



UNIVERSITÀ DEGLI STUDI DI PADOVA
Dipartimento di Diritto Privato e Critica del Diritto

Corso di laurea magistrale in Giurisprudenza
a.a. 2023/2024

**Intelligenza artificiale e responsabilità civile: nuove prospettive di
regolamentazione alla luce dell'Artificial Intelligence Act**

Relatore: Chiar.mo Prof. Claudio Sarra

Laureanda: Giulia Bersan

Matricola 1127262

Indice

Introduzione	1
I. La responsabilità civile per i danni cagionati dai sistemi di IA: un vuoto normativo da colmare	5
1. Inquadramento concettuale: cos'è l'intelligenza artificiale?	5
1.1 Una panoramica storica: le origini e le prime definizioni	5
1.2 La nozione di intelligenza artificiale oggi: la macchina intelligente	6
1.3 Funzionamento e metodi di apprendimento dei sistemi intelligenti	8
2. Il problema dell'imputazione della responsabilità civile alla luce delle caratteristiche dell'intelligenza artificiale	12
2.1 Nascita e problematicità del così detto responsibility gap	12
2.2 Una tesi intermedia: la necessità di circoscrivere il problema	15
2.3 Il “falso problema” del responsibility gap: lo strumento interpretativo come idoneo ad allocare in modo soddisfacente la responsabilità	17
2.4 Una ricapitolazione delle soluzioni legali proposte	19
II. L'attuale panorama giuridico e le prospettive europee: un nuovo paradigma per l'intelligenza artificiale?	23
1. La normativa allo stato dell'arte: la Direttiva 85/374/CEE e le sue criticità	23
1.1 Il modello della Product Liability: natura, oggetto e finalità della normativa unionale	23
1.2 La nozione di prodotto	25
1.2.1 Update e upgrade del software: si può ancora parlare di prodotto?	28
1.2.2 L'algoritmo quale componente del prodotto finale	29
1.2.3 La fondamentale distinzione fra prodotto e servizio	30

1.3 I legittimati passivi	31
1.4 La spinosa questione del prodotto difettoso	33
1.4.1 La responsabilità del produttore alla luce della nozione di difetto: responsabilità oggettiva o presunta?	35
1.4.2 Il requisito dell'insicurezza	36
1.4.3 Le cause di esclusione della responsabilità del produttore.....	37
1.5 Il difetto nel prodotto intelligente.....	38
1.5.1 Le legittime aspettative di sicurezza degli utenti	40
1.5.2 L'onere della prova e le difficoltà del soggetto leso	43
1.6 Il danno risarcibile.....	45
2. La nuova proposta di Direttiva della Commissione europea.....	46
2.1 La necessità di un adeguamento della disciplina.....	46
2.2 L'allargamento della nozione di prodotto, i danni risarcibili e i legittimati passivi	47
2.3 Il concetto di difetto.....	48
3. Sistemi di Intelligenza artificiale: res o centri di imputazione giuridica?	49
3.1 La proposta di una nuova regolamentazione per i dispositivi intelligenti.....	49
3.2 Comparazione tra persona naturale e IA: la retorica antropomorfa	51
3.3 Comparazione tra persona giuridica e IA: il modello delle corporations.....	53
3.4 La personalità elettronica come approdo finale del processo di oggettivizzazione delle fonti dell'obbligazione.....	54
3.5 L'esternalizzazione del rischio e le possibili soluzioni.....	55
III. Artificial Intelligence Act: l'approccio europeo alla regolazione dell'Intelligenza artificiale	59
1. Le sfide dell'UE nell'era digitale: un nuovo modello regolatorio.....	59

1.1 L'Agenda Digitale europea: verso il mercato unico digitale	59
1.2 Il contesto geopolitico: la competizione con Cina e Stati Uniti	61
1.2.1 Le peculiarità del modello statunitense e del modello cinese.....	63
1.2.2 Il modello europeo e l'effetto Bruxelles	65
2. AI Act: la struttura e il modello risk-based	69
2.1 La definizione di IA e le critiche che solleva.....	69
2.2 Il modello risk-oriented: una breve analisi dell'impostazione seguita dal legislatore europeo	71
2.2.1 Rischio inaccettabile e pratiche di intelligenza artificiale proibite.....	73
2.2.2 Rischio alto	74
2.2.3 Rischio limitato e rischio minimo.....	76
2.3 Il bilanciamento ex ante nella prospettiva della valutazione del rischio	76
3. AI Act: il principio di accountability e il confronto con il GDPR	79
3.1 La premessa per una analisi comparata	79
3.2 La responsabilità del titolare del trattamento nel GDPR: fra liability e accountability.....	80
3.3 Il principio di accountability nel Regolamento sull'intelligenza artificiale e altre considerazioni critiche	82
4. La proposta di direttiva sulla responsabilità dell'IA nel solco della strategia digitale dell'Unione europea.....	87
4.1 IA Liability Directive: brevi cenni introduttivi.....	87
4.2 Le regole procedurali in breve	89
4.3 Riflessioni conclusive sulla proposta di AI Liability Directive.....	90
IV. Il modello interno della responsabilità extracontrattuale: gli strumenti del diritto civile italiano come risposta ai “nuovi” danni da sistemi di IA	93

1. Le tradizionali ipotesi di responsabilità vicaria: il robot come essere senziente.....	93
1. Le tradizionali ipotesi di responsabilità vicaria: il robot come essere senziente.....	93
1.1 Una breve ricognizione degli strumenti sin qui analizzati	93
1.2 La responsabilità per danno cagionato dall'incapace e la sua applicazione analogica.....	95
1.3 La responsabilità dei precettori e la sua applicazione analogica	97
1.4 La responsabilità dei committenti e la sua applicazione analogica	100
2. L'applicabilità degli artt. 2050 e 2051 c.c.: il robot come prodotto	102
2.1 Le evoluzioni storiche della responsabilità da cose in custodia e da attività pericolosa, dal Code Napoleon al Codice civile del 1942	102
2.2 La responsabilità ex art. 2050 c.c. e la sua cumulabilità con quella da prodotto difettoso	104
2.3 Il regime di cui all'art. 2051 c.c. e la qualificazione giuridica della responsabilità da cose in custodia.....	107
2.4 L'art. 2051 c.c. e l'intelligenza artificiale.....	110
2.4.1 Le figure del produttore e del trainer: quale responsabilità?	112
3. L'art. 2054 c.c. e il futuro della r.c.a.	113
3.1 La disciplina dell'art. 2054 c.c.	113
3.1.1 Le nozioni di "circolazione", "veicolo" e "conducente"	115
3.1.2 I criteri di imputazione della responsabilità	116
3.2 Livelli di automazione e applicazione dell'art. 2054 c.c.	117
Conclusioni	<i>119</i>
<i>Bibliografia</i>	<i>123</i>

Introduzione

Non vi è giorno in cui non si senta parlare di intelligenza artificiale; siti di informazione, *mass media* ed esperti del settore cercano di delineare il futuro che ci attende tra prospettive di grandi conquiste e timori di un'evoluzione esponenziale delle nuove tecnologie che potrebbe portare a conseguenze disastrose. Cosa accadrebbe se la macchina superasse l'uomo? Se l'intelligenza non umana, già da tempo in grado di svolgere attività tradizionalmente riservate agli individui e spesso capace di raggiungere risultati preclusi ad essi, potesse in futuro sviluppare una coscienza? Segnerebbe questo traguardo la fine del primato dell'essere umano sulla terra? Questi sono solo alcuni dei quesiti che vengono posti, ormai da molto tempo, con l'obiettivo di intavolare una discussione sul tema. Se da una parte non vi è dubbio che il progresso tecnologico e il rapido sviluppo delle applicazioni di IA faccia sorgere degli interrogativi sulla società del futuro, non va dimenticato che già la società del presente necessita di risposte per questioni molto più urgenti. Dal punto di vista giuridico si indaga, infatti, sugli effetti che questa così detta quarta rivoluzione industriale sta attualmente esplicando e, in particolare, sulle ripercussioni che la massiccia diffusione di tali sistemi sta provocando con riferimento alla violazione dei diritti fondamentali. Segnatamente, molti studiosi hanno concentrato la loro attenzione sulla relazione che viene ad instaurarsi fra l'intelligenza artificiale (o, meglio detto, le intelligenze artificiali, essendo condivisa l'opinione per cui non esiste un'unica intelligenza non umana che presenta caratteristiche univoche) e la responsabilità civile: chi risponde per i danni cagionati dai sistemi intelligenti? Quali criteri di imputazione della responsabilità risultano più opportuni ai fini della migliore allocazione della stessa in tali scenari? Si tratta di un tema largamente esplorato e che, tuttavia, continua ad essere oggetto di interesse poiché attualmente disciplinato da una normativa *in fieri* che forse ancora non è completamente in grado di rispondere all'esigenza di regolamentazione della materia. Le caratteristiche dell'IA più avanzata pongono a dura prova l'idoneità

delle tradizionali norme in materia di responsabilità extracontrattuale a offrire adeguata tutela ai soggetti lesi dall'agire della macchina intelligente.

Questo lavoro di tesi si propone di fotografare lo stato dell'arte della disciplina tanto europea come interna, di raccogliere i principali orientamenti dottrinali che, negli ultimi anni, hanno cercato di trovare una soluzione al problema e di interrogarsi sulle prospettive future, soprattutto alla luce di un nuovo regolamento europeo che promettere di incidere in maniera sostanziale nella regolamentazione del settore.

Si cercherà innanzitutto di inquadrare il problema del “*responsibility gap*” e di comprendere le circostanze (si anticipa, legate al modo di essere dei sistemi di IA più complessi) che portano all'originarsi di un vuoto di responsabilità; ci si interrogherà sulla reale esistenza di questa lacuna e, soprattutto, sulla possibilità di colmarla senza dover necessariamente ricorrere ad una nuova produzione normativa. Si offrirà, a riguardo, una panoramica degli strumenti di cui l'interprete attualmente dispone; a questo proposito, ci si concentrerà sull'esame della Direttiva 85/374/CEE relativa alla responsabilità per prodotto difettoso, al fine di comprenderne pregi e limiti alla possibilità di applicazione al campo dei “nuovi” danni da dispositivo intelligente. Si darà anche conto di un orientamento che, attraverso l'elaborazione del concetto di “personalità elettronica”, vorrebbe riconoscere il sistema di IA quale soggetto dotato di capacità giuridica, al fine di vedergli imputata la responsabilità per i danni verificatisi in conseguenza della sua attività. Una volta delineato il quadro attuale, si passerà ad esaminare luci e ombre dell'*AI Act*, regolamento europeo che, nonostante non sia ancora entrato in vigore, sta già facendo parlare molto di sé. Il capitolo dedicato all'analisi del provvedimento rappresenta il cuore del percorso che si intende svolgere; l'approccio che le Istituzioni dell'Unione europea adottano nel campo dell'intelligenza artificiale mostra quali siano le vere sfide del futuro. Nello specifico, come il problema dell'imputazione della responsabilità possa essere affrontato attraverso una impostazione che pone il *focus* sulla necessità di ridurre a monte il rischio del verificarsi del danno, piuttosto che concentrarsi sulla risarcibilità *ex post*. Ma soprattutto si cercherà di sottolineare come l'approccio *risk-based* adottato dal legislatore europeo rappresenti la vera chiave di volta di un sistema che si propone di

coniugare tutela dei diritti fondamentali e promozione della ricerca e dello sviluppo tecnologico. Si riserverà l'ultima parte di questo lavoro all'esame delle ipotesi di responsabilità extracontrattuale contemplate nel Codice civile italiano, con l'obiettivo di comprendere se vi sia, fra queste, una fattispecie concretamente applicabile al caso di cui si discute.

Da ultimo, le conclusioni saranno dedicate a fare il punto della situazione; l'*AI Act* riesce, così come concepito allo stato attuale, a rispondere efficacemente all'esigenza di allocare la responsabilità per i danni cagionati dai sistemi di IA? Quale criterio di imputazione pare essere il più adeguato alla luce dell'analisi svolta? Ad oggi, quali sono gli strumenti giuridici di cui può avvalersi il soggetto leso? A queste e altre domande si cercherà di dare risposta nel corso di questa trattazione.

I. La responsabilità civile per i danni cagionati dai sistemi di IA: un vuoto normativo da colmare

1. Inquadramento concettuale: cos'è l'intelligenza artificiale? 2. Il problema dell'imputazione della responsabilità civile alla luce delle caratteristiche dei dispositivi intelligenti.

1. Inquadramento concettuale: cos'è l'intelligenza artificiale?

1.1 Una panoramica storica: le origini e le prime definizioni

Le origini dell'intelligenza artificiale si fanno risalire intorno al 1950, anno in cui viene pubblicata l'opera *Computing Machinery and Intelligence*, il cui autore, Alan Mathison Turing, è considerato a tutti gli effetti il padre dell'informatica. L'espressione "intelligenza artificiale", tuttavia, fa la sua comparsa solo qualche anno più tardi, nel 1955, quando, tra gli altri John McCarthy e Marvin Minsky propongono l'uso del termine in un documento noto come Proposta di Dartmouth. L'evento che ne segna la vera e propria nascita è, invece, il *Dartmouth Summer Research Project on Artificial Intelligence*, svoltosi nel 1956¹. Una delle prime definizioni che vengono date di intelligenza artificiale risale proprio al 1956 e procede dallo stesso McCarthy, il quale ne parla in questi termini: "the science and engineering of creating intelligent machines". Nel 1968 Marvin Minsky la descrive come "the science of making machines do things that would require intelligence if done by men". Bellman, matematico statunitense, la definisce nel 1978 in questo modo: "the automation of activities that we associate with human thinking, activities such as decision-making, problem solving, learning, creating, game playing and so on". Si tratta di definizioni che si ricollegano a quanto espresso da Turing attraverso il suo celebre test²: la

¹ M.TAMPIERI, *L'intelligenza artificiale tra storia e utopia per il futuro*, in *L'Intelligenza Artificiale e le sue evoluzioni*, CEDAM, 2022, pp. 9 e ss.

² Il test di Turing si pone l'obiettivo di identificare se una macchina sia in grado di esibire un comportamento intelligente attraverso un gioco che coinvolge, nella sua versione originaria, 3 soggetti: un uomo A, una donna B, e una terza persona C, la quale, separata da A e B, deve stabilire qual è l'uomo e qual è la donna. Per raggiungere questo obiettivo C deve porre una serie di domande ad A e B, i quali a loro volta devono fargli pervenire delle risposte: il tutto avviene in forma

macchina può essere definita intelligente se è in grado di imitare in maniera indistinguibile il comportamento umano³.

