti dei requisiti, che andavano a costituire il "test di difettosità" del prodotto all'art.6: con gli aggiornamenti alla direttiva il test è stato notevolmente ampliato ed adeguato alle nuove esigenze.

Vengono comprese ora non solo la presentazione del prodotto, ma anche le istruzioni per l'uso, l'installazione e la manutenzione; oltre all'uso, anche l'abuso prevedibile in relazione alle aspettative degli utenti cui è destinato il prodotto.

Relativamente ai prodotti digitali le previsioni più esplicite dell'art. 6 riguardano la valutazione 1) della possibilità di apprendimento successivo alla diffusione del prodotto 2) degli effetti di altri prodotti che possono essere utilizzati insieme al prodotto: riferimento questo alla connettività dei dispositivi IoT[82] 3) dei requisiti di *cyber-security* rilevanti per la sicurezza del prodotto.

All'art. 7 la proposta di direttiva garantisce al consumatore come punto di contatto primario quello del fabbricante del prodotto e della componente causa del difetto, lasciando poi a questi l'onere eventuale di dimostrare che la responsabilità del difetto non è propria, o non esclusivamente propria. Con il connesso e più rilevante dal punto di vista economico riparto successivo del risarcimento, obbligando all'art. 11 gli Stati membri ad attuare misure per distribuire solidalmente la responsabilità quando più operatori economici siano responsabili per uno stesso danno.

[81] Regolamento 2016/679/UE del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, cit

[82] i dispositivi che rientrano nell'Internet of Things sono prodotti con sensori, collegati ad una rete di dispositivi, non necessariamente online, che offrono funzionalità aggiuntive grazie all'acquisizione, elaborazione o trasmissione di dati

2.2.1 Modifiche a prodotti: economia circolare e prodotti digitali

Infine ampio il favore tra tutti i portatori di interesse per l'attribuzione di responsabilità a chi in seguito a "modifiche al di fuori del controllo del fabbricante originario" immette nel mercato prodotti che risultano difettosi, venendo considerato il risultato di tale elaborazione al pari di un nuovo prodotto[83]. A prima lettura tale misura sembrerebbe tutelare i produttori dei prodotti originali dalle responsabilità per le modifiche fisiche apportate successivamente da altre persone, come accade nei nuovi modelli produttivi dell'economia circolare[84]. Più avanti però viene specificato che, quando questa previsione riguarda prodotti digitali, e quindi tra le "modifiche" rientrano anche aggiornamenti del *software* o variazioni dovute alla capacità di auto-apprendimento e decisione autonoma dei sistemi di intelligenza artificiale, la misura acquisisce tutt'altra rilevanza.

In questo modo in linea teorica si responsabilizzano tutti i soggetti che fanno parte della catena del valore dei prodotti digitali: dallo sviluppatore, passando per l'addestratore dell'algoritmo di intelligenza artificiale, fino al distributore finale. In pratica però l'individuazione di tali soggetti può risultare pressoché impossibile. Infatti la direttiva prevede nuove misure per favorire la divulgazione di informazioni che possono aiutare ad individuare l'elemento difettoso.

Il legislatore però è andato oltre, consapevole della difficoltà di individuare l'elemento difettoso, necessario di regola per richiedere il risarcimento e dimostrare il nesso causale: l'onere della prova infatti è stato ancora alleggerito, inserendo in determinati casi considerabili troppo complessi, proprio come quelli di prodotti che integrano algoritmi di intelligenza artificiale, una doppia presunzione: sia di difettosità che del nesso causale con il danno[85]. Risulta così

[83]Proposta COM/2022/495 final, cit., considerando 29

[84] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Un nuovo piano d'azione per l'economia circolare - Per un'Europa più pulita e più competitiva" (COM(2020) 98 final)

[85]Proposta COM/2022/495 final, cit., art. 9

chiara la volontà di rispondere alle difficoltà di individuazione del difetto in caso di prodotti digitali.

2.2.2. Conclusioni

La disciplina rientrante in questa normativa risponde esclusivamente ai danni da prodotto difettoso contro persone fisiche sorti in rapporti extracontrattuali, dunque non può rispondere a tutte le esigenze che possono nascere dai danni da prodotti che integrano tecnologie di intelligenza artificiale, come nel caso di danni che violano diritti fondamentali, o danni che avvengono nei confronti di persone giuridiche. Per rispondere a queste esigenze ci sono primariamente gli ordinamenti nazionali, ma da una parte l'*AI Act*, e dall'altra la *AI Liability Directive*, cercano di offrire un quadro uniforme di riferimento.