1.2 La nozione di intelligenza artificiale oggi: la macchina intelligente

Attualmente non esiste una definizione universale di intelligenza artificiale sulla quale vi sia unanime concordanza. La nozione di IA copre una vasta gamma di concetti e di termini, il che rende particolarmente arduo il compito di definirla. Le definizioni di cui disponiamo spesso fanno riferimento a termini quali “imparare”, “pensare” e “intelligenza”⁴, ragion per cui la maggior parte dei tentativi di definizione non tecnica tendono a descrivere l’IA come macchine e/o applicazioni dotate di capacità umane e di intelligenza. In senso contrario si noti la tesi di A. Bertolini, così come espressa nello studio commissionato dal Parlamento europeo *Artificial Intelligence and Civil Liability*, 2020, il quale sostiene non solo che nessuna macchina sia in grado di manifestare un grado di intelligenza simile a quello umano, ma che addirittura la ricerca stessa non persegua questo obiettivo, tentando invece di favorire lo sviluppo di una specifica abilità, la quale, molte volte, supera le capacità dell’essere umano in quel campo di applicazione. Bertolini sottolinea in secondo luogo come le definizioni della nozione di IA tendano, alle volte, ad elencare una serie di caratteristiche tutte umane che rappresenterebbero il *proprium* dell’IA: percezione visiva, riconoscimento vocale, capacità di tradurre diverse lingue e capacità di prendere delle decisioni. Orbene, anche questo non sarebbe corretto: si tratterebbe, infatti, di funzioni che non conducono ad individuare caratteristiche qualificanti, ma piuttosto tratti posseduti da singole applicazioni di IA. Semplificando, Bertolini sostiene che si stia cercando di definire e

dattiloscritta. Il test prevede che, in un determinato momento, A venga sostituito da una macchina: se la percentuale di volte in cui C indovina chi sia l’uomo e chi la donna si mantiene simile prima e dopo la sostituzione con la macchina, allora il test si considera superato. Ciò significa che la macchina può essere considerata intelligente, poiché il suo comportamento, in quel contesto, si considera non distinguibile da quello di un essere umano.

³ Cfr. TURING, *Computing Machinery and Intelligence*, in *Mind*, 1950.

⁴ A. HAUSELMANN, *Disciplines of AI: An Overview of Approaches and Techniques*, in *Law and Artificial Intelligence*, Springer, 2022.

di spiegare l'intelligenza artificiale soltanto attraverso alcune delle sue applicazioni e sulla base della capacità di queste di replicare tratti umani. Questo dimostrerebbe, da un lato, che per comprendere l'IA è necessario soffermarsi sulle singole applicazioni della stessa; dall'altro, che la premessa maggiore a cui si ricorre per definire l'IA, ovvero la capacità della macchina di agire utilizzando un'intelligenza simile a quella umana, restringe inevitabilmente l'ambito della definizione, dal momento che disponiamo di molte applicazioni di IA che non si fondano su tale modello.

A prescindere dall'approccio antropomorfo sin qui descritto e dalle critiche ad esso rivolte, vi sono poi ulteriori tentativi di definizione che hanno posto, nel corso degli anni, significative distinzioni all'interno della vasta categoria IA. In particolare, si parla di IA debole e IA forte, accostandosi al tema attraverso una impostazione più filosofica che tecnica. Con l'espressione *weak artificial intelligence* ci si riferisce alla capacità della macchina di simulare il pensiero umano, vale a dire di agire come se fosse intelligente, con il mero intento di assolvere alla funzione di *problem solving*, senza necessariamente dover comprendere i processi cognitivi dell'uomo; mentre l'espressione *strong artificial intelligence* individua l'attitudine della macchina ad agire sulla base di una capacità cognitiva che non può essere distinta da quella umana che la induce a pensare in maniera autonoma. Tale dicotomia si deve a John Rogers Searle, il quale, peraltro, a differenza di McCarthy, nega l'esistenza di una IA forte ritenendo impossibile dal punto di vista teorico la creazione di artefatti capaci di pensiero in senso proprio.⁵ Ancora, sul piano pratico è possibile individuare una ulteriore distinzione fra sistemi di IA *software-based*, quali, fra tutti, motori di ricerca o assistenti vocali e sistemi intelligenti incorporati in dispositivi *hardware*, quali droni o auto a guida autonoma.

⁵ J.R. SEARLE, *Minds, Brains and Programs*, in *The Behavioural and Brain Science*, 1980, pp. 417 ss.

Nonostante la varietà delle proposte definitorie alle quali si è sin qui fatto cenno, si è giunti, su invito del Parlamento europeo⁶, alla elaborazione di una definizione di *artificial intelligence* tale da poter ricomprendere al suo interno la gran parte delle applicazioni rappresentative di questa tecnologia. Nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni⁷ si parla di “sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni con un certo grado di autonomia, per raggiungere specifici obiettivi”.

1.3 Funzionamento e metodi di apprendimento dei sistemi intelligenti

Comprendere i meccanismi che stanno alla base dell’agire dei sistemi intelligenti risulta particolarmente significativo ai fini della disamina della questione che verrà affrontata successivamente relativa all’imputazione della responsabilità civile per i danni cagionati da tali sistemi. È difatti il processo di apprendimento e di funzionamento di un certo tipo di *software* IA che dà origine ad alcune delle peculiarità del fenomeno che si pongono a fondamento del problema giuridico qui in esame.

Va anzitutto introdotto il concetto di algoritmo, il quale rappresenta la logica di funzionamento di un programma. L’algoritmo può essere definito come “una sequenza non ambigua di passi che determina la procedura di soluzione di un problema”. Per la scrittura di questa sequenza si utilizza di solito uno pseudo-codice che mescola linguaggio naturale, linguaggio matematico e linguaggio di programmazione, il che allontana qualsiasi rischio di ambiguità. Altro concetto fondamentale è quello di *software*, definito come “il codice di un programma scritto in un preciso linguaggio di programmazione ed eseguibile da un computer”. Proprio per la relazione che li lega si tende spesso a confondere questi due concetti. In realtà non sussiste alcuna

⁶ Tale invito è contenuto nella Risoluzione del Parlamento europeo recante “*Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*”, 16.2.2017 e, in particolare, nell’allegato alla Risoluzione.

⁷ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni dal titolo “*L’intelligenza artificiale per l’Europa*”, Bruxelles, 25.4.2018.

intercambiabilità, dal momento che per poter essere realizzato in un modo possibile l'algoritmo necessita di essere implementato in un *software*: solo questa traduzione renderà l'algoritmo eseguibile.⁸ I sistemi di intelligenza artificiale sono quindi *software* sui quali vengono implementati algoritmi.

Per quanto concerne il metodo di apprendimento dei sistemi intelligenti, è possibile individuare due paradigmi che negli anni ne hanno guidato la ricerca e lo sviluppo: quello simbolico⁹, denominato anche “approccio *top-down*” e quello sub-simbolico, denominato anche “approccio *bottom-up*”. Il metodo simbolico consiste nel fornire alla macchina una rappresentazione formale della conoscenza espressa mediante regole e concetti e accompagnata da algoritmi facenti ricorso a ragionamenti logici; in questi casi l'operato della macchina intelligente risulta più comprensibile all'osservatore umano, ma sfocia in un ostacolo alla crescita e all'adattamento dei sistemi intelligenti. Oggetto di un rinnovato interesse pare essere oggi, invece, l'approccio sub-simbolico, fondato sull'applicazione di procedure numeriche e statistiche. Attraverso tale paradigma si passa dalla rappresentazione formale della conoscenza fornita dall'uomo ad un metodo di apprendimento automatico che il sistema intelligente può sviluppare a partire da grandi masse di dati.¹⁰ Si suole riferirsi a tale modello di apprendimento attraverso l'uso dell'espressione *Machine Learning*, segnatamente definito quale “quella branca dell'informatica che permette ad una macchina di imparare ad eseguire un compito senza essere stata programmata per farlo”.¹¹ I sistemi di autoapprendimento differiscono tra loro sia per il modello di algoritmo utilizzato, sia per il procedimento attraverso il quale il sistema impara. In particolare, è possibile distinguere tre diversi approcci: l'apprendimento

⁸ Le definizioni di algoritmo e di software e la distinzione fra questi due concetti si trova in S. CRAFA, *Dalle competenze alla consapevolezza digitale: capire la complessità e la non neutralità del software*, in P. Moro (a cura di), *Etica, Diritto e Tecnologia*, FrancoAngeli, Mio 2021.

⁹ A. NEWELL, H.A. SIMON, *Computer Science as Empirical Inquiry: Symbols and Search*, in *Communications of the ACM*, 1976, pp. 113 ss.

¹⁰ G. SARTOR, F. LAGIOIA, Le decisioni algoritmiche tra etica e diritto, in *Intelligenza artificiale: il diritto, i diritti e l'etica*, U. Ruffolo (a cura di), 2020.

¹¹ A.L. SAMUEL, *Some studies in machine learning using the game of checkers*, in *IBM Journal of Research and Development*, 1959, pp. 210 ss.

supervisionato, l'apprendimento per rinforzo e l'apprendimento non supervisionato. Nel primo caso, alla macchina si fornisce un ampio set di dati e di informazioni specifiche che vengono codificate e preinstallate nel software, relative anche ai risultati che si desidera ottenere; da queste la macchina ricava le indicazioni su cui fonda la propria decisione. ¹² Sulla base degli esempi che le vengono forniti, la macchina elabora un modello generale che collega la descrizione di un caso alla risposta esatta dello stesso e successivamente applica tale regola generale a casi nuovi, parzialmente diversi da quelli forniti durante l'addestramento.¹³ L'apprendimento per rinforzo avviene ugualmente mediante esempi, ma in questo caso il sistema apprende dai risultati delle proprie azioni, non avendo bisogno di alcun istruttore. Per correggere la propria azione e rendere possibile l'addestramento, allora, il sistema stesso si autosomministra premi o penalità sulla base del risultato raggiunto. Diventa in questo caso essenziale l'interazione con l'ambiente in cui il dispositivo è immerso, affinché possa effettivamente adeguare il proprio comportamento al contesto in cui svolge la propria azione. Nell'apprendimento non supervisionato, infine, alla macchina vengono forniti solo set di dati in entrata, di tal modo che la macchina non riceve alcuna istruzione né da fonti esterne né dai risultati del proprio operato; è essa stessa ad utilizzare questo set di dati per creare esempi di problema a cui dare poi soluzione. All'interno della categoria del *Machine Learning* è poi possibile individuare diversi approcci pratici che danno vita ad altrettanti sistemi di autoapprendimento, il più importante dei quali, per lo meno ai fini di questa disamina, è rappresentato dalle reti neurali artificiali (*artificial neural network*). Si tratta di sistemi sub-simbolici che, ispirandosi ad un parallelismo con la struttura e il funzionamento del cervello umano, operano mediante neuroni artificiali posti in connessione fra loro tentando di riprodurre le basilari operazioni neurali proprie degli esseri viventi. La rete si compone di norma di tre strati: il primo si occupa dell'azionamento dei neuroni al momento della ricezione degli input, il secondo provvede ad elaborare i dati in entrata, mentre il

¹² U. RICCIARDELLI, *Automazione self-learning e responsabilità civile: note a margine di una riflessione europea*, in *Cammino Diritto*, <https://rivista.camminodiritto.it>, n.5/2020, p.34.

¹³ G. SARTOR, *L'intelligenza artificiale e il diritto*, Giappicchelli, 2022, p.46.

terzo è dedicato agli output.¹⁴ Il secondo strato (c.d. strato nascosto) può essere costituito da un unico livello, parlandosi allora di *simple neural networks*, ovvero da più livelli, parlandosi in questo caso di *deep neural networks*.¹⁵ Queste ultime sono spesso costituite da molti strati, ciascuna inglobante migliaia di neuroni e di connessioni: risulta pertanto impossibile verificare le informazioni codificate all'interno di questo secondo strato e il processo di elaborazione dei dati che in tale sede ha luogo. Ci si riferisce a tale metodo di apprendimento automatico con l'espressione *Deep Learning*: in questo caso il comportamento finale della macchina diviene potenzialmente imprevedibile, configurandosi perciò i suddetti sistemi come scatole nere (*black-boxes*).

Chiarito in maniera pressoché semplificata il meccanismo di funzionamento e di autoapprendimento dell'intelligenza artificiale, va sottolineato allora come la complessità che caratterizza queste tecnologie e, in particolar modo, le macchine che utilizzano sistemi di *Deep Learning*, non permetta di comprendere quali siano i passaggi che hanno portato il sistema ad adottare una determinata decisione o un certo comportamento. Il procedimento eseguito non solo è opaco *ex post*, ma anche imprevedibile *ex ante*, dipendendo da tutta una serie di fattori indipendenti dagli stimoli predefiniti che la macchina riceve attraverso l'algoritmo che incorpora. Ciò conduce all'individuazione di quella che è, probabilmente, la più rilevante caratteristica delle tecnologie *self-learning*: la capacità di assumere decisioni autonome, frutto di un processo di adattamento del dispositivo all'ambiente nel quale tali tecnologie sono tenute ad operare. Il sistema modifica così il proprio comportamento sulla base dei dati e delle informazioni che la realtà circostante gli fornisce, risultando particolarmente arduo se non addirittura impossibile, esercitare un controllo sugli esiti dell'agire tecnologico.¹⁶

¹⁴ U. RICCIARDELLI, *Automazione self-learning e responsabilità civile: note a margine di una riflessione europea*, in *Cammino Diritto*, <https://rivista.camminodiritto.it>, n.5/2020, p. 7.

¹⁵ L. RODOLFI, *Appunti sparsi di Machine learning. Un vademecum per comprendere uno degli argomenti più affascinanti dei nostri giorni*, 2019, p. 19.

¹⁶ U. SALANTIRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Rivista di diritto civile*, n.6/2020, p. 1247.

2. Il problema dell'imputazione della responsabilità civile alla luce delle caratteristiche dell'intelligenza artificiale

2.1 Nascita e problematicità del così detto responsibility gap

Tra le più importanti e impegnative sfide che l'evoluzione scientifica e tecnologica dell'intelligenza artificiale pone in capo al giurista contemporaneo si rintraccia proprio quella che origina dall'avvento delle macchine *self-learnig* e che, in particolare, si ricollega a quella peculiare caratteristica che le contraddistingue che è l'autonomia. È proprio tale tratto, tipico solo di alcune applicazioni di intelligenza artificiale, che pone il problema giuridico di cui ci si occupa in questo lavoro di tesi: in capo a chi deve essere imputata la responsabilità civile per i danni che potrebbero essere cagionati da un sistema di intelligenza artificiale *self-learning*? Le preoccupazioni espresse in dottrina circa l'eventuale nascita di un vuoto normativo legato al concetto di autonomia dei sistemi di IA emergono dalla difficoltà tecnica nel ricostruire la sequenza dei processi decisionali e di autoapprendimento che tali sistemi eseguono. È possibile riassumere, perciò, il concetto di *responsibility gap* in questi termini: la capacità di apprendimento rende l'azione del robot potenzialmente imprevedibile, con la conseguenza che, nell'ipotesi di danno, vista la difficoltà nell'ottenere informazioni sul processo decisionale sotteso alla condotta, l'attuale assetto normativo porterebbe ad imputare la responsabilità in modo moralmente ed economicamente ingiusto, rischiando di lasciare in capo alla vittima il costo dell'innovazione tecnologica¹⁷. Si tratta, invero, di una problematica maggiormente condivisa dai filosofi del diritto come, ad esempio, A. Matthias, il quale inquadra la questione focalizzandosi, da un punto di vista strettamente giuridico, sul concetto di controllo così come connesso al necessario ideale di giustizia al quale ciascun ordinamento giuridico dovrebbe tendere. Matthias parte dal presupposto che, in accordo con il nostro senso di giustizia, un

¹⁷ U. RICCIARDELLI, *Automazione self-learning e responsabilità civile: note a margine di una riflessione europea*, in *Cammino Diritto*, <https://rivista.camminodiritto.it>, n. 5/2020, p. 8.

soggetto possa essere ritenuto responsabile per le proprie azioni solo quando abbia un effettivo controllo sulle stesse, vale a dire quando sia cosciente dell'ambiente che lo circonda e possa, quindi, decidere liberamente di agire. Lo stesso principio si applica anche nel caso in cui dette azioni vengano poste in essere attraverso l'utilizzo di macchine: si ritiene responsabile colui il quale abbia la possibilità di esercitare un controllo sulle stesse (vale a dire l'operatore) nel caso in cui la macchina non presenti alcun difetto; mentre, nel caso in cui la difettosità della macchina impedisca all'operatore di esercitare il necessario controllo sulle sue azioni, si imputerà la responsabilità in capo al produttore. Pertanto, secondo Matthias, il problema dell'imputazione della responsabilità sorge in concomitanza con la mancanza di un effettivo controllo esercitabile sulla macchina. Ed è proprio questo ciò che accade allorquando si ricorre all'utilizzo delle così dette macchine *self-learning*. A tal proposito, l'autore presenta una esaustiva classificazione dei sistemi intelligenti che vede la divisione di tali sistemi in quattro principali categorie: *symbolic systems*, *connectionism e neural nets*, *genetic algorithms*, *autonomous agents*. Senza soffermarsi, in questa sede, sull'analisi di ciascuna categoria, si prendano in considerazione, nello specifico, le peculiarità dei già brevemente summenzionati *symbolic systems*, tali da evidenziare la distinzione tra questi e le restanti categorie: si tratta di dispositivi creati sulla base del presupposto che molte funzioni cognitive tipiche dell'essere umano, come ad esempio l'intelligenza, possano essere riprodotte ed espresse attraverso la manipolazione sintattica di simboli linguistici (i quali, non per forza, debbono essere simboli del nostro linguaggio naturale). I sistemi simbolici sono in grado di agire sia sulla base delle informazioni immagazzinate nel loro *database*, sia estendendo essi stessi il proprio *database* attraverso l'aggiunta di nuove regole e conoscenze (il che costituisce la loro capacità di auto apprendere). Ciò che più preme sottolineare, tuttavia, è il fatto che le informazioni in virtù delle quali il sistema agisce sono immagazzinate nel sistema stesso nella forma di simboli quasi -linguistici, espliciti e distinguibili. Questo comporta che, in qualsiasi momento, il

sistema possa essere ispezionato e, se del caso, corretto.¹⁸ Il programmatore, dunque, può ben essere considerato “*coder*”, ovverosia colui che crea il programma linea dopo linea, impartendo alla macchina una serie di istruzioni rappresentate linguisticamente, le quali vengono direttamente eseguite dalla macchina capace di decifrare quel linguaggio simbolico. Il programmatore è così in grado di controllare ogni singolo comportamento del dispositivo e di spiegare come lavora l’algoritmo; mentre un qualunque osservatore potrà seguire detta spiegazione e verificarne la correttezza. Gli errori sono sempre e solo errori del programmatore, non errori del programma; possono essere, in qualunque momento, identificati, isolati e corretti e il programmatore potrà sempre essere ritenuto responsabile per qualsiasi comportamento erroneo della macchina. La perdita di controllo del programmatore è ciò che caratterizza, per converso, le restanti categorie: il “*coder*” viene sostituito dal creatore di *software*, il quale trasferisce parte del suo controllo sulla macchina all’ambiente nel quale la macchina opera. Il comportamento della macchina non è più definito unicamente dal programma così come scritto dal programmatore, ma si modella sempre più attraverso le proprie interazioni con l’ambiente circostante, il quale fornisce alla macchina stessa nuovi schemi di condotta che la macchina utilizzerà per la risoluzione dei problemi che le si presenteranno. Viene superata la tradizionale distinzione tra la fase della programmazione, dell’addestramento e dell’operatività; tali dispositivi *self-learning* vengono addestrati direttamente durante la fase dell’operatività, il che significa, inoltre, che dovranno commettere degli errori durante tale fase per poter apprendere autonomamente quale sia il comportamento corretto in ogni situazione. E questi errori non potranno essere evitati in alcun modo, essendo parte del “training” della macchina e non essendoci soggetti in grado di esercitare un vero e proprio controllo sulla stessa. Ed è proprio questa circostanza che, secondo Matthias, rende le tradizionali regole di imputazione della responsabilità incompatibili con il nostro senso di giustizia e con la morale sociale. Si creerebbe, allora, un vuoto

¹⁸ A. MATTHIAS, *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics and Information Technology*, 2004, p. 178.

normativo che impedirebbe di ascrivere la responsabilità secondo giustizia; lacuna che andrebbe colmata attraverso nuove previsioni legislative.

2.2 Una tesi intermedia: la necessità di circoscrivere il problema

La discussione circa la reale esistenza di una lacuna normativa nell'ambito delle disposizioni volte ad individuare il soggetto responsabile in caso di danni cagionati dalle macchine intelligenti si arricchisce, poi, anche grazie agli interessanti spunti proposti dal giurista olandese Peter Konigs, il quale non nega a priori l'esistenza di eventuali *responsibility gaps*, ma evidenzia, piuttosto, la necessità di specificare le circostanze in cui tali vuoti normativi verrebbero a crearsi. Konigs, anzitutto, chiarisce cosa lui intenda per "*responsibility*" nel contesto in questione: si tratterebbe, a suo dire, di quell'aspetto della responsabilità che ha a che vedere con l'*accountability*¹⁹. Ma non è tutto; una ulteriore distinzione necessaria sarebbe poi quella tra *moral* e *legal responsibility*, la prima essendo legata al dovere morale di ristorare la vittima del danno, la seconda all'obbligazione di natura legale di risarcirla. Nel caso di specie i *responsibility gaps* concernerebbero l'aspetto morale della responsabilità, essendo sempre possibile individuare il soggetto tenuto, da un punto di vista legale, a risarcire il danno.²⁰ Circoscritto il significato del termine "*responsibility gap*", Konigs formula la sua critica ai così detti "*responsibility gap pessimists*" lanciando loro una sfida: quella di definire con accuratezza le specifiche circostanze in cui possa dirsi esistente tale vuoto di responsabilità. Affinché ciò avvenga deve essere dimostrata, secondo l'autore, la sussistenza di due condizioni, l'una specificatrice dell'altra. La prima condizione viene identificata con l'assenza di responsabilità: tale condizione è soddisfatta quando sarebbe ingiusto e scorretto incolpare qualcuno. La seconda condizione precisa l'ambito di applicazione della prima. Non è sufficiente che non vi

¹⁹ Si rimanda l'analisi del termine "*accountability*", così come distinto dal termine "*responsibility*" al capitolo successivo.

²⁰ Lo stesso pensiero viene espresso da A. BERTOLINI, in *Artificial Intelligence and Civil Liability*, 2020, p.33, il quale afferma: "There is no responsibility gap. It is always possible to identify a human being who might be deemed responsible for damages arising from the production, operation and use of a machine or AI-system, based on different legal criteria".

sia alcuna responsabilità; al contrario, è necessario che l'assenza di responsabilità sia relazionata all'autonomia del sistema di IA. L'idea è che sia l'autonomia del sistema - vale a dire la capacità della macchina di operare indipendentemente dall'intervento dell'uomo e di prendere decisioni che non si fondano sulle istruzioni impartite da esso - che esclude la responsabilità per i danni cagionati dal sistema intelligente. Detto ciò, sorge poi la necessità di una precisazione: l'idea che nessuno possa mai essere ritenuto responsabile per le azioni poste in essere dal sistema autonomo deve essere rifiutata. Ci sono, invero, alcune situazioni in cui l'uomo, persona fisica, deve, ad ogni modo, essere ritenuto responsabile per i danni cagionati dalla macchina dotata di autonomia. Ci si riferisce al caso in cui i danni cagionati dai sistemi autonomi siano il frutto di condotte colpose o dolose dell'operatore umano. Tali evenienze escludono, a parere dell'autore, la nascita di qualsiasi *responsibility gap*. La sfida che lancia Konigs ai così detti "*responsibility gap pessimists*", allora, è, prima di tutto, quella di specificare le situazioni in cui, essendoci un soggetto che opera attraverso macchine autonome e che le utilizza con la dovuta attenzione, non sia possibile individuare alcun responsabile per i danni cagionati dalle stesse. Vi è, tuttavia, una seconda sfida: qualora i *responsibility gaps* effettivamente sorgessero, sarebbe bene spiegare per quale motivo dovremmo esserne preoccupati. Una parte della dottrina cerca di dare risposta a questo quesito e identifica tale motivo di preoccupazione nella circostanza che, se non si potesse attribuire la responsabilità a nessun soggetto, non vi sarebbe alcun incentivo ad agire utilizzando la dovuta diligenza. Tuttavia, l'autore risponde a questa affermazione ricordando come, a suo avviso, non sorga alcun vuoto di responsabilità laddove si agisca con imperizia, imprudenza o negligenza; e anche qualora si potesse parlare di *responsibility gaps* in presenza dell'elemento soggettivo della colpa o del dolo, questo implicherebbe solo l'impossibilità di ritenere i soggetti agenti responsabili, non l'impossibilità di obbligarli a risarcire il danno; come precedentemente ricordato, infatti, l'autore ritiene che il *responsibility gap* abbia a che vedere con la così detta "*moral liability*" e non con l'opportunità di obbligare un soggetto a risarcire il danno, circostanza che dipenderà dall'ordinamento giuridico di ciascuno Stato. Konigs conclude mettendo in evidenza che, a suo parere, pur esistendo

una vera e propria difficoltà, in queste situazioni, ad allocare correttamente la responsabilità, si tratta di un problema più epistemico che metafisico; un problema che non consiste, tanto, nell'attuale assenza di un soggetto agente responsabile, quanto più nella difficoltà epistemica di determinare correttamente come andrebbe allocata la responsabilità.²¹

2.3 Il “falso problema” del responsibility gap: lo strumento interpretativo come idoneo ad allocare in modo soddisfacente la responsabilità

Esiste poi una dottrina, sostenuta soprattutto dai giuristi del diritto positivo, la quale nega in principio la sussistenza di un vero e proprio vuoto di responsabilità legato all'autonomia dei dispositivi intelligenti. Ugo Ruffolo ed Andrea Amidei partono dalla contestazione di ciò che emerge dalla Risoluzione del Parlamento europeo del 16 febbraio 2017 in materia di “norme di diritto civile sulla robotica”, per arrivare alla proposta di una soluzione che non contempla la creazione di nuove leggi, bensì cerca di risolvere il dilemma attraverso risposte sistemiche. Con la Risoluzione del 2017 il Parlamento invita la Commissione ad elaborare una proposta di direttiva che enunci nuove norme civilistiche, in grado di disciplinare in modo coerente ed uniforme, su tutto il territorio dell'Unione europea, l'utilizzo dei robot e dell'intelligenza artificiale sia nelle attività industriali che nella vita privata. Già nelle considerazioni iniziali è possibile ravvisare l'esigenza che conduce il Parlamento all'adozione della Risoluzione: risolvere, attraverso una nuova regolamentazione, i problemi posti dalla diffusione di nuove forme di robotica, più o meno intelligenti, e tutelare i soggetti che necessitano di maggiore protezione in siffatto nuovo quadro tecnologico (tra cui i consumatori), per un verso; assicurarsi che tale nuova regolamentazione sia sufficientemente flessibile da non ostacolare le innovazioni robotiche che apportano evidenti vantaggi, per altro verso. Il fulcro, o meglio, il *fil rouge* della Risoluzione è costituito dalla problematica della responsabilità civile, comune denominatore di quasi

²¹ P. KONIGS, *Artificial intelligence and responsibility gaps: what is the problem?*, in *Ethics and information Technology*, 2022.

tutte le tematiche affrontate dal Parlamento, che, come già visto precedentemente, diventa tema oggetto di preoccupazione proprio a causa della novità delle tecnologie di cui si discute. Ciò che, *in primis*, viene contestato al Parlamento europeo è la necessità, ravvisata da quest'ultimo, di adottare previsioni normative inedite; secondo Ruffolo e Amidei la caratteristica dell'autonomia non sarebbe sufficiente a giustificare l'elaborazione di nuove categorie e nuove disposizioni di legge nell'ambito della responsabilità civile, essendo adeguata anche solo una applicazione ed interpretazione evolutiva delle norme già esistenti in materia di contratti e di responsabilità extracontrattuale (eccettuato, forse, qualche adeguamento relativo alle disposizioni in materia di responsabilità da prodotto). Nuove disposizioni di legge, inoltre, andrebbero ad innestarsi su ordinamenti civilistici per lo più fondati su codici e norme ad impostazione codicistica, con previsioni e categorie sovente di carattere generale.²² Si tratta di ordinamenti contraddistinti da una pretesa di completezza, il che comporta l'idoneità dello strumento interpretativo, dell'analogia (quando praticabile) e del ricorso ai principi generali dell'ordinamento e alla interpretazione costituzionalmente orientata come mezzo per regolare il futuro; l'introduzione di ogni non indispensabile nuova norma porterebbe con sé la possibilità di alterare ed inquinare tali sistemi e creerebbe un rischio di "iperfetazione legislativa". Per questo motivo, secondo Ruffolo, appare preferibile circoscrivere il ricorso allo strumento normativo principalmente agli aspetti regolatori e tecnici di settore, senza sottovalutare, invece, la capacità di mediazione giuridica della disciplina generale, in particolare quella in materia di contratti e responsabilità civile, integrata con le norme di *product liability* (che andremo ad analizzare successivamente). Tali norme hanno il pregio di essere già esistenti, relativamente uniformi a livello europeo e, soprattutto, aperte ad evoluzioni interpretative in grado di disciplinare le sfide future.²³ Altra ragione che giustificerebbe la preferenza per il ricorso allo strumento interpretativo delle norme

²² A. AMIDEI, *Robotica intelligente e Responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Intelligenza Artificiale e Responsabilità*, a cura di Ugo Ruffolo, 2017, pp. 82-88.

²³ U. RUFFOLO, *La responsabilità da algoritmo*, in *XXVI lezioni di diritto dell'Intelligenza Artificiale*, a cura di Ugo Ruffolo, 2020, pp. 132-133.

già esistenti è il fatto che la stessa Risoluzione del 2017 prospetta due possibili “modelli” di attribuzione di responsabilità che il Parlamento europeo concepisce come alternativi: l’approccio della responsabilità oggettiva (“*strict liability*”) e l’approccio di gestione dei rischi. Per quanto riguarda la responsabilità oggettiva, giova ricordare come il nostro ordinamento abbia superato, ormai da qualche decennio, il pregiudizio connesso al tabù del “nessuna responsabilità senza colpa”²⁴; il danneggiante risponde del danno come conseguenza immediata e diretta della propria condotta, anche qualora mancasse l’elemento soggettivo del dolo o della colpa. Ciò consentirebbe, pertanto, di avvalersi di alcune delle norme già presenti nel nostro Codice civile in materia di responsabilità extracontrattuale.²⁵ L’approccio di gestione dei rischi si basa, invece, sull’individuazione, all’interno del processo di ideazione, progettazione, produzione e commercializzazione del robot, del soggetto più vicino al prodotto a seconda del malfunzionamento che si verifica, dunque colui che meglio degli altri soggetti coinvolti è in grado di gestire e minimizzare il rischio del verificarsi del danno. Anche in questo caso non si rinviene necessariamente l’elemento soggettivo della colpa. Il Parlamento europeo parla di tali modelli in termini di alternatività, mentre, a parere di Amidei, ben potrebbero costituire due diversi momenti dello stesso fenomeno, componenti entrambe necessarie per addivenire ad una allocazione soddisfacente delle responsabilità: si tratterebbe di identificare, nella catena produttiva commerciale i soggetti cui potrebbe essere attribuita tale responsabilità oggettiva.²⁶

2.4 Una ricapitolazione delle soluzioni legali proposte

Quando si fa riferimento al concetto di responsabilità civile è necessario tenere a mente che ci si riferisce sempre all’inadempimento di una obbligazione. La fonte dell’obbligazione determina le due principali forme di responsabilità: contrattuale ed

²⁴ U. RUFFOLO, *Per i fondamenti di un diritto della robotica self-learning; dalla Machinery produttiva all’auto driverless: verso una “responsabilità da algoritmo”?*, in *Intelligenza Artificiale e Responsabilità*, a cura di Ugo Ruffolo, 2017, p. 14.