2.3 Proposta c.d. *AI Liability Directive*

Il campo di intervento della Proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale[86] sono "le domande di risarcimento del danno causato da un sistema di IA nel quadro di azioni civili di responsabilità extracontrattuale, qualora tali azioni siano intentate nell'ambito di regimi di responsabilità per colpa, ossia, in particolare, regimi che prevedono la responsabilità legale di risarcire i danni causati da un'azione o un'omissione intenzionalmente lesiva o colposa"[87].

La direttiva nasce dalla preoccupazione che a partire dalle strategie nazionali per far fronte alle novità portate dalle tecnologie di intelligenza artificiale, gli Stati membri variassero la propria legislazione in modo disomogeneo, causando incertezza giuridica che spaventa le aziende del settore, comportando un

[86] Proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione COM/2021/206 final

[87] Relazione alla Proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale COM/2021/206 final, p.13

rallentamento negli investimenti e quindi lo sviluppo legato a questa tecnologia. In questo modo invece da una parte gli attori economici possono valutare con maggior precisione il proprio livello di esposizione al rischio, e i soggetti danneggiati possono accedere a strumenti più efficienti per portare a termine le proprie azioni di risarcimento del danno.

L'intervento normativo è stato approvato in congiunzione con l'aggiornamento della direttiva sulla responsabilità per danno da prodotti difettosi, e va ad intervenire in modo mirato sulle disposizioni riguardo l'onere della prova. Senza dunque influenzare definizioni riguardo la responsabilità civile che hanno grande variabilità tra stati e che ricoprono un ruolo cruciale in ogni ordinamento giuridico, come quella di responsabilità, nesso di causalità o danno.

L'attenzione dedicata all'onere della prova deriva proprio dalle problematiche intrinseche nella tecnologia coinvolta: l'alto livello di conoscenza tecnica necessario per affrontare la complessità del funzionamento della tecnologia, l'opacità che caratterizza la tecnologia, e a valle di tutto questo l'autonomia che questi sistemi manifestano[88].

Gli strumenti giuridici messi così a disposizione dunque facilitano l'onere della prova per i soggetti danneggiati.

Nel primo caso, per sistemi di IA "ad alto rischio" come definiti nel regolamento sull'intelligenza artificiale[89] il soggetto danneggiato, in seguito all'aver fornito fatti e prove per sostenere la domanda di risarcimento, deve poter accedere agli elementi che possano costituire una prova. Gli Stati membri devono quindi predisporre dei meccanismi che permettano da una parte l'accesso a questi sistemi, ma che dall'altra tutelino i dati personali ed i segreti commerciali.

[88] D'ALFONSO, 2022

[89] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

Il complicato bilanciamento tra gli interessi delle parti dovrà sottostare ai principi di necessità e proporzionalità come da Direttiva 2016/943/UE, rispettando gli ordinamenti nazionali ed europei, e dovendo essere valutati di volta in volta dai giudici che dovranno disporre gli ordini di divulgazione delle informazioni.

Dall'altra parte viene offerta in alcune circostanze la presunzione relativa all'onere della prova del nesso di causalità tra l'*output* o il mancato *output* del sistema di IA e la colpa del convenuto. Il ricorrente dovrà comunque portare elementi a sostegno per poter accedere a tale presunzione.

Gli organi giurisdizionali potranno ammettere la presunzione dell'esistenza del nesso di causalità solo in presenza di determinate condizioni: un'inosservanza colposa di obblighi di diligenza posti a prevenzione del danno in oggetto; la probabilità che nel caso specifico tale inosservanza abbia influito sull'*output* o il mancato *output;* che l'*output* o il mancato *output* abbia provocato il danno.

Per i sistemi di IA "ad alto rischio" invece è previsto un regime differenziato: la presunzione di causalità è limitata al mancato rispetto degli obblighi definiti nell'*AI Act* rispettivamente per "fornitori" e per "utenti".

Per i sistemi di IA non ad alto rischio, e quindi non soggetti alla normativa dell'*AI Act,* la presunzione si applica solo se viene ritenuto dall'organo giurisdizionale nazionale eccessivamente difficile per l'attore dimostrare l'esistenza del nesso di causalità.

Nel caso in cui la domanda di risarcimento sia nei confronti di un soggetto che ha fatto un uso non professionale del sistema di IA, la presunzione del nesso di causalità si applica solamente se il convenuto ha interferito materialmente con le condizioni di funzionamento del sistema di IA, o se aveva l'obbligo ed aveva le capacità di determinare le condizioni di funzionamento e non l'ha fatto.

La presunzione del nesso di causalità può sempre essere confutata dal convenuto.[90]

L'introduzione di una presunzione di causalità così ampia sembra ben rispondere alle esigenze di tutela di soggetti deboli che non possono tecnicamente condurre in autonomia, o se si dovessero servire di altri professionisti sarebbe troppo oneroso, l'analisi dei sistemi di intelligenza artificiale necessari ad individuare gli elementi di prova.

[90] Proposta COM/2021/206 final, cit., art 4

3. *AI Act*: una panoramica

Abbiamo visto come il percorso per l'inserimento di una legislazione aggiornata per far fronte alle sfide delle nuove tecnologie, e dell'intelligenza artificiale nello specifico, sia parte di un processo di proposte e leggi dipendenti le une dalle altre che cercano di rispondere a tutte le nuove esigenze normative, tanto nelle previsioni imperative rivolte a cittadini, imprese e pubbliche amministrazioni, quanto nelle definizioni.

A livello europeo il primo passo nella direzione di fornire strumenti adeguati alle esigenze derivanti dall'IA è stato la definizione di linee guida che garantissero lo sviluppo di un'intelligenza artificiale sicura, etica e rispettosa dei diritti dei cittadini, L'obiettivo dichiarato è quello di normare un fenomeno dal potenziale vastissimo, imprimendo i principi europei di democrazia e legalità: ponendosi come pioniera l'Unione punta a replicare il c.d. *effetto Bruxelles*[91], esplicitando l'intenzione di veder replicato lo stesso approccio normativo in altre aree del mondo, come è stato in parte con il GDPR[92].

Tale approccio orientato ad una stretta normazione, è risultato agli occhi dei competitor internazionali, ovvero Stati Uniti e Cina, come una risposta spaventata e di chiusura nei confronti di una tecnologia che ha il potenziale di impattare ogni ambito della vita. Si cerca di tutelare dai potenziali effetti negativi stringendo briglie, su una tecnologia che ancora non si conosce bene, invece di proporre una serie di regole generali che permettano uno sviluppo libero da eccessivi fardelli burocratici[93].

Oltre ad aggiornare il sistema giuridico nella capacità di rispondere sul piano civile con misure adeguate, l'Unione Europea ha ravvisato la necessità di fornire un *framework* che definisca gli obblighi cui i fornitori e i *deployer*[94] di sistemi di

[91] BRADFORD, 2020
[92] Regolamento 2016/679/UE del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, cit
[93] FINOCCHIARO, 2022
[94] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale), art. 3, 1° comma, n. 4

IA devono sottostare per poter interagire con i cittadini europei: la soluzione individuata è stato l'approccio *risk based* dettato nel Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale (c.d. *AI Act*)[95].

In seguito ad una serie di interventi che hanno dato o stanno dando forma ad un quadro generale a livello europeo, di seguito saranno presentate alcune integrazioni dell'*AI Act* con la normativa vigente, le autorità competenti nazionali ed europee e la legge sulla responsabilità civile extracontrattuale.

3.1 Approccio *risk based*: una soluzione definitiva?

La misura più adatta per fornire una legislazione "alta e armonizzata"[96] in tema di intelligenza artificiale è stata ravvisata dal legislatore europeo nella definizione di livelli di rischio relativi alla sicurezza e ai diritti fondamentali, entro cui inserire i sistemi di intelligenza artificiale in uso nell'UE.

La definizione di tali livelli di rischio si va ad inserire in quella delicata sinergia tra *issues of liability* e *issues of permittance* che va ad offrire idealmente un quadro completo per la sicurezza dei prodotti all'interno dei confini dell'Unione. Entro tale spazio le imprese possono agire avendo chiari tanto i rischi legati alle responsabilità che corrono compiendo la loro attività, quanto i requisiti di sicurezza da rispettare, gli *standard* da applicare, le certificazioni da conseguire, la documentazione da produrre per garantire una completa applicazione dei principi della *product safety*[97].

Sono stati definiti quattro livelli di rischio a seconda delle finalità per cui saranno impiegati i sistemi: *inaccettabile*, a cui fanno però seguito una serie di eccezioni ampiamente discusse; *rischio alto*, principale oggetto degli obblighi della normativa; *rischio specifico di trasparenza*, e infine *rischio basso*, per il

[95] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, cit.
[96] D'ALFONSO, 2022, p.39
[97] AMIDEI, 2020, -a

quale è prevista l'applicazione volontaria a codici di condotta da parte dei *provider*.

Il legislatore ha deciso di qualificare invece in modo diverso i sistemi di intelligenza artificiale per finalità generali: alla base del sistema di IA per finalità generali c'è un modello di IA per finalità generali. La valutazione di rischio verrà effettuata su tale modello: potrà essere classificato "a rischio sistemico" secondo certi parametri che riguardano la capacità di impatto[98].