²⁵ Si rimanda la trattazione di questo argomento al capitolo III.

²⁶ A. AMIDEI, *Robotica intelligente e Responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Intelligenza Artificiale e Responsabilità*, a cura di Ugo Ruffolo, 2017, pp. 86-87.

extra-contrattuale. Tale distinzione conduce a conseguenze diverse sia sul piano dell'onere della prova, sia sul piano delle regole in materia di prescrizione. Nel caso della responsabilità contrattuale l'inadempimento riguarderà un'obbligazione già sorta precedentemente fra le parti; in questo caso il creditore dovrà solo dimostrare l'esistenza dell'obbligazione e affermare che il debitore non ha adempiuto o ha adempiuto male, mentre spetterà a quest'ultimo discolarsi. L'onore della prova, pertanto, grava su di lui. Nell'illecito extracontrattuale, per converso, sarà colui che afferma di essere stato danneggiato a dover provare l'effettiva violazione dell'obbligo generale del *neminem laedere*, quindi l'esistenza di un bene protetto dalla legge e la sua violazione ad opera del debitore. Anche le regole in materia di prescrizione si presentano più favorevoli al creditore della prestazione nel caso di illecito contrattuale. Ciò che interessa rilevare in questa sede è come entrambe queste forme di responsabilità civile possano venire in rilievo nel caso di danni cagionati da un sistema di intelligenza artificiale, procedendo la distinzione dal tipo di obbligazione e di relazione che esiste a monte tra le parti coinvolte. Attualmente, tuttavia, l'applicazione di entrambe le forme di responsabilità in tali contesti sembra condurre a risultati insoddisfacenti.²⁷ Una delle soluzioni proposte ai fini di arginare il problema della responsabilità è, come già ricordato, il ricorso al regime della responsabilità oggettiva, quale auspicato anche dalla Risoluzione del Parlamento europeo del 2017. Gli ordinamenti giuridici europei ammettono una limitata applicazione di questo tipo di regimi e di vari altri regimi che da esso derivano come, ad esempio, quello relativo alla responsabilità da prodotto (*product liability*), alla responsabilità collegata alla circolazione dei veicoli, così come regimi che riguardano settori specifici (ad esempio, il settore medico o il finanziario). In questi casi la parte danneggiata dovrà provare il danno subito, l'anomalia che a suo dire ha provocato il danno e il nesso di causalità intercorrente tra questi ultimi, mentre al danneggiante spetterà fornire la prova di non aver cagionato alcun danno o di aver fatto tutto il possibile per evitare il prodursi di

²⁷ S. DE CONCA, *Bridging the Liability Gaps: Why AI Challenges the Existing Rules on Liability and How to Design Human-empowering Solutions*, in *Law and Artificial Intelligence*, Springer, v. 35, 2022, pp. 239-256.

detto danno. La configurazione di queste forme di responsabilità le rende particolarmente appropriate a disciplinare casi di esercizio di attività pericolose, come la guida di autoveicoli, o situazioni di asimmetria informativa o di potere, come nel caso dell'utilizzo di prodotti difettosi da parte dei consumatori. Pur ammettendo che tali forme di responsabilità oggettiva possano effettivamente regolamentare i casi in cui si producano danni cagionati da sistemi di IA, va tuttavia ricordato che si tratta di regimi che costituiscono un'eccezione alla norma; non potranno, quindi, applicarsi come norma generale, limitandosi a disciplinare determinati settori e circostanze. Una soluzione potrebbe essere rappresentata dalla creazione di un regime speciale di responsabilità oggettiva *ad hoc* per l'intelligenza artificiale, tale da disciplinare i casi in cui allocare la responsabilità civile "secondo giustizia" risulti particolarmente difficile nel contesto normativo così delineato. Probabilmente si tratta di un'idea irrealizzabile, benché allettante, dal momento che i sistemi di IA presentano una vasta gamma di applicazioni ed usi in quasi tutti i settori economici e l'applicazione di un solo, identico regime di responsabilità appare problematica.²⁸

Se da un lato, allora, vi è chi propone di risolvere il problema dell'imputazione della responsabilità mediante l'applicazione del criterio della responsabilità oggettiva, attraverso la creazione di una responsabilità *ad hoc*, piuttosto che attraverso un'interpretazione evolutiva o una applicazione analogica di norme giuridiche già esistenti (siano esse quelle in materia di responsabilità civile extra-contrattuale dei singoli ordinamenti o quelle contenute nella direttiva 85/374/CEE in tema di responsabilità del produttore), dall'altro vi è chi reputa più appropriato il riconoscimento di una soggettività giuridica direttamente in capo ai dispositivi di IA. Proprio sulla disamina di queste due prospettive si incentrano i capitoli che seguono, che cercheranno di mettere in luce le problematiche connesse con ciascuna delle proposte avanzate dagli studiosi che pionieristicamente si sono occupati del tema.

²⁸ S. DE CONCA, *Bridging the Liability Gaps: Why AI Challenges the Existing Rules on Liability and How to Design Human-empowering Solutions*, in *Law and Artificial Intelligence*, Springer, v. 35, 2022, pp.248-249.

II. L'attuale panorama giuridico e le prospettive europee: un nuovo paradigma per l'intelligenza artificiale?

1. La normativa allo stato dell'arte: la direttiva 85/374/CEE e le sue criticità. 2. La nuova proposta di Direttiva della Commissione europea. 3. Sistemi di Intelligenza artificiale: res o centri di imputazione giuridica?

1. La normativa allo stato dell'arte: la Direttiva 85/374/CEE e le sue criticità

1.1 Il modello della Product Liability: natura, oggetto e finalità della normativa unionale

Con la direttiva 85/374/CEE - recepita a livello nazionale dal D.P.R. 24 maggio 1988 e poi trasfusa nel codice del consumo agli articoli 114 e ss. - il legislatore europeo armonizza le legislazioni degli Stati membri in materia di risarcimento dei danni cagionati da prodotti difettosi, riconoscendo in capo al produttore del prodotto difettoso una responsabilità oggettiva, autonoma e diversa rispetto a quella del venditore. Si tratta di una normativa inizialmente concepita con l'obiettivo di rafforzare il mercato unico mediante il bilanciamento tra gli interessi dei consumatori e quelli dei produttori, benché abbia poi acquisito ulteriori funzioni come assicurare una tutela effettiva ai danneggiati e, al contempo, incoraggiare l'innovazione. Proprio tali finalità hanno indotto le istituzioni comunitarie a commissionare una serie di studi e di rapporti incentrati sulla valutazione dell'adeguatezza di tale normativa a disciplinare le nuove sfide delle tecnologie digitali. La fiducia che le istituzioni comunitarie ripongono nella disciplina della responsabilità del produttore, tuttavia, pare stridere con la bassa incidenza, denunciata da tempo dalla dottrina che si occupa della materia, che la stessa sembra avere nelle corti giudiziarie degli Stati membri; basti pensare al fenomeno tutto italiano della "fuga dalla disciplina del danno da prodotto difettoso", ovvero alla tendenza dei giudici italiani a prediligere l'applicazione di altre norme che permettano al danneggiato di ottenere un

risarcimento, in particolare l'art. 2050 c.c. sulla responsabilità per esercizio di attività pericolosa. Va tuttavia ricordato come la giurisprudenza della Corte di giustizia dell'Unione europea abbia ultimamente cercato di rivitalizzare la disciplina della direttiva in materia di *product liability*, con l'obiettivo di creare una forma di tutela che sia invocabile in alternativa o in concorso con le tutele previste dai singoli Stati membri. Questa soluzione garantisce il rispetto del principio di effettività della tutela, principio che, assieme a quello di neutralità tecnologica contraddistingue la materia. Dalla neutralità tecnologica deriva che a coloro che abbiano subito un danno cagionato da un prodotto intelligente debba essere assicurato un grado di tutela pari a quello assicurato agli utenti dei prodotti tradizionali: si parla, a questo riguardo, di principio di c.d. equivalenza funzionale, il quale costituisce un corollario del principio di effettività della tutela.²⁹ La normativa in esame si ispira ad un principio di *favor* per il danneggiato: il legislatore aggrava la posizione del produttore ponendo in capo a quest'ultimo il rischio del verificarsi di un danno dovuto alla difettosità del prodotto e riconosce al consumatore danneggiato il diritto al risarcimento del danno ogni qual volta riesca a fornire la prova del danno, del difetto del prodotto e del nesso di causalità tra danno e difetto. La direttiva si pone pertanto l'obiettivo di alleggerire la posizione processuale del danneggiato, non richiedendo che egli fornisca la prova dell'elemento soggettivo dalla colpa del produttore, la responsabilità del quale verrà accertata anche qualora il difetto non dovesse dipendere dalla mancanza di diligenza nella progettazione o nella fabbricazione del prodotto o, ancora, nelle informazioni che devono essere fornite al consumatore. La legislazione in materia di *product liability* pare essere, tenuto conto della natura, dell'oggetto e delle finalità, la più appropriata a disciplinare la responsabilità per danni cagionati dai dispositivi intelligenti o, quanto meno, a costituire un modello normativo dal quale trarre spunto per poter eventualmente procedere ad una normazione della "responsabilità da robot" che non

²⁹ R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law*, in *Persona e Mercato* 2020/4, pp. 366-368.

si limiti al solo ambito della *consumer protection*.³⁰ La stessa direttiva 85/374/CEE viene citata nella sopra menzionata Risoluzione del Parlamento europeo del 2017. È opportuno, pertanto, soffermarsi sugli aspetti principali che caratterizzano la normativa in esame per verificare se le nozioni di produttore, prodotto e difetto siano sufficientemente ampie ed elastiche da poter essere applicate anche in relazione alle nuove tecnologie.

1.2 La nozione di prodotto

La nozione di prodotto individuata dalla direttiva 85/374/CEE risulta particolarmente rilevante al fine di verificare se la stessa sia capace di includere anche i prodotti dotati di intelligenza artificiale. L'art. 115 del Codice del consumo, il quale recepisce l'art. 2 della Direttiva *Product Liability*, definisce prodotti “*ogni bene mobile, anche se incorporato in altro bene mobile o immobile*”. Il primo interrogativo che tale definizione pone, dunque, riguarda la possibilità di considerare i dati, l'algoritmo o il *software* come prodotti ai sensi di tale disciplina. Si tratta di elementi immateriali che, anche quando incorporati in un bene mobile tecnologico caratterizzato da materialità, assumono spesse volte il peso maggiore sia dal punto di vista economico, sia per quanto concerne il rischio del prodursi di un danno. Alla luce di quanto appena detto, i commentatori della direttiva si sono concentrati, inizialmente, sull'opportunità di ricondurre il *software* alla categoria del prodotto, piuttosto che a quella del servizio. Va ricordato, infatti, che la normativa sul danno da prodotto difettoso non si applica ai servizi; si tratta di una scelta di *policy*, la quale è stata ribadita anche dalla Corte di giustizia UE nel 2011 nel caso *CHU Besançon*.³¹ Non sembra porre problemi l'ipotesi in cui il *software* intelligente sia inserito in un *hardware*, in un bene mobile o prodotto finale: quest'ultimo è soggetto all'applicazione della disciplina sul danno da prodotto

³⁰ A. AMIDEI, *Robotica intelligente e Responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Intelligenza Artificiale e Responsabilità*, a cura di Ugo Ruffolo, 2017, p. 88.

³¹ Corte di giustizia dell'Unione europea, 21 dicembre 2011, ECLI:EU: C:2011:869, *Centre hospitalier universitaire de Besançon v. Thomas Dutrueux & Caisse primaire d'assurance maladie du Jura*, curia.europea.eu/juris/documents.jfs?num=C-495/10: (cfr. par. 35).

difettoso e il produttore del prodotto finale sarà responsabile in solido con il produttore della componente. Più problematica risulta, invero, la possibilità di considerare il *software* un prodotto ai sensi della Direttiva 85/374/CEE quando il *software* non sia incorporato in un prodotto finale *hardware* e venga, perciò, venduto solo. E le incertezze crescono nel caso di sistema intelligente capace di autoapprendimento, dotato di un *software* la cui anima è costituita da un bene ancora più immateriale del *software* stesso, quale è l'algoritmo; si tratta, infatti, di una formula matematica o una linea di codici spesso ideata da un soggetto diverso sia dal produttore del bene finale, che dal produttore del *software* e, talvolta, creato tempo addietro rispetto al momento in cui il prodotto finale nel quale è incorporato viene messo in commercio.

Per quanto riguarda la possibilità di qualificare il *software* come prodotto, è bene ricordare che la stessa nozione di "prodotto" di cui all'art. 2 della Direttiva non fa alcun riferimento al carattere materiale degli stessi; al contrario, menziona una serie di esempi di cosa il legislatore intenda per "*movables*", specificando che anche l'elettricità, bene certamente immateriale, è considerata "prodotto" ai sensi della Direttiva. La lettura dell'art. 2 si è prestata, tuttavia, a varie interpretazioni, le quali hanno condotto principalmente a due opzioni che permettono di includere il *software* all'interno della categoria dei prodotti. La prima opzione si fonda su un'interpretazione ampia di "*movables*", la quale include qualsiasi cosa che non sia un bene immobile o un servizio; l'altra opzione, invece, consiste in una interpretazione analogica dell'art. 2, al fine di farvi rientrare i beni immateriali. Ciò che più confonde è il fatto che il legislatore europeo menzioni, successivamente, un elenco di esempi che riguardano tutti beni materiali, salvo poi aggiungere, alla fine, che anche l'elettricità deve essere considerata un prodotto. Vi è chi, allora, propende per la seconda opzione di lettura dell'art. 2, affermando che fosse intenzione del legislatore definire il prodotto come un bene materiale; di lì la necessità di aggiungere il riferimento all'elettricità come rientrante nella già menzionata categoria. Si potrebbe, tuttavia, replicare che l'elettricità venga citata solo come esempio di bene non materiale che rientra nella categoria di prodotto alla stregua di tutti gli altri beni materiali utilizzati come esempio dal legislatore e che il *software*, allora, costituisca un ulteriore esempio di bene non

materiale che può, ciononostante, essere considerato un “prodotto” ai sensi della Direttiva 85/374/CEE.³² Ancora, a proposito della possibilità di qualificare il *software* come prodotto, un’autorevole opinione³³ distingue tra *software* creato appositamente per il fruitore, avendo riguardo alle sue esigenze, e *software* prodotto in serie, integrato in un apposito bene mobile materiale e venduto al pubblico dei consumatori; solo quest’ultimo rientrerebbe nella nozione di “prodotto” di cui all’art. 2 della Direttiva *Product Liability*; tesi, quest’ultima, che si richiama alla dottrina statunitense, la quale propone di risolvere il problema attraverso l’analisi del caso concreto, andando a vedere, caso per caso, il tipo di contratto in base al quale il *software* viene fornito per comprendere se sia prevalente, o meno, la componente del servizio. Giova ricordare, tuttavia, che la disciplina del danno da prodotto difettoso si applica pacificamente anche ai prodotti non industriali: non è rilevante, a tale fine, che il bene sia realizzato in serie o su misura, richiedendosi solo che il bene risponda alle scarse caratteristiche indicate dalla Direttiva. E inoltre, sulla base delle considerazioni sopra esposte, appare privo di interesse il richiamo alla fisicità del supporto in cui il *software* dovrebbe essere integrato per poter essere soggetto alla normativa in esame. Anche sulla scorta di quanto sopra esposto, la dottrina maggioritaria ha optato per una interpretazione estensiva dell’art. 2 della Direttiva *Product Liability*, focalizzandosi, in particolare, sugli obiettivi che la stessa si propone di perseguire; difatti, la soluzione restrittiva per la quale il *software*, essendo bene immateriale, non dovrebbe essere considerato un “prodotto” ai fini dell’applicazione della normativa in materia di danno da prodotto difettoso condurrebbe ad escludere dal novero delle tutele offerte ai danneggiati da prodotti tradizionali difettosi, coloro che siano danneggiati dai nuovi prodotti delle tecnologie digitali.³⁴ E tale risultato contrasterebbe non solo con lo scopo di tutela del

³² G. WAGNER, *Robot Liability*, p. 11.