Nel caso in cui il rischio sistemico venga rilevato, vengono applicati diversi obblighi relativi alla comunicazione alle autorità, dovendo il fornitore di tale modello comunicare direttamente alla Commissione la rilevazione di tale requisito. Viene prevista anche la possibilità a favore del fornitore di argomentare come il proprio modello non sia a rischio "sistemico" nonostante il soddisfacimento dei requisiti che lo classificherebbero come tale, in luce di caratteristiche specifiche legate al modello. C'è una presunzione di rischio sistemico per modelli di IA per finalità generali qualora l'art. 51, 2° comma, sia soddisfatto.

Tali sistemi richiedono di applicare un modello di *governance* differenziato. La scelta appare ragionevolmente giustificata, dato il massiccio utilizzo che ne è già stato fatto da quando sono stati introdotti ed il conseguente impatto che hanno e potranno avere nella società.

Resta il problema dei requisiti con cui è stato identificato un sistema a rischio "sistemico". I requisiti sono stati inseriti nel testo, e saranno modificabili tramite atti delegati della Commissione per adeguarli allo stato dell'arte della tecnologia. Si rileva come la capacità di reazione dell'istituzione probabilmente non sarà sufficiente a soddisfare gli obiettivi di tutela che la norma persegue[99].

[98] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, art. 4, 1° comma, 64. Vengono valutate le modalità di *training* dei dati, le competenze dimostrate in ambiti diversi, la capacità di calcolo quantitativamente rilevabile, la potenzialità di diffusione che l'utilizzo di tale modello può raggiungere.
[99] NOVELLI, et al., 2024

La definizione di intelligenza artificiale adottata è tanto ampia da includere ogni tipo di applicazione che integra intelligenza artificiale afferente a qualsiasi ambito, da quello medico a quello finanziario. Il testo suggerisce che la maggior parte dei sistemi di IA saranno classificati a rischio "basso", e che quindi gli oneri del Regolamento per i sistemi a rischio "alto" non saranno pervasivi in ogni attività.

Oltre alle applicazioni vietate, facili da individuare grazie all'elenco dell'art. 5; la valutazione del livello di rischio "alto" viene effettuata in base ai criteri indicati all'art. 6 comma 1°, dove vengono indicati i sistemi di IA indipendentemente dai prodotti indicati alle lettere a) "*componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I*" e b) "*il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è 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*" dello stesso comma, o i sistemi come da allegato III, il quale potrà però essere integrato ed aggiornato dalla Commissione con atti delegati reagendo alle rilevazioni del mercato[100].

I maggiori obblighi fanno riferimento alla fase precedente all'immissione nel mercato del sistema di IA, e così si è previsto che non solo il fornitore, o il *provider*, siano responsabili della verifica dei requisiti, ma che anche l'importatore e il distributore possano essere destinatari di obblighi di verifica dei requisiti, redazione di documentazione, segnalazione alle autorità in caso di rischi per la salute, la sicurezza o la tutela dei diritti fondamentali delle persone.

Seguendo il *principio di proporzionalità* che investe tutta la normativa in esame, viene prevista in particolare la traslazione in capo a *chiunque modifichi in*

[100] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale), art. 6

modo sostanziale il sistema o i suoi fini degli obblighi in capo al *fornitore* originale, e quindi la cessazione per questo della responsabilità[101].

Nella fase di applicazione della norma sarà allora necessario specificare i requisiti in base ai quali le modifiche vengono ritenute "sostanziali". Tale dettaglio dovrà essere fornito attraverso la compilazione di linee guida interpretative, le quali dovrebbero anche chiarire quali sono i metodi di *assessment.* Ci sono ancora grossi vuoti da colmare prima di poter applicare il Regolamento nella sua interezza, confidando nelle misure correttive e integrative già previste nel testo[102].

Altro punto in cui il legislatore europeo non ha differenziato è l'imposizione di obblighi indipendentemente dalla dimensione dell'impresa fornitrice: è chiaro che tutti gli oneri documentali che derivano da questa normativa saranno maggiormente gravosi in proporzione, per le PMI, le quali probabilmente in gran parte non riusciranno a sopportare la pressione burocratica ed economica così introdotta. Dovranno allora prevedersi misure ancora più incisive per semplificare le procedure affinché non venga meno la spinta innovativa che può arrivare da piccole imprese, o nascenti, quali sono per natura le *start-up*: grande motore dell'innovazione legata al digitale[103].

Alcuni propongono di rendere minore il carico burocratico in capo ai *provider* prevedendo dei possibili cambiamenti ai sistemi di IA in una fase precedente l'immissione nel mercato, così se in un secondo momento vengono messe in pratica tali modifiche, non si deve rifare tutto il procedimento di certificazione. Si riprenderebbe in questo modo il metodo in uso per macchinari medici: si stila un documento programmatico con le possibili modifiche e le relative verifiche, compiute prima dell'immissione del prodotto nel mercato.

Si va così ad ampliare il fascicolo degli obblighi documentali in una fase preventiva, ma si offre una via per semplificare l'introduzione di modifiche, che

[101] *Ibidem*, art. 25
[102] NOVELLI, et al. 2024
[103] *Ibidem*

in particolare nel caso di macchinari con interfacce digitali o connessione con la rete, sono necessarie: basti pensare all'aggiornamento del *software* per prevenire minacce informatiche non conosciute al momento dell'immissione del prodotto nel mercato[104].

3.2 Impatto sistemico dell'*AI Act*

Il precedente maggiormente rilevante in sede europea che ha adottato il modello *risk based* è il Regolamento generale sul trattamento dei dati personali[105]. Con la differenza però che nel regolamento del 2016 la valutazione del rischio è *bottom-up*: in capo al titolare del trattamento dei dati, il quale deve "attuare le misure tecniche e organizzative adeguate" in base all'applicazione, finalità e contesto del trattamento. L'impostazione dell'*AI Act* invece è *top-down*: prevedendo le *griglie* indicate dal legislatore, in cui poi i fornitori di sistemi di IA dovranno far rientrare le applicazioni di volta in volta sviluppate.

Viene ancora una volta in luce il problema di definire limiti troppo stretti per normare una nuova tecnologia ancora in fase di forte sviluppo, andando a creare categorie valide nel momento in cui vengono formalizzate, ma che rischiano di diventare velocemente obsolete.

Basti pensare al periodo di tre anni che intercorre tra l'approvazione e l'entrata in vigore integrale del regolamento: previsione necessaria, data l'entità degli obblighi introdotti, ma che evidenzia ancor di più il ritardo rispetto al passo dimostrato dall'evoluzione tecnologica.

Per rimediare a questo problema si rimanda all'applicazione del principio della neutralità tecnologica, che in sede internazionale prevale, ed è in verità anche già stato applicato dal legislatore europeo[106]. Sono necessari principi

[104] *Ibidem*

[105] Regolamento 2016/679/UE del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, cit

[106] cfr. FINOCCHIARO, 2022 *ad esempio nel Regolamento 2014/910/UE, il c.d. Reg. e-IDAS, allorché ha introdotto delle definizioni di firma elettronica e firma elettronica avanzata non riferite a specifiche tecnologie.*

chiari, entro cui le aziende possano operare conoscendo gli obiettivi che la norma giuridica vuole perseguire, ma avendo la possibilità di individuare in maggiore libertà la soluzione tecnica per perseguirli[107].

In continuità con le linee guida etiche originariamente delineate nel 2019 dal Gruppo di Esperti per l'IA, la declinazione del principio antropocentrico di *human agency and oversight*[108] è riscontrabile nell'obbligo di predisporre i sistemi in modo che abbiano documentazione comprensibile agli utenti, e la registrazione automatica degli eventi (*log)*[109], ovvero delle operazioni che vengono svolte dal sistema, per poter tenere traccia dei processi decisionali delle macchine.

Sul piano della responsabilità civile il rapporto tra il Regolamento 2024/1689/UE e la Proposta di direttiva sulla responsabilità civile extracontrattuale da IA[110] è obbligato, in quanto le definizioni adottate dal Regolamento sono espressamente richiamate nella Proposta di direttiva.

In particolare viene in rilievo sia la definizione di intelligenza artificiale, che la classificazione di "sistema di IA ad alto rischio". L'alleggerimento dell'onere della prova a favore del danneggiato di un sistema di IA è legato agli obblighi documentali in capo ai *provider* dei sistemi di IA ad alto rischio. Si capisce così il rilievo della prescrizione di produrre documentazione relativa all'attività dei sistemi in modo che sia comprensibile agevolmente anche dagli utenti, e non solo dagli operatori specializzati.

Allo stesso modo tale documentazione acquisisce rilievo in merito all'aggiornamento della Direttiva da *product liability*[111]*,* che in seguito agli aggiornamenti relativi proprio alle nuove tecnologie e in particolare

Non può dirsi, invece,"tecnologicamente neutra" la nozione di firma elettronica qualificata, collegata a livelli di sicurezza predeterminati.

[107] FINOCCHIARO, 2022

[108] principio esposto negli *"Orientamenti Etici per un'IA Affidabile", Gruppo Indipendente di Esperti ad Alto Livello sull'intelligenza Artificiale,* 8 aprile 2019

[109] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale), art. 12 comma 1°,

[110] Proposta COM/2021/206 final, cit

[111] Proposta COM/2022/495 final, cit

all'intelligenza artificiale, è intesa per far fronte ad una varietà di domande di risarcimento per danno da prodotto difettoso.