³³ G. PONZANELLI, *Responsabilità per danno da computer: alcune considerazioni comparative*, in *Resp. civ. prev.*, 1991, p. 653, A. ZACCARIA, *La responsabilità del “produttore” di software*, p. 303. *Contra*, invece, G. ALPA, *Responsabilità extracontrattuale ed elaboratore elettronico*, in *Diritto dell’informazione e dell’informatica*, 1986, p. 385.

³⁴ R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft e hard law*, in *Persona e Mercato*, 2020/4, pp. 371-372.

consumatore che la Direttiva mira a conseguire (e, di conseguenza, con il principio di effettività della tutela e con il suo corollario, il principio di equivalenza funzionale), ma anche con il principio di neutralità tecnologica, al quale l'intera normativa in questione è ispirata. La stessa Commissione europea ha affermato espressamente nel 1988 che il *software* deve essere considerato un prodotto ai sensi dell'art. 2 della Direttiva sul prodotto difettoso, pur non chiarendo se alla medesima conclusione possa pervenirsi nel caso di *software* non incorporato in un supporto fisico; mentre la Corte di giustizia ha qualificato il *software* come dispositivo medico, soggetto pertanto alle relative disposizioni di sicurezza, quando il suo produttore abbia assegnato allo stesso uno scopo medico-sanitario.³⁵ Sulla scia di tali pronunce, il Regolamento 2017/745/UE del Parlamento europeo e del Consiglio del 5 aprile 2017, in vigore dal 26 maggio 2020, relativo ai dispositivi medici, include il *software* tra i dispositivi medici, o lo considera comunque parte integrante degli stessi, equiparandolo dunque ad un prodotto (anche se solo ai fini della disciplina ivi contenuta).

1.2.1 Update e upgrade del software: si può ancora parlare di prodotto?

Le cose si fanno più complicate allorché si introduce il concetto di "aggiornamento" del *software*. Tre possibili soluzioni sono state individuate dalla dottrina. La prima consiste nel qualificare l'aggiornamento come un pezzo del prodotto al quale accede, vale a dire un prodotto esso stesso; questo condurrebbe a ritenere che, se si ammette che la Direttiva *Product Liability* sia applicabile al *software* in quanto prodotto, ecco che allora anche l'aggiornamento dovrebbe essere soggetto all'applicazione della Direttiva qualora la difettosità di quest'ultimo fosse causa del verificarsi di un danno. Diversamente, vi è chi ritiene che l'aggiornamento debba essere considerato un mero servizio che accede al *software* di base, essenziale per evitare un malfunzionamento dello stesso in futuro; da questo punto di vista, l'aggiornamento non può essere considerato un prodotto. Infine, una terza soluzione

³⁵ Corte di Giustizia dell'Unione europea, 22 novembre 2022, Brian Products, C-219/11; 15 gennaio 2009, Hecht-Pharma, C-140/07.

intermedia distingue fra *updates* e *upgrades*. In accordo con questa terza via solo l'*upgrade* dovrebbe essere considerato un prodotto, poiché in grado di aggiungere nuove funzionalità alla precedente versione del *software*; l'*update*, viceversa, andrebbe qualificato come mero servizio. La soluzione intermedia è senz'altro ragionevole, pur presentando alcuni inconvenienti. Risulta, infatti, non sempre agevole utilizzare il criterio delle nuove funzionalità per distinguere tra *update* e *upgrade*, con il rischio che colui che sviluppa il *software* abbia la possibilità di decidere se essere o meno soggetto alla Direttiva, qualificando egli stesso la parte del *software* che mette in commercio. Diverrebbe cruciale, allora, definire cosa siano le “minori funzionalità” che qualificano l'*update* e le “maggiori funzionalità” che qualificano l'*upgrade*; tale sfida definitoria farebbe tuttavia sorgere una grande incertezza giuridica.³⁶

1.2.2 L'algoritmo quale componente del prodotto finale

Quanto detto circa la possibilità di includere il *software* nella nozione di prodotto o di componente del prodotto finale non esaurisce la disamina della questione; invero, rimane da affrontare il problema della qualificazione dell'algoritmo. Quando si parla di dispositivi intelligenti con capacità di autoapprendimento, difatti, ci si riferisce a sistemi in cui non solo l'algoritmo è presente, ma anche prevalente nel conferire i caratteri tipici del *machine learning*; e proprio da un difetto di tale algoritmo può derivare un danno non previsto o non prevedibile né dal produttore del prodotto finale o del *software*, né dall'ideatore dello stesso algoritmo. Risulta in effetti complesso qualificare l'algoritmo - mera linea di codice, pertanto bene decisamente immateriale - come “prodotto” ai sensi dell'art. 2 della Direttiva. Tuttavia, anche in questo caso è possibile interpretare estensivamente la nozione di prodotto e, procedendo ad una lettura teleologicamente orientata, considerare l'algoritmo quantomeno “componente” del prodotto finale. Ciò comporterebbe il sorgere di una autonomia e diretta responsabilità dell'ideatore dell'algoritmo per i danni provocati da un difetto dello

³⁶ M. CHATZIPANAGIOTOIS, *Product Liability Directive and Software Updates on Automated Vehicles*, in *Proceedings of SETN 2020, 11th Hellenic Conference on Artificial Intelligence* (SETN, 2020).

stesso, che può consistere anche in una condotta imprevista del dispositivo; responsabilità che, ai sensi della Direttiva, sarebbe concorrente e solidale con quella del produttore del bene finale. La Direttiva 85/374/CEE configura, infatti, una responsabilità diretta, nei confronti del soggetto leso, gravante su tutti i soggetti che abbiano preso parte al processo produttivo in quanto produttori di una componente del prodotto finale, laddove la difettosità del primo sia stata causa del danno cagionato attraverso l'impiego del secondo. Tale soluzione ermeneutica se, da un lato, potrebbe apparire iniqua per il produttore del bene finale, chiamato a rispondere di un comportamento della macchina intelligente spesso non prevedibile ed oscuro nel suo processo di sviluppo, dall'altro risulta essere la strada più idonea a tutelare in maniera adeguata il consumatore, per il quale sarebbe estremamente complesso, se non addirittura a volte impossibile, risalire all'ideatore dell'algoritmo o anche solo identificare un algoritmo difettoso coinvolto nella verifica del danno; per contro, risulta più agevole, per quest'ultimo, identificare il produttore finale del dispositivo di *machine learning*.³⁷ Rimane priva di risposte, invece, la questione dell'applicabilità della Direttiva per danno da prodotto difettoso al caso in cui l'algoritmo non sia incorporato in un *hardware* o in un *software*, ma ceduto separatamente (c.d. "*stand-alone algorithm*"); seppure si tratti di una problematica sollevata da alcuni commentatori, non vi è dubbio che lo spazio ad essa riservato sia meramente residuale dal punto di vista della tutela del consumatore, tenuto conto del fatto che risulta difficile che un consumatore possa voler acquistare e utilizzare un algoritmo che non sia inserito in un dispositivo intelligente, sia esso un *software* o un *hardware*.³⁸

1.2.3 La fondamentale distinzione fra prodotto e servizio

Un'ultima, interessante questione riguarda le dinamiche dell'*Internet of Things (IoT)* e le problematiche sollevate dalla difficoltà di distinguere, in tale ambito, tra prodotto

³⁷ L. DI DONNA, *Software intelligenti e responsabilità del produttore*, in *Intelligenza artificiale e rimedi risarcitori*, 2022, pp. 91-93.

³⁸ A. AMIDEI, *Le responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in *XXVI Lezioni di diritto dell'intelligenza artificiale*, Ugo Ruffolo (a cura di), 2021, p. 153-154.

e servizio. Quando si parla di *IoT* ci si riferisce alla possibilità che una molteplicità di dispositivi intelligenti siano tra loro connessi e interagiscano grazie alla rete, consentendo, tale coordinamento, prestazioni e risultati che il singolo prodotto non potrebbe raggiungere. La prestazione finale che discende dal modo di operare dei prodotti attraverso il *network* non può essere considerata la somma delle prestazioni dei singoli, ma va configurata come qualcosa di nuovo e di diverso, più simile alla concezione di servizio che a quello di prodotto; in questo modo il produttore non solo offre un dispositivo intelligente, ma anche un servizio intelligente, quale risultato dell'interagire e della connessione di tali dispositivi grazie alla rete. Sorge quindi il problema, per il consumatore, di stabilire se il danno subito sia stato cagionato dal difetto di un dispositivo intelligente, ovvero da un difetto sviluppatosi nel processo di connessione tra più prodotti imputabili a diversi produttori e, dunque, da un difetto non del prodotto, bensì del servizio intelligente complessivo.³⁹

1.3 I legittimati passivi

Per ciò che concerne i legittimati passivi l'art. 3 della Direttiva 85/374/CEE include nella nozione di produttore non solo colui che realizza il prodotto finale, bensì anche il fabbricante della componente di tale prodotto e il fornitore della materia prima.⁴⁰ Ciò significa che, qualora si consideri il *software* o l'algoritmo una componente del prodotto finale, al consumatore sarà riconosciuta la possibilità di esperire un'azione di risarcimento del danno direttamente nei confronti di questi soggetti; ma sarà possibile anche - data la difficoltà che spesso i consumatori incontrano nel risalire alla fonte del difetto o all'identità dello sviluppatore del *software* o del creatore dell'algoritmo – agire nei confronti del produttore del bene che incorpora tali componenti. Qualora,

³⁹ L. DI DONNA, *Software intelligenti e responsabilità del produttore*, in *Intelligenza artificiale e rimedi risarcitori*, 2022, pp. 93-95.

⁴⁰ Ai sensi dell'ottavo considerando della Direttiva, inoltre "ai fini della protezione del consumatore è necessario considerare responsabili tutti i partecipanti al processo produttivo se il prodotto finito o la parte componente o la materia prima da essi fornita sono difettosi". La disciplina in questione responsabilizza anche colui che importi il prodotto difettoso all'interno dell'Unione europea, così come "chiunque si presenti come produttore apponendo il suo nome, marchio o altro segno distintivo" o "fornisca un prodotto il cui produttore non possa essere identificato".

invero, ci si trovi di fronte a dispositivi le cui componenti siano immesse sul mercato separatamente rispetto all'*hardware*, sarà necessario per il danneggiato indagare da dove provenga il difetto che ha cagionato il danno, non potendo agire nei confronti del produttore del bene finale se, ad esempio, il danno discenda da un difetto del *software* introdotto sul mercato da un fornitore del *software* originale, ovvero da un difetto del *software* prodotto da un terzo ed installato sul dispositivo dall'utente stesso, o ancora da un difetto di alcune modificazioni apportate dall'utente successivamente all'acquisto del dispositivo. Gli eventuali scenari appena prospettati implicano un aggravio (ulteriore rispetto a quelli di cui si dirà qui di seguito) dell'onere della prova a carico del danneggiato, scoraggiando l'instaurazione della causa davanti al giudice o minando il successo di azioni meritorie.⁴¹ Infine, merita un accenno la questione legata alle figure professionali del *trainer* e del *trainer data*. Il problema discende dall'inquadramento di tali figure come fornitori di servizi che, in quanto tali, non partecipano al processo di produzione e commercializzazione del prodotto intelligente, ma operano in una fase temporale che si colloca tra la produzione e la messa in commercio del dispositivo. Ciò comporta che ad essi non si applichi la Direttiva *Product Liability*, con la conseguenza che il danneggiato non potrà esperire azione diretta nei confronti di questi soggetti se entrambi diversi dai soggetti indicati dalla Direttiva. Il danneggiato potrà allora agire nei loro confronti soltanto in base alle norme codicistiche in materia di responsabilità extracontrattuale. Risulta, tuttavia, discutibile non considerare il *trainer* e il fornitore dei *training data* soggetti che non partecipano al processo produttivo del dispositivo intelligente, incidendo sia l'addestramento che i dati alla base dello stesso sul processo di autoapprendimento che lo caratterizza.⁴² Con una efficace immagine A. Amidei li paragona al carburante

⁴¹ G. WAGNER, *Robot Liability*, p. 15.

⁴² L. DI DONNA, *Software intelligenti e responsabilità del produttore*, in *Intelligenza artificiale e rimedi risarcitori*, 2022, pp. 95-96.

dell'automobile, necessario per il funzionamento della macchina e possibile fonte di danni, ma non passibile di essere considerato una componente.⁴³

1.4 La spinosa questione del prodotto difettoso

Prima di affrontare il tema della applicabilità della nozione di difetto ai prodotti delle tecnologie digitali, giova soffermarsi brevemente sull'analisi della definizione di "prodotto difettoso" ai sensi della Direttiva *Product Liability*. La nozione di "prodotto difettoso" di cui all'art. 6 della Direttiva 85/374/CEE è stata oggetto di grande dibattito fra i commentatori della normativa in esame, dibattito dovuto, da un lato, alla correlazione che tale definizione crea con una diversa ma complementare normativa, ossia la Direttiva 2001/95/CE del Parlamento europeo e del Consiglio del 3 dicembre 2001 relativa alla sicurezza generale dei prodotti, dall'altro alla possibilità di applicare i criteri individuati dalla definizione in questione alle nuove tecnologie digitali con le incertezze e le difficoltà che ciò comporta. L'art. 6 stabilisce che il prodotto è difettoso *"quando non offre la sicurezza che ci si può legittimamente attendere tenuto conto di tutte le circostanze, e tra esse la presentazione del prodotto, l'uso cui è destinato ed il momento della sua messa in circolazione"* alla luce delle legittime aspettative dei consumatori. Va anzitutto osservato come la nozione di difetto non coincida né con quella di "vizio" del bene venduto di cui agli artt. 1490 ss. del Codice civile (laddove si desume che vizio è il difetto che rende la cosa inidonea all'uso cui è destinata o che ne diminuisce in modo apprezzabile il valore), né con quella di difetto di conformità introdotto dalla disciplina sulla vendita dei beni di consumo.⁴⁴ Si tratta, invero, di un concetto che va interpretato in modo più elastico, tenuto conto del richiamo che il legislatore europeo fa alle legittime aspettative di sicurezza; non solo, allora, vi sarà un prodotto difettoso allorquando sia presente un difetto di fabbricazione o un difetto di progettazione in senso stretto che rendano la cosa inidonea all'uso, ma anche di fronte al cagionarsi di danni che siano dipesi da una mancanza di sicurezza nelle

⁴³ A. AMIDEI, *Intelligenza Artificiale e responsabilità da prodotto*, in RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti l'etica*, 2020, p. 137.

⁴⁴ Trib. Modena, Sez. I, 14 marzo 2011, in *Resp. civ.*, 2011, 794.

condizioni di utilizzo del prodotto che pur non presenti alcun difetto di fabbricazione dal punto di vista tecnico. Come specificato poi dall'art. 117 cod. cons., che recepisce il già citato art. 6 della Direttiva, l'insicurezza va verificata sulla base di varie circostanze, tra cui l'uso al quale il prodotto può essere ragionevolmente destinato, i comportamenti che si possono ragionevolmente prevedere in relazione ad esso o le istruzioni che accompagnano la messa in circolazione del prodotto. Si pensi, ad esempio, ad un giocattolo che non presenti alcun difetto di fabbricazione e del quale venga fatto un uso improprio; non è possibile, nemmeno in questo caso, escludere la difettosità del prodotto, posto che il produttore avrebbe dovuto prevedere tale possibile uso anomalo e adottare tutti gli accorgimenti necessari ad evitarlo.⁴⁵ La mancanza di sicurezza che il comma 1 dell'art. 117 cod. cons. lega alla difettosità, dunque, altro non è che la difformità che sussiste tra le condizioni di sicurezza concretamente offerte dal prodotto e quelle che, dallo stesso, è legittimo attendersi.⁴⁶ Come si accennava precedentemente, il richiamo alla sicurezza configura una complementarità tra la disciplina in materia di responsabilità del produttore e quella relativa alla sicurezza generale dei prodotti; la sicurezza, infatti, rappresenta l'indispensabile condizione di accesso al mercato europeo dei prodotti, condizione soddisfatta qualora i prodotti presentino i requisiti essenziali di sicurezza prescritti dalle direttive di carattere verticale (le quali disciplinano specifiche categorie di prodotti) o, in assenza, qualora rispondano alle caratteristiche del "prodotto sicuro" di cui alla direttiva sulla sicurezza generale dei prodotti. Tale precisazione risulta essenziale segnatamente in relazione al tema dell'onere della prova: il danneggiato dovrà provare non solo il danno cagionato dal prodotto, ma anche la difettosità del prodotto e il nesso di causalità tra difetto e danno. La stessa giurisprudenza ritiene che l'oggetto dell'onere della prova gravante sul danneggiato non coincida con uno specifico vizio di progettazione o di fabbricazione in senso tecnico, ma corrisponda ad una più estesa nozione di sicurezza

⁴⁵ G. STELLA, *Causa ignota del danno derivante dall'uso del prodotto e responsabilità del produttore per prodotto difettoso*, in *Responsabilità civile e previdenza*, n. 5/2017, pp. 1445-1447.

⁴⁶ E. BELLISARIO, *Il danno da prodotto conforme tra regole preventive e regole risarcitorie*, in *Europa e diritto privato*, 2016, p. 34.

nel senso sopra ricordato. Si sviluppa a questo proposito un orientamento giurisprudenziale fatto proprio, in particolare, dai giudici di merito, secondo il quale, sulla base di un ragionamento logico-presuntivo, l'insicurezza del prodotto sarebbe provata ogni qual volta risulti che l'utente abbia subito un danno in occasione di un utilizzo normale del prodotto, escludendosi dunque qualsiasi uso anomalo o improprio da parte dell'utente. Si tratta, a ben vedere, di un alleggerimento dell'onere probatorio per il danneggiato, soprattutto se comparato con l'oggetto dell'onere che grava su chi agisce in giudizio ai sensi dell'art. 2043 c.c., il quale dovrà non solo provare il danno e il nesso di causalità tra questo e un fatto illecito, ma anche la colpa del soggetto agente quale elemento costitutivo del fatto illecito.

1.4.1 La responsabilità del produttore alla luce della nozione di difetto: responsabilità oggettiva o presunta?

Proprio tale agevolazione sotto il profilo dell'onere della prova che le norme del Codice del consumo riconoscono all'utente danneggiato ha fatto sì che tradizionalmente la responsabilità del produttore si configuri come responsabilità oggettiva⁴⁷, ossia fondata sul nesso causale tra difetto e danno e indipendente da qualsiasi negligenza, imprudenza o imperizia del produttore. Più precisamente, si parla a tale riguardo di responsabilità oggettiva relativa o parziale, da contrapporsi alla responsabilità oggettiva assoluta: il produttore non si libera dando una generica dimostrazione di diligenza o mancanza di colpa, pur potendo tuttavia addurre la sussistenza di una delle tassative cause di esonero dalla responsabilità di cui all'art. 118 cod. cons. Tale articolo prevede l'esclusione della responsabilità del produttore in una serie di casi tassativi, solo alcuni dei quali coincidono con la mancanza di colpa. Ecco allora che si ammette che in taluni casi la diligenza del danneggiante assuma rilevanza. Più recentemente, invero, la Corte di legittimità ha adottato un orientamento

⁴⁷ Cass. civ., 1° giugno 2010, n. 13432: "il d.P.R. n. 224/1988 pone a carico del produttore una responsabilità extracontrattuale di natura oggettiva, posto che il produttore è responsabile delle conseguenze della difettosità del prodotto prescindendo ed anche in assenza di una colpa nella creazione della difettosità".

secondo il quale la responsabilità del produttore non ha natura di responsabilità oggettiva (sebbene parziale o relativa), ma di responsabilità presunta, dal momento che prescinde dall'accertamento della colpevolezza del produttore, "ma non anche dalla dimostrazione dell'esistenza di un difetto del prodotto utilizzato".⁴⁸ Il danneggiato dovrà allora provare il nesso di causalità tra difetto del prodotto e danno, non essendo sufficiente la prova di un nesso causale tra il danno e l'utilizzo del prodotto. La formulazione di una responsabilità del produttore in termini di responsabilità oggettiva piuttosto che di responsabilità presunta è stata nondimeno oggetto di grande confusione, dato l'utilizzo alternativo che la Cassazione ha fatto di questi termini negli ultimi anni. Come osservato da G. Stella entrambe le qualificazioni sembrano essere compatibili con il modello della responsabilità del produttore di cui alla Direttiva 85/374/CEE: responsabilità oggettiva in quanto il danneggiato non deve provare la colpa del produttore e responsabilità presunta in quanto una volta provato il danno, il difetto e il nesso di causalità tra difetto e danno la responsabilità del produttore si presume, salva la prova contraria ai sensi dell'art. 118 cod. cons.⁴⁹

1.4.2 Il requisito dell'insicurezza

Sempre la giurisprudenza di legittimità chiarisce, inoltre, nel suo più recente orientamento che ai fini della prova della difettosità del prodotto non è sufficiente la dimostrazione di una sua genericainsicurezza, intesa come mancanza di una condizione oggettiva di innocuità del bene, essendo necessaria piuttosto la prova di unainsicurezza qualificata; tale specificainsicurezza si delinea sulla base dei parametri di cui all'art. 117 cod. cons., come integrati dagli art. 103 ss. cod. cons. (i quali recepiscono la normativa in materia di sicurezza generale dei prodotti). Si tratta, allora, di prendere atto del fatto che esistono prodotti che per loro natura presentano un certo grado diinsicurezza ineliminabile (i così detti *unavoidably unsafe products*), i quali non per ciò solo possono considerarsi difettosi e dannosi; sarà quindi necessario

⁴⁸ Cass. civ., 28 luglio 2015, n. 15851; Cass. civ., 19 febbraio 2016, n. 3258.

⁴⁹ G. STELLA, *Causa ignota del danno derivante dall'uso del prodotto e responsabilità del produttore per prodotto difettoso*, in *Responsabilità civile e previdenza*, n. 5/2017, pp. 1455-1456.

per il danneggiato provare l'esistenza di un difetto in senso tecnico di progettazione o di fabbricazione o, per coloro che accolgono l'interpretazione più elastica di cui si è dato conto precedentemente, dimostrare che il danno si è prodotto in presenza di un uso normale e ragionevole del prodotto e in assenza di cause esterne che possano aver inciso sulla sua verifica, pur senza allegare la prova di un vero e proprio vizio in senso tecnico del bene. Grande importanza riveste, a questo proposito, la complessa questione della causa ignota del danno, che si muove sulla linea di confine fra il concetto di "causa del danno" e di "causa del difetto" e che, a conti fatti, dipende dall'interpretazione più restrittiva o più estesa del concetto di "difetto". Come evidenziato da G. Stella pare più coerente sia con la formulazione normativa dell'art. 117 cod. cons., sia con le istanze di protezione dell'utente ad essa sottese ritenere che, al fine di provare la difettosità del prodotto il danneggiato non sia tenuto a dimostrare l'esistenza di uno specifico vizio del prodotto e del nesso di causalità fra questo e il danno subito, ma debba piuttosto provare una serie di circostanze riguardanti l'uso del prodotto dalle quali sia possibile presumere, attraverso un ragionamento logico-deduttivo, l'insicurezza di quest'ultimo e che da questa sia derivato un danno. Una volta accertato che il prodotto è insicuro in relazione alle condizioni normali e ragionevolmente prevedibili di impiego e che da ciò è derivato un danno, il produttore risulta essere responsabile anche qualora la causa di tale insicurezza qualificata, ossia la causa del difetto, rimanga ignota.

1.4.3 Le cause di esclusione della responsabilità del produttore

Infine, per concludere la disamina del concetto di prodotto difettoso ai sensi della Direttiva sulla responsabilità del produttore e completare il tema inerente all'onere della prova, si rende necessaria l'analisi del già richiamato art. 118 cod. cons., il quale prevede l'esclusione della responsabilità del produttore in alcuni casi tassativi. Quelli che più rilevano ai fini di questa trattazione sono, nello specifico, l'ipotesi in cui "b) ...il difetto che ha cagionato il danno non esisteva quando il produttore ha messo il prodotto in circolazione"; e l'ipotesi in cui "c) ...lo stato delle conoscenze scientifiche

e tecniche, al momento in cui il produttore ha messo in circolazione il prodotto, non permetteva ancora di considerare il prodotto come difettoso". La prima ipotesi riconosce al produttore la possibilità di dimostrare che il difetto, e quindi il fattore di insicurezza qualificata, si è sviluppato in un momento successivo alla messa in commercio del prodotto e, quindi, esclusivamente a causa del fatto di un terzo o del comportamento dello stesso danneggiato. Rileva dunque il tempo in cui il prodotto è stato immesso nel mercato, essendo qualsiasi difetto sopravvenuto successivamente a quel momento non imputabile al produttore. La seconda ipotesi, invece, prevede il c.d. "rischio da sviluppo", ossia il caso in cui il difetto esistesse già al momento della messa in circolazione del bene, pur tuttavia non potendo essere identificato non solo dallo stesso produttore, ma da qualunque soggetto sulla base delle conoscenze tecniche e scientifiche esistenti in quel dato momento storico; si deve trattare, pertanto, di una non conoscibilità oggettiva e non di una lacuna del singolo produttore. Tornando al tema della causa ignota del danno, allora, una volta accertato che il danno è stato cagionato da un prodotto "difettoso" poiché insicuro, il produttore assume la responsabilità di tale danno anche se la causa specifica dell'insicurezza qualificata rimanga non conosciuta, salvo che riesca a provare una delle circostanze tassative di cui all'art. 118 cod. cons.⁵⁰

1.5 Il difetto nel prodotto intelligente

Una delle difficoltà che si incontrano quando si cerca di attrarre nel campo di applicazione della Direttiva *Product Liability* il prodotto intelligente è legata alla peculiarità di queste tecnologie di essere *open by design*, il che significa che al fine di funzionare adeguatamente necessitano di ulteriori integrazioni ed aggiornamenti della componente immateriale, successivi rispetto alla messa in commercio del prodotto stesso. Due concetti fondamentali, allora, vanno nuovamente sottolineati: la rilevanza del tempo della messa in circolazione del bene e l'opinione secondo cui

⁵⁰ G. STELLA, *Causa ignota del danno derivante dall'uso del prodotto e responsabilità del produttore per prodotto difettoso*, in *Responsabilità civile e previdenza*, n. 5/2017, pp. 1457-1465.

l'aggiornamento del *software* deve essere concepito come parte del prodotto finale e, dunque, esso stesso prodotto. Va ricordato, innanzitutto, come l'art. 7 della Direttiva 85/374/CEE esoneri il produttore dalla responsabilità qualora il difetto si manifesti dopo la commercializzazione del prodotto; l'aggiornamento viene rilasciato in un momento necessariamente successivo, con la conseguenza che solo considerando tale aggiornamento un vero e proprio prodotto si potrebbe imputare la responsabilità di un suo eventuale difetto al produttore. Tuttavia, questa estensione di responsabilità combinata con la natura oggettiva della stessa rischia di creare un contro-incentivo allo sviluppo degli aggiornamenti *software* determinando problemi di obsolescenza e di sicurezza dei prodotti in questione.⁵¹ Viene però sottolineato a tal proposito da R. Montinaro come anche il fatto che non vengano fornite modifiche o aggiornamenti previsti (e necessari, dunque, non solo per il funzionamento del dispositivo, ma anche per il mantenimento di un ragionevole livello di sicurezza) possa determinare la sussistenza di un difetto, in quanto il produttore verrebbe meno a quei doveri di monitoraggio della sicurezza dei prodotti che su di lui gravano anche dopo il momento della immissione in commercio. È necessario, pertanto, rovesciare l'approccio adottato con i prodotti tradizionali, che vede il controllo del fabbricante sul prodotto venir meno al momento della sua messa in circolazione; con il dispositivo intelligente il produttore continua a mantenere una stretta relazione, consentendogli ciò di monitorare lo stato di sicurezza e i possibili rischi connessi all'utilizzo del prodotto.⁵² La stessa prospettiva, poi, viene in rilievo con riferimento ai prodotti dotati di capacità di auto-apprendimento: in virtù del già citato controllo che il produttore dovrebbe esercitare sulla macchina, spetterebbe a lui adottare tutti gli accorgimenti tecnici necessari a governare tale autonomia, in difetto dei quali sarebbe tenuto a limitare tale capacità di auto-apprendimento, essendogli imputabili in caso contrario eventuali conseguenze dannose. Il presupposto normativo che permette di poter sostenere la tesi secondo cui

⁵¹ M. CHATZIPANAGIOTOIS, *Product Liability Directive and Software Updates of Automated Vehicles*, in *Proceedings of SETN 2020, 11th Hellenic Conference on Artificial Intelligence* (SETN 2020).

⁵² R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft e hard law*, in *Persona e Mercato*, 2020/4, pp. 375-377.

la Direttiva 85/374/CEE sarebbe applicabile anche in caso di difetto derivante dalla capacità di auto-apprendimento della macchina o di sua interazione con altri prodotti intelligenti nell'ambito dell'*Internet of Things* è, chiaramente, l'adozione di una prospettiva interpretativa che dilati il perimetro della nozione di "difetto" e lo allarghi a vizi non genetici del dispositivo⁵³, così come esposto precedentemente a proposito del requisito dell'insicurezza qualificata. Inoltre, la natura oggettiva (seppur relativa) della responsabilità del produttore ben si adatta al caso di comportamenti difettosi della macchina intelligente che dipendano dalla sua capacità di interazione con l'ambiente circostante, non essendo richiesta, in ogni caso, alcuna colpa del produttore ed essendogli imputabile la responsabilità anche nel caso in cui abbia agito diligentemente.