Appare così ben strutturato il quadro per una vasta applicazione del principio di *accountability*, con la declinazione di una nozione di responsabilità civile più ampia, integrando le istanze di responsabilizzazione di tutti i soggetti presenti nel ciclo di vita dei sistemi digitali[112].

3.3 Pratiche di IA vietate

Le previsioni relative ai sistemi di IA vietati hanno suscitato un grande dibattito, in particolare relativamente alle eccezioni previste. Il Regolamento, in quanto tale, si rivolge anche agli Stati membri e alle amministrazioni degli stessi.

Come da sempre nel bilanciamento tra le previsioni relative alla salvaguardia dell'integrità della sfera giuridica dei cittadini, ci sono le ragioni di polizia e di gestione delle emergenze di cui sono investiti gli apparati statali. Così nonostante ci fossero voci che spingevano per mantenere fermo il divieto di applicare sistemi di IA all'identificazione biometrica in tempo reale in spazi aperti al pubblico, sono state previste delle eccezioni relativamente alla persecuzione di determinati reati gravi.

Data la natura problematica dell'utilizzo di tale tecnologia, tra cui il rischio di essere abusata per fini politici, per attuare controllo di massa, o per altre violazioni dei diritti dei cittadini, l'ammissibilità dell'uso in determinate circostanze viene accettata solamente in concomitanza con il rispetto di ulteriori obblighi in capo alle autorità che ne facciano uso.

Restano vietati in ogni caso invece sistemi di IA che sfruttano le vulnerabilità delle persone; per creare sistemi di punteggio sociale: per attività di polizia predittiva individuale; per la raccolta non mirata di materiale da Internet o CCTV al fine di ampliare banche dati; per il riconoscimento delle emozioni sul

[112] D'AMBROSIO, 2022

luogo di lavoro o negli istituti di istruzione; categorizzazione biometrica per dedurre informazioni personali sensibili[113].

3.4 Governance a livello unionale e nazionale

Tra le misure introdotte dall'*AI Act* ci sono anche le previsioni riguardanti le autorità che dovranno monitorare e governare l'applicazione del Regolamento. Sono state designate per certe funzioni autorità nazionali ed unionali già esistenti, come per alcuni aspetti di vigilanza del mercato; mentre per altre funzioni è stata predisposta la costituzione di nuove autorità.

Già il 24 gennaio 2024 la Commissione ha istituito l'Ufficio per lA[114], che sia fungerà da interlocutore per le altre istituzioni ed autorità che si occuperanno di IA, sia dovrà supportare l'elaborazione di atti delegati della Commissione. L'Ufficio dunque sarà il fulcro per la *governance* dell'IA a livello europeo, in quanto si occuperà dell'armonizzazione di tutto il nuovo *framework* europeo sull'IA, tra cui l'aggiornamento della direttiva sulla *product liability* e la direttiva sulla responsabilità dell'IA in arrivo.

Nelle sue attività l'Ufficio dovrà fare riferimento alle raccomandazioni che arriveranno da altri due organi: il gruppo degli esperti scientifici indipendenti (*Scientific Panel*) e il forum consultivo (*Advisory Forum*). Questi organi supporteranno nell'elaborazione degli *standard* per individuare i livelli di rischio dei sistemi di IA, elaborare linee guida e *best practices*, per analizzare le segnalazioni in merito a possibili violazioni della salute, della sicurezza e dei diritti fondamentali.

A differenza di altre autorità di controllo europee, come ad esempio lo EDPB[115], l'Ufficio per l'IA non ha la base giuridica per prendere decisioni

[113] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale), art. 5

[114]Commission Decision establishing the European Artificial Intelligence Office, Brussels, 24.1.2024, C(2024) 390 final

[115] *European Data Protection Board*, autorità di coordinazione a livello europeo istituita seguendo il dettato del Regolamento 2016/679/UE

vincolanti relative alla revisione delle decisioni delle agenzie nazionali o alla risoluzione delle eventuali controversie tra agenzie nazionali. Alcuni[116] sostengono che la mancanza di tale possibilità sarà un grosso ostacolo ad una effettiva armonizzazione dell'applicazione dell'*AI Act*.

Per garantire la rappresentanza politica in merito agli orientamenti che verranno presi in fase di attuazione del Regolamento, verrà istituito il Comitato europeo per l'intelligenza artificiale, composto da un rappresentante per ogni Stato membro, mentre come membri osservatori parteciperanno il Garante europeo per la protezione dei dati e l'Ufficio per l'IA. Il comitato dovrà coordinare l'attività delle autorità nazionali designate ad attuare l'applicazione del Regolamento, oltre a svolgere attività simili a quelle dell'Ufficio per l'IA.

Relativamente alle autorità nazionali invece il Regolamento all'art. 28[117] prevede per ogni Stato membro l'istituzione o la designazione di almeno un'autorità di notifica per gli organismi di valutazione della conformità dei sistemi ad alto rischio e del loro monitoraggio.