1.5.1 Le legittime aspettative di sicurezza degli utenti

Ciò chiarito con riferimento all'attitudine dei dispositivi intelligenti ad essere *open by design* e ad avere, in alcuni casi, capacità di auto-apprendere, rimane da analizzare il riferimento alle legittime aspettative di sicurezza degli utenti relativamente alle nuove tecnologie digitali. Per quanto riguarda i prodotti tradizionali, vi è chi lega indissolubilmente tali aspettative all'aderenza dei prodotti agli standard tecnici previsti dalla normativa di settore; va ricordato, infatti, che il legislatore ha predisposto complessi sistemi di regole tecniche che definiscono nel dettaglio le caratteristiche che determinati prodotti debbono presentare per poter essere considerati sicuri. Fra queste, grande rilevanza rivestono le cc.dd. "norme armonizzate", che l'UE promuove ma non impone. Il prodotto si presume sicuro se conforme a tali norme, così come stabilito dall'art. 105, co. 2, cod. cons.: si tratta di una presunzione relativa *iuris tantum*. Può accadere poi che, in alcuni casi, il legislatore stabilisca che le norme tecniche abbiano carattere obbligatorio al fine di tutelare interessi pubblici collettivi, quali la salute, la sicurezza o l'ambiente; in questo caso le regole tecniche sono contenute in regolamenti

⁵³ L. DI DONNA, *Software intelligenti e responsabilità del produttore*, in *Intelligenza artificiale e rimedi risarcitori*, 2022, p. 100.

cogenti e definiscono i requisiti essenziali di sicurezza che i prodotti debbono possedere. Tornando, quindi, al tema dell'incidenza della conformità del prodotto alle norme tecniche armonizzate al fine di esonerare il produttore da qualsiasi responsabilità va sottolineato come, a riguardo, la dottrina italiana sia prevalentemente orientata verso una soluzione negativa. A. Amidei ricorda, ad esempio, che la Direttiva 2001/95/CE precisa come la stessa non debba “*interferire*” con i diritti previsti dalla Direttiva 85/374/CEE e che, se certamente la verifica della difettosità del prodotto va eseguita anche sulla base della conformità dello stesso ai requisiti previsti dalla normativa tecnica di settore, ciò solo non è sufficiente ad escludere la difettosità del prodotto poiché così come la categoria del “prodotto dannoso” non si esaurisce del tutto in quella del “prodotto difettoso”, allora anche quest’ultima non si esaurisce del tutto nella categoria del “prodotto pericoloso”.⁵⁴ Anche E. Bellisario, al termine di una articolata analisi sulla complementarietà tra regole preventive e regole risarcitorie in materia di danno da prodotto conforme, sostiene che non vi possa essere coincidenza fra presunzione di sicurezza ai sensi della disciplina in materia di sicurezza dei prodotti e presunzione di non difettosità ai sensi della Direttiva *Product Liability*. La presunzione di sicurezza andrebbe relegata all’ambito di operatività della regolamentazione preventiva, il cui fine è l’immissione in commercio del prodotto; estendere la sua operatività in sede di tutela successiva vorrebbe dire disciplinare in modo identico situazioni considerate diverse dallo stesso legislatore, giacché l’obiettivo della tutela *ex post* è verificare se i danni cagionati debbano essere risarciti.⁵⁵ Il prodotto conforme agli standard di *product safety* potrà essere nondimeno difettoso, dal momento che tale standard individua un livello minimo di sicurezza; negare ciò porterebbe ad una considerevole diminuzione della tutela del consumatore.⁵⁶ La questione diventa ulteriormente complessa se si considera che in

⁵⁴ A. AMIDEI, *La responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in U. RUFFOLO, *XXVI Lezioni di diritto dell’intelligenza artificiale* (a cura di), 2020, p. 156.

⁵⁵ E. BELLISARIO, *Il danno da prodotto conforme tra regole preventive e regole risarcitorie*, in *Europa e diritto privato*, 2016.

⁵⁶ A. AMIDEI, *La responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in U. RUFFOLO, *XXVI Lezioni di diritto dell’intelligenza artificiale* (a cura di), 2020, p. 156.

settori come quello dell'*artificial intelligence*, caratterizzati da un'evoluzione esponenziale, l'elaborazione di standard adeguati richiede del tempo e che, anche qualora si addivenisse alla determinazione di adeguate norme tecniche queste ultime sarebbero destinate a divenire presto obsolete e, perciò, inadatte ad evitare i rischi connessi alla tecnologia in questione. Si tratta di un aspetto del così detto "*pacing problem*", ossia l'incapacità della regolazione di stare al passo con l'innovazione.⁵⁷ Chiarito tutto questo, va evidenziato come la dottrina abbia cercato ulteriori soluzioni, ravvisandole in particolare nel concetto di sicurezza *by design*, laddove si richiede al produttore che adotti delle misure di prevenzione dei rischi già a partire dalla stessa ideazione e fabbricazione del prodotto incorporando la prevenzione già al progetto. A ben vedere si tratta di un principio enunciato anche in materia di protezione dei dati personali e, in tale ambito, già divenuto cogente (art. 25 GDPR). Con rispetto alle macchine dotate di capacità cognitive il concetto di sicurezza *by design* implicherebbe il ricorso ad attività di *training e testing* tali da evitare certi rischi o che, in assenza di ciò, l'autonomia o l'auto-apprendimento fossero in tutto o in parte negato con lo scopo di mantenere il rischio al di sotto di una certa soglia che si consideri ragionevole. Per quanto concerne, invece, i dispositivi basati su un *software* comporterebbe la necessità di adottare misure idonee ad evitare il prodursi di danni derivanti da un cattivo funzionamento del *software* e da vulnerabilità del sistema che possa incidere sulla sua sicurezza. Lo stesso A. Amidei propone come strada percorribile quella di "attribuire rilevanza, ai fini della valutazione della difettosità del prodotto, alla mancata attivazione di blocchi di sicurezza idonei ad impedire allo *smart product* di porre in essere determinate condotte giudicate anche a priori potenzialmente lesive, in ottemperanza ad una sorta di "*do-no-harm rule*" algoritmica.⁵⁸

⁵⁷ R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft e hard law*, in *Persona e Mercato*, 2020/4, pp. 379-380.

⁵⁸ A. AMIDEI, *La responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in U. RUFFOLO, *XXVI Lezioni di diritto dell'intelligenza artificiale* (a cura di), 2020, p. 155.

1.5.2 L'onere della prova e le difficoltà del soggetto leso

Per concludere l'analisi resta da esaminare il tema dell'onere della prova avente ad oggetto lo *smart product* difettoso. Riacciandoci a quanto sopra esposto, R. Wagner mette in luce come l'avvento delle nuove tecnologie operi in un certo senso uno slittamento della capacità di controllo del dispositivo dall'utente al produttore. I prodotti tradizionali si affidano ad una struttura meccanica progettata e fabbricata dal produttore, la quale tuttavia necessita poi del contributo operativo dell'utente; è l'utente che esercita il controllo del prodotto nel mondo reale e che è in grado di determinare il comportamento della macchina. L'esempio più immediato è costituito dagli autoveicoli. Nel caso delle macchine convenzionali il controllo è operato dal conducente, il quale potrà determinare la direzione dei movimenti del veicolo e la sua velocità; qualora si verifici un incidente dovuto ad un cattivo utilizzo del mezzo, il produttore non sarà coinvolto in tale situazione, essendo egli incapace di influire sul comportamento del veicolo nel caso concreto. Al contrario, il veicolo autonomo non sarà controllato dal conducente, bensì da un algoritmo sviluppato e installato nel dispositivo dal suo autore.⁵⁹ Ecco allora che, segnatamente con riferimento ai sistemi *software* chiusi che non ammettono modifiche dell'algoritmo da parte di terzi (incluso l'utente), si ritiene che il produttore sia non solo il così detto "*cheapest cost avoider*", ma anche l'unico soggetto in grado di adottare tutte le precauzioni necessarie al fine di minimizzare il rischio. Si tenga conto anche del fatto che, specialmente quando si ha a che fare con prodotti caratterizzati da opacità e da un'elevata complessità tecnologica, si rivela particolarmente arduo per il danneggiato individuare la fonte del danno e assolvere all'onere probatorio che la Direttiva pone in capo all'utente; come già sottolineato, infatti, spesso la distinzione tra presunzione della causa del danno e presunzione della causa del difetto non è così semplice da tracciare e i due piani di indagine finiscono per sovrapporsi.⁶⁰ Questo comporterebbe la necessità, per il

⁵⁹ R. WAGNER, *Robot Liability*, 2018.

⁶⁰ C. BALDASSARRE, *Responsabilità del produttore: danno risarcibile, onere della prova e logica giuridica*, in *Danno e resp.*, 2014, p. 1444 ss.

danneggiato, di rivolgersi a un consulente tecnico esperto della materia, il che renderebbe gravosa, da un punto di vista economico, la possibilità di agire in giudizio e il più delle volte potrebbe scoraggiare azioni processuali anche meritorie. Il tema dell'asimmetria informativa tra produttore ed utente non è certo un tratto distintivo del solo campo delle tecnologie emergenti; si è già dato conto del fatto che, con riferimento ai prodotti tradizionali, la giurisprudenza di merito ha adottato un orientamento volto a privilegiare il principio di vicinanza della prova e dell'effettività della tutela, riconoscendo al danneggiato la possibilità di assolvere al proprio onere probatorio fornendo la prova del danno e dell'uso del prodotto in condizioni normali e ragionevoli, sollevandolo in tal modo dalla prova del difetto. In merito alla necessità di trovare una soluzione a tale problematica, una via d'uscita è offerta dalla *soft law*, che cerca di puntare sulle potenzialità stesse dei dispositivi intelligenti, la cui complessità tecnologica se, da un lato, rende più difficoltosa la prova del difetto, dall'altro offre soluzioni in grado di ridurre la situazione di asimmetria informativa tra danneggiati e produttori. Attraverso il così detto *logging by design*, difatti, sarebbe possibile dotare lo smart product di strumenti di registrazione di dati e di informazioni relative al proprio funzionamento, impiego, manutenzione, ecc. A ciò si dovrebbe accompagnare il dovere di comunicare simili dati al danneggiato in un formato leggibile; questa soluzione costituisce espressione del già ricordato principio della *sicurezza by design*.⁶¹ Divergente soluzione è, invece, proposta da R. Wagner che prospetta la possibilità di invertire l'onere della prova di cui all'art. 4 della Direttiva *Product Liability* e porre in capo al produttore l'onere di provare che il prodotto non fosse difettoso, sollevando il danneggiato dalla necessità di fornire la prova del difetto; ma, ancora, spingendosi più in là, prospetta la sostituzione di un sistema di responsabilità oggettiva relativa con un sistema di responsabilità oggettiva assoluta per i dispositivi intelligenti dotati di autonomia. In quest'ultimo caso, sul produttore graverebbe la responsabilità per qualsivoglia danno cagionato dalla macchina

⁶¹ R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft e hard law*, in *Persona e Mercato*, 2020/4, p. 385.

autonoma, a meno che tale danno non sia dovuto ad un agire colpevole del danneggiato o di un soggetto terzo o a cause di forza maggiore.⁶²

1.6 Il danno risarcibile

Anche il concetto di danno solleva qualche criticità se applicato ai nuovi prodotti intelligenti. L'art. 9 della Direttiva 85/374/CEE, trasposto nel Codice del consumo all'art. 123, ne offre una specifica definizione secondo la quale il risarcimento è limitato al “danno cagionato dalla morte o da lesioni personali” e alla “distruzione e deterioramento di cosa diversa dal prodotto difettoso” purché destinata all'uso e consumo privato. Un primo interrogativo sorto fin già dall'entrata in vigore della Direttiva riguarda la possibilità di considerare danno da “lesione” alla persona non solo il danno fisico, ma anche il danno patrimoniale. A questo proposito, alcuni autori escludono, sulla base di una interpretazione restrittiva fondata su argomenti di ordine logico e sistematico, taluni pregiudizi patrimoniali dal novero dei danni risarcibili, come ad esempio il lucro cessante e i danni a soggetti diversi dalle persone lese.⁶³ Diversamente, nel caso Boston Scientific la Corte di giustizia Ue, valorizzando gli obiettivi perseguiti dalla Direttiva, ha interpretato estensivamente il concetto di danno facendovi rientrare qualsiasi pregiudizio derivante da una lesione personale, poiché solo così si potrebbe garantire al danneggiato tutela integrale. Con particolare riferimento ai prodotti intelligenti il dubbio che sorge riguarda il danno cagionato ai dati e, più in generale, ai beni e contenuti digitali di proprietà dell'utente del prodotto; ci si chiede se sia necessario limitare il risarcimento ai danni causati a cose materiali o se sia possibile estenderlo anche ai danni cagionati a beni immateriali. Secondo R. Montinaro la risposta dipende dal significato attribuibile alle norme nazionali di trasposizione della Direttiva, le quali utilizzano talvolta il concetto di bene e talaltra il

⁶² R. WAGNER, *Robot Liability*, 2018.

⁶³ E. AL MUREDEN, *Autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense*, in *GIURISPRUDENZA ITALIANA*, 2019, p. 1706.

concetto di cosa.⁶⁴ R. Wagner, invece, commentando la Direttiva propone un'interpretazione estensiva del termine “*property item*”, includendovi qualsiasi cosa abbia un valore economico, a prescindere dalla sua tangibilità. E non vi è alcun dubbio, allora, che il danno cagionato ai dati sia risarcibile ai sensi della Direttiva 85/374/CEE, avendo gli stessi sicuramente un valore monetario nella moderna economia.⁶⁵ In ultima analisi rimane il tema della risarcibilità del danno derivante da lesione a diritti della personalità diversi dal diritto alla vita e alla integrità fisica; può darsi il caso, infatti, che vengano lese situazioni soggettive quali la protezione dei dati personali e della riservatezza. La tutela è affidata innanzitutto, in simili casi, al GDPR, il cui art. 82 stabilisce i presupposti al ricorrere dei quali sorge la responsabilità per illecito trattamento dei dati personali. Problemi di applicazione nel campo delle tecnologie digitali nascono laddove, ai sensi del già citato art. 82, sia necessario individuare il titolare del trattamento ai fini dell'attuazione di tale regime di responsabilità. Non solo: risulta complesso talvolta anche stabilire se i dati in questione rientrino nella categoria dei dati personali, costituendo solo questi ultimi l'oggetto della disciplina in questione. Ecco allora che, estendendo la portata del danno risarcibile sino a farvi rientrare la lesione dei diritti della personalità diversi dal diritto alla vita e alla integrità personale si potrebbe dar luogo ad una tutela integrale dell'individuo.⁶⁶

2. La nuova proposta di Direttiva della Commissione europea

2.1 La necessità di un adeguamento della disciplina

Il 22 settembre 2022 la Commissione europea ha presentato una proposta di Direttiva in materia di responsabilità per danni cagionati da prodotti difettosi volta a sostituire integralmente la Direttiva 85/374/CEE. Come già accennato, l'avvento delle nuove

⁶⁴ R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft e hard law*, in *Persona e Mercato*, n.4/2020, p. 386.

⁶⁵ R. WAGNER, *Robot Liability*, 2018.

⁶⁶ R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft e hard law*, in *Persona e Mercato*, n.4/2020, pp. 385-387.

tecnologie ha messo in dubbio la capacità della Direttiva *Product Liability* di disciplinare in modo soddisfacente le conseguenze normative in relazione a danni verificatisi in seguito al funzionamento difettoso di prodotti che, spesse volte, il legislatore del 1985 non avrebbe potuto nemmeno immaginare. I maggiori problemi si sono verificati con riguardo alla nozione di prodotto, al concetto di difetto così come parametrato al criterio delle aspettative dei consumatori e, di riflesso, all'oggetto dell'onere della prova gravante sul danneggiato, il quale, a causa di una situazione di asimmetria informativa che si acuisce nel caso dei prodotti intelligenti, rischia di fatto di sbarrare l'accesso alla giustizia al consumatore danneggiato. Anche l'esimente del rischio da sviluppo di cui all'art. 118 lettera e), se applicata alle nuove tecnologie minaccia di frustrare le istanze risarcitorie di questi ultimi: potrebbe, difatti, attenuare la funzione deterrente della responsabilità e disincentivare il produttore a investire nella ricerca, dal momento che proprio la scoperta di nuove conoscenze scientifiche e tecniche renderebbe non più operativa l'esimente. Infine, problematica appare in particolar modo la questione dell'istante temporale da prendere in considerazione ai fini dell'imputazione della responsabilità al produttore, vale a dire il momento dell'immissione in commercio del prodotto. Ciò comporta che il produttore si disinteressi, dopo questo momento, della sicurezza del prodotto e che manchino da parte sua investimenti in ricerca volti ad aumentare la sicurezza dei beni messi in commercio. Vediamo, allora, quali sono le più rilevanti novità della proposta di Direttiva.

2.2 L'allargamento della nozione di prodotto, i danni risarcibili e i legittimati passivi

Per quanto concerne la nozione di prodotto vi è la riconduzione all'interno di questa categoria sia dei *software* che dei *file per la fabbricazione digitale*; in particolare, i *software* si considerano prodotti a prescindere dal fatto che siano o meno integrati in un dispositivo dotato di materialità. Si esclude, invece, che possa essere qualificato come prodotto il codice sorgente del *software*, trattandosi unicamente di informazioni;

altresì si escludono tutti quei “*software liberi e open source sviluppati o forniti nel corso di una attività non commerciale*”. Si persevera poi nella volontà di escludere la risarcibilità dei danni occorsi al prodotto stesso, lasciando l’eventuale ristoro degli stessi alla disciplina della normativa nazionale; tale decisione appare in contrasto con l’obiettivo della direttiva di tutelare la sicurezza del consumatore. Si prevede poi la risarcibilità dei danni cagionati dai cc.dd. prodotti “*dual use*”: mentre l’attuale versione della direttiva richiede, al fine della risarcibilità dei danni, che il bene leso sia utilizzato dal danneggiato principalmente “*per proprio uso e consumo privato*”, la proposta escluda la risarcibilità solo qualora detto bene leso venga usato esclusivamente a fini professionali. La proposta di Direttiva prevede poi l’ampliamento della platea dei legittimati passivi, responsabilizzando l’importatore del prodotto difettoso e il rappresentante autorizzato del fabbricante nell’eventualità in cui quest’ultimo sia stabilito al di fuori dell’Unione europea; qualora anche questi soggetti risiedano in territorio extra UE ad essere tenuto responsabile sarà “*il fornitore di servizi di logistica*”; e, infine, nel caso in cui non sia stato possibile identificare alcuno dei soggetti sopra citati si prevede che il consumatore possa agire nei confronti del distributore ove egli, entro un mese da quando il danneggiato ne abbia fatto domanda, non fornisca tutte le informazioni necessarie all’identificazione dell’operatore economico o della persona che ha fornito il prodotto al distributore.

2.3 Il concetto di difetto

La proposta di direttiva puntualizza all’art. 6, con riferimento al concetto di difetto, che il parametro delle legittime aspettative di sicurezza dei consumatori non è il singolo individuo, bensì il grande pubblico dei consumatori considerato nel suo complesso. Ciò equivale a dire che, qualora nel caso concreto il singolo consumatore avesse effettivamente delle aspettative di sicurezza maggiori rispetto a quelle che dovrebbe avere il pubblico dei consumatori, tali aspettative sarebbero da considerarsi “illegittime”, poiché basate su un giudizio di difettosità avente natura soggettiva e non oggettiva, come dovrebbe invece essere. Viene poi ampliato l’elenco delle circostanze

non tassative da prendere in considerazione ai fini del giudizio sul difetto. Tra le altre spiccano per potenzialità di innovazione quella che invita a considerare “*gli effetti sul prodotto dell’eventuale capacità di continuare ad imparare dopo la sua diffusione*”, legata ai processi di *machine learning*; l’estensione dell’arco temporale rilevante ai fini della responsabilità fino al momento “*in cui il prodotto è uscito dal controllo del fabbricante*”; infine, il richiamo alla necessità di tenere presenti “*gli effetti sul prodotto di altri prodotti che ci si può ragionevolmente attendere siano utilizzati insieme al prodotto*”. Risulta tuttavia difficoltoso per il produttore prevedere tutte le possibili interazioni che il bene da lui commercializzato possa avere con altri prodotti digitali e, proprio per questo, grande rilevanza avrà il ruolo delle Corti nel delimitare i confini di ciò che il produttore debba ragionevolmente prefigurarsi.⁶⁷

3. Sistemi di Intelligenza artificiale: res o centri di imputazione giuridica?

3.1 La proposta di una nuova regolamentazione per i dispositivi intelligenti

Come già accennato in precedenza, vi è chi ritiene che il problema della imputazione della responsabilità per i danni cagionati dai sistemi di intelligenza artificiale necessiti di una nuova cornice normativa attraverso la quale il legislatore possa disciplinare i nuovi scenari creati dall’evoluzione tecnologica. In particolare, negli ultimi anni la dottrina si è interrogata sulla possibilità di attribuire ai sistemi di intelligenza artificiale la qualifica di soggetti di diritto e di dotarli di una di personalità giuridica creata *ad hoc* per questi ultimi e denominata, a ragion veduta, “personalità elettronica”. L’interesse degli autori per il tema è divenuto considerevole segnatamente dopo che il Parlamento europeo, con la Risoluzione del 16 febbraio 2017, ha avanzato la proposta di un riconoscimento della personalità elettronica per i robot, con lo specifico obiettivo

⁶⁷ L’intero contenuto dedicato alla nuova proposta di Direttiva è tratto da 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*, n.2/2023, pp. 656 e ss.

di far gravare sugli stessi una responsabilità diretta per i danni da essi cagionati, senza però specificare cosa debba intendersi con tale espressione.⁶⁸ Va tuttavia sottolineato come con Risoluzione del 20 ottobre 2020 lo stesso Parlamento europeo abbia poi fatto marcia indietro, precisando al punto 7 che “non è necessario conferire personalità giuridica ai sistemi di IA”. Nonostante l’inversione di rotta del legislatore europeo, però, si è continuato a discutere della possibilità di conferire alle macchine intelligenti uno status giuridico al fine di risolvere i problemi di *responsibility gap* di cui si è dato conto innanzi; in merito a tale possibilità la maggior parte della dottrina si pronuncia in termini negativi, sostenendo che non solo l’attribuzione dello status di soggetto e della capacità giuridica non risolverebbe la questione, ma che addirittura porterebbe ad una diminuzione della tutela per i danneggiati, la cui protezione risulta in realtà essere il fine ultimo della disciplina sulla responsabilità extracontrattuale. Non mancano, tuttavia, voci fuori dal coro. Nello specifico, V. Papakonstantinou e P. De Hert, nel rivolgere una critica alla Risoluzione del Parlamento europeo del 2020, affermano che il riconoscimento di una personalità elettronica aumenterebbe il livello di tutela dei consumatori consentendo a questi ultimi di individuare più facilmente il soggetto a cui rivolgere la pretesa di risarcimento per i danni cagionati; si ritorna, così, al complesso problema dell’onere della prova che, specialmente quando si tratti di dispositivi intelligenti, rischia di impedire al consumatore danneggiato di godere di quella protezione che il diritto dovrebbe garantirgli. Come già evidenziato, infatti, la complessità tecnologica e l’opacità che caratterizzano le macchine intelligenti rendono particolarmente gravoso il compito del danneggiato di individuare il soggetto, facente parte della catena di produzione del dispositivo, effettivamente responsabile per il comportamento anomalo della macchina; la creazione di una persona elettronica, al contrario, permetterebbe all’utente finale di individuare senza alcuna difficoltà il soggetto a cui rivolgere la sua pretesa di risarcimento. Gli autori, inoltre, identificano i due principali vantaggi che l’istituzione della personalità elettronica garantirebbe:

⁶⁸ L. DI DONNA, *La controversa soggettività giuridica dei robot*, in *Intelligenza artificiale e rimedi risarcitori*, 2022.

flessibilità e prossimità. La prima indicherebbe la capacità di questo nuovo soggetto di diritto di adattarsi ai vari settori dell'ordinamento risolvendo le eventuali questioni giuridiche che dovessero sorgere in quello specifico campo; la seconda, invece, farebbe riferimento, come già accennato, all'opportunità per il consumatore danneggiato di individuare agevolmente il soggetto responsabile in quanto il più prossimo al comportamento illecito.⁶⁹ Come già accennato, tuttavia, la dottrina maggioritaria guarda alla personalità elettronica con scetticismo e affronta la questione attraverso un interrogativo emblematico: l'intelligenza artificiale non può o, piuttosto, non dovrebbe essere considerata una persona giuridica? A questa domanda cercano di rispondere molti autori e, nel fare ciò, esaminano la problematica allargando il campo di indagine anche alla sfera dell'etica, oltre che a quella del diritto.

3.2 Comparazione tra persona naturale e IA: la retorica antropomorfica

Si è cercato, innanzitutto, di partire dalla constatazione che agli occhi del diritto gli esseri umani sono veri e propri soggetti capaci di divenire centri di imputazione di diritti e di doveri. Il primo passo, in questo senso, è stato quello di verificare se le caratteristiche possedute dalle cc.dd. persone naturali potessero essere ravvisate anche nei sistemi di IA, in modo tale da poter garantire loro pari dignità giuridica. Come riportato da Wagner, ad esempio, già nel 1992 Lawrence B. Solum identifica nell'intelligenza l'attributo che, in un primo momento, permetterebbe all'IA di essere qualificata come persona giuridica. Ma Solum non si ferma qua e aggiunge che, in secondo luogo, i sistemi di intelligenza artificiale potrebbero essere qualificati tali sulla base di ulteriori peculiarità che contraddistinguono la persona naturale da un punto di vista costituzionale: la coscienza, la capacità di provare emozioni, il possedere un'anima, l'aver degli interessi, il fissare da sé i propri obiettivi e, infine, il libero arbitrio. Si tratta, senza alcun dubbio, di qualità che caratterizzano l'essere umano e lo differenziano da qualsiasi altra creatura e dagli oggetti. Solum, però, aggiunge anche

⁶⁹ V. PAPAKONSTANTINOY, P. DE HERT, *Refusing to award legal personality to AI: why the European Parliament got it wrong*, in *European Law blog*, 2020.

che non tutte le suddette caratteristiche devono necessariamente essere riscontrate in un sistema di IA e, tuttavia, non indica quali possano mancare e quali siano invece indispensabili. Come poi notato da Wagner, spesso e volentieri non si tratta di possedere o non possedere, bensì di possedere, magari, in modo graduato tutte o alcune di queste qualità.⁷⁰ Si ricorre anche alle teorie filosofiche per cercare di spiegare in cosa consista il tratto distintivo dell'essere umano che lo qualifica come persona. Secondo la nota corrente degli utilitaristi, ciò che caratterizza la persona è la capacità di provare piacere e dolore; a questa affermazione Wagner ribatte osservando che se così fosse anche gli animali dovrebbero essere considerati tali e che, ad ogni modo, qualora vi fossero esseri umani non in grado di provare tali sensazioni, essi non dovrebbero essere considerati persone. Anche Kant cerca di riempire di contenuto il concetto di persona, ma lo fa avendo riguardo al modo di agire dell'essere umano, più che al risultato al quale tale agire conduce nel mondo reale; in questo senso, "persona" sarebbe colui che agisce secondo un principio morale, capace di rispettare le leggi morali e, di conseguenza, in grado di pensare in modo razionale e di "auto-governarsi". Kant rompe il paradigma della moralità associata all'obbedienza e, facendo ciò, crea un nuovo paradigma: quello della moralità associata all'autonomia. Quando, però, si parla di autonomia delle macchine intelligenti non ci si riferisce ad una siffatta condizione, bensì alla loro capacità di svolgere dei compiti senza la necessità della supervisione umana, piuttosto che alla loro capacità di apprendere continuamente dai dati che l'ambiente in cui operano gli fornisce per poter migliorare le proprie prestazioni.⁷¹ Questo esempio ben dimostra come vi sia una tendenza a proiettare sui dispositivi intelligenti peculiarità tipiche dell'essere umano, con l'obiettivo di giustificare la proposta di riconoscere a tali dispositivi lo *status* di persona. Anche qui Wagner evidenzia, tuttavia, come tale impostazione non sia aderente alla realtà, in quanto si danno casi di esseri umani non in grado di auto-determinarsi o di agire

⁷⁰ G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, pp. 594-595.

⁷¹ S. M. C. AVILA NEGRI, *Robot as Legal Person: Personhood in Robotics and Artificial Intelligence*, in *Frontiers in Robotics and AI*, 2021, p. 5.

moralmente in senso kantiano e, ciò nondimeno, si tratta di entità che il diritto considera a tutti gli effetti persone naturali.⁷² L'autore giunge così alla conclusione che il diritto non riconosca lo status di persona all'essere umano in virtù delle sue intrinseche caratteristiche, ma, più banalmente, in forza della sua appartenenza ad una specie.⁷³ E ciò spiegherebbe anche la ragione per cui gli animali, pur presentando molti tratti in comune con l'essere umano, non vengano considerati persone dal diritto, seppur gli venga accordata tutela a seguito del loro riconoscimento quali esseri senzienti. Va in ogni caso ricordato come la storia dimostri che non sempre il diritto ha accordato lo status di persona sulla base⁷⁴ dell'appartenenza ad una specie: basti pensare all'eclatante caso dello schiavo romano, che il diritto dell'epoca considerava a tutti gli effetti *res* di proprietà del suo *dominum*.

3.3 Comparazione tra persona giuridica e IA: il modello delle corporations

Appurato che ai sistemi di intelligenza artificiale non possa essere accordato dalla legge lo *status* di persone sulla base di un approccio filosofico ed etico che li accomuni alle persone naturali, resta ora da analizzare il caso emblematico delle società, enti ad associazioni a cui il diritto riconosce personalità giuridica, al fine di comprendere se vi siano ragioni che possano condurre allo stesso esito per le macchine intelligenti. Le ragioni che hanno portato a qualificare le *corporations* come persone giuridiche, innanzitutto, sono di ordine economico: la società funge da scudo per l'investitore, il quale può permettersi di intraprendere ambiziosi progetti economici, certo del fatto che solo il cc.dd. patrimonio di rischio verrà coinvolto nell