Tali organismi saranno terzi rispetto all'autorità, ma saranno sottoposti al suo controllo e alla verifica dell'assenza di conflitti di interesse. Gli organismi notificati dovranno verificare il rispetto della normativa da parte dei sistemi di IA ad alto rischio, emanare certificazioni, e condurre *audit* periodici.

All'art. 70 del Regolamento[118] viene prevista da parte di ogni Stato membro la designazione o istituzione di un'autorità di vigilanza del mercato, e di un'autorità di notifica. I dati relativi a tali autorità devono essere comunicati sia alla Commissione che al pubblico, designando un "punto di contatto unico" con il pubblico, in modo da agevolare la comunicazione tra il pubblico e l'autorità.

[116] Cfr. NOVELLI, et al., 2024

[117] Regolamento 2024/1689/UE del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale), art. 28

[118] *Ibidem*, art. 70

Conclusioni

A fronte del dilagare di un nuovo fenomeno sociale il legislatore ha tentato di individuare una soluzione in fretta, nella speranza di riuscire a mantenere lo *status quo.* L'obiettivo riguarda la tutela della salute, della sicurezza, dei diritti dei cittadini e dell'ambiente, ma quando si ha a che fare con le nuove tecnologie, caratterizzate da capacità di diffusione mai viste, che travalicano confini geografici e temporali, i paradigmi tradizionali hanno bisogno di un'interpretazione innovativa per mantenere la loro validità.

L'Unione Europea si fa promotrice del progresso tecnologico nei propri territori e nel mondo, attraverso la definizione di strategie di lungo periodo e piani di investimento su ricerca e promozione dell'imprenditorialità[119]. A ciò accompagna lo sforzo descritto *supra* di rimanere riferimento mondiale per lo sviluppo normativo in merito alle nuove tecnologie.

Alla prova dei fatti il piano su cui sembra avere il maggior successo è proprio quello del primato normativo, dal momento che si è parlato di *Bruxelles effect,* ma il panorama tecnologico è ancora dominato dagli Stati Uniti per quanto riguarda lo sviluppo *software*, e dalla Cina per quanto riguarda la produzione di dispositivi digitali.

Il tentativo di applicazione della normativa anche al di fuori dei confini europei, come fatto con il GDPR[120], dimostra l'intenzione di fronteggiare l'intrinseca a-territorialità dei prodotti digitali, ma si devono fare i conti con le altre caratteristiche dei prodotti digitali: immaterialità, a-temporalità, riproducibilità a costi vicini allo zero, e sempre maggiore difficoltà nel poterli comprendere nel loro reale funzionamento.

Il rispetto delle norme che si stanno introducendo dovrà dunque essere garantito attraverso un'attenta attività di controllo da parte delle autorità

[119] strategia digitale della Commissione del febbraio 2020, programma strategico per il 2030 "Percorso per il decennio digitale"

[120]Regolamento 2016/679/UE del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati art. 3

nazionali, che necessiteranno di adeguati finanziamenti e di un livello di coordinazione sovranazionale molto elevato, in modo da rendere omogenea l'applicazione in tutti gli Stati membri. L'attenzione dovrà essere massima su ogni componente dei prodotti analizzati, avendo riguardo per le garanzie relative alla fonte dei *dataset*, alla loro *compliance* con le leggi di proprietà intellettuale, oltre al consueto rispetto dei requisiti di sicurezza. La mancanza di un adeguato livello di omogeneizzazione dell'applicazione della normativa produrrebbe delle storture al mercato oltre che ineguaglianze nella tutela dei diritti dei cittadini

Confidando che i passaggi necessari per attuare nel modo più semplice ed efficace la normativa vengano fatti in accordo alle raccomandazioni provenienti dal mondo delle imprese, dell'accademia e dei gruppi di cittadini, raggiungendo gli obiettivi di tutela e allo stesso tempo promuovendo lo sviluppo della famiglia di tecnologie dal maggior impatto nei prossimi anni.

Bibliografia

1. S. ACETO DI CAPRIGLIA, *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità: Le soluzioni assunte dai governi unionale, statunitense e sinico. Uno studio comparato*, in *federalismi .it,* 9, 2024, pp. 1-38
2. a- A. AMIDEI, *Intelligenza Artificiale e responsabilità da prodotto,* in U. Ruffolo (a cura di), *Intelligenza artificiale Il diritto, i diritti, l'etica,* Giuffrè Francis Lefebvre, Milano, 2020, pp 125-152
3. b- A. AMIDEI, *La governance dell'IA: profili e prospettive di diritto dell'UE* in U. Ruffolo (a cura di), *Intelligenza artificiale Il diritto, i diritti, l'etica,* Giuffrè Francis Lefebvre, Milano, 2020, pp 571-588
4. J. ANGWIN, et al. *Machine bias,* in *Ethics of data and analytics*, Auerbach Publications, 2022, pp 254-264.
5. I. ASIMOV, *I, robot,* Gnome Press, New York 1950
6. A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Faculty Books, 232, New York, 2020
7. M. CAPPARELLI, *Le invenzioni dell'Intelligenza Artificiale: questioni aperte di tutela autoriale e brevettabilità,* in U. Ruffolo (a cura di), *Intelligenza artificiale Il diritto, i diritti, l'etica,* Giuffrè Francis Lefebvre, Milano, 2020, pp 345-362
8. F. CAROCCIA, *Soggettività giuridica dei robot?* in Alpa G. (a cura di), *Diritto e intelligenza artificiale,* Pacini Editore, Pisa, 2020, pp 213-250
9. G. D'ALFONSO, *Danni algoritmici e sviluppi normativi europei tra "liability" e "permittance rules"* in *European Journal of Privacy Law & Technologies*, 2, 2022, pp 18-66
10. G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Il diritto dell'informazione e dell'informatica*, Giuffrè Francis Lefebvre, Milano, 2022, pp 303-322
11. L. FLORIDI, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach*, disponibile online su SSRN: https://ssrn.com/abstract=3873273 o http://dx.doi.org/10.2139/ssrn.3873273
12. B. GOODMAN, S. FLEXMAN, *European Union Regulation on algorithmic decision-making and a "Right to explanation"*, in *AI Magazine*, 2017, 38, 3 pp 50-57
13. Gruppo Indipendente di Esperti ad Alto Livello sull'intelligenza Artificiale istituito dalla Commissione Europea nel giugno 2018, *Orientamenti Etici per un'IA Affidabile*, 8 aprile 2019
14. S. KARTHI, P. KASTJURIRENGAN et al, *An Investigation of Deep Learning*, in "*Integrating Deep Learning Algorithms to Overcome Challenges in Big Data Analytics*", CRC Press, 2021, pp 87-100
15. NJ. NILSSON, *The Quest for Artificial Intelligence*, Cambridge University Press, 2009, pp 408-409

16. C. NOVELLI, P. HACKER, J. MORLEY, J. TRONDAL, L. FLORIDI, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities,* in *European Journal of Risk Regulation*, 2024
17. G. RINALDI, *Meccanizzazione del contratto nel paradigma della blockchain*, in Alpa G. (a cura di), *Diritto e intelligenza artificiale,* Pacini Editore, Pisa, 2020, pp 343-376
18. a- U. RUFFOLO, *Il problema della "personalità elettronica",* in *Journal of Ethics and Legal Technologies*, 2, 2020, pp 75-88
19. b- U. RUFFOLO, *La personalità elettronica*, in U. Ruffolo (a cura di), *Intelligenza artificiale Il diritto, i diritti, l'etica,* Giuffrè Francis Lefebvre, Milano, 2020, pp 213-236
20. c- U. RUFFOLO, *La responsabilità da* artificial intelligence, *algoritmo e* smart product in U. Ruffolo (a cura di), *Intelligenza artificiale Il diritto, i diritti, l'etica,* Giuffrè Francis Lefebvre, Milano, 2020, pp 93-124
21. A. L. SAMUEL, *Some Studies in Machine Learning Using the Game of Checkers*, in "*IBM Journal of Research and Development*", 1959, vol. 3, no. 3, pp 210-229
22. C. SARRA, *Il mondo dato,* Cleup, Padova, 2019, pp 127-166
23. G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi,*in *Il diritto dell'informazione e dell'informatica*, Giuffrè Francis Lefebvre, Milano, 2003, pp 55-87
24. a- G. TADDEI ELMI, *I diritti dell'intelligenza artificiale tra soggettivitá e valore: Fantadiritto o jus condendum,* in L.LOMBARDI VALLAURI (a cura di), *Il meritevole di tutela,* Giuffrè Francis Lefebvre, Milano, 1990, pp 685-771
25. b- G. TADDEI ELMI, *Il Quid, il Quomodo e il Quid iuris dell'IA,* in *Rivista italiana di informatica e diritto*, CNR-IGSG, Firenze 2, 2021, pp 131-139
26. A. TURING, *Computing Machinery and Intelligence*, Mind, New Series, 1950, Vol. 59, No. 236, pp. 433-460
27. S. WATCHER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does non Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 7, 2, pp 76–99
28. R. ZIMMERMANN, *The German Civil Code and the Development of Private Law in Germany*, Oxford University Comparative Law Forum 1, in ouclf.law.ox.ac.uk , 2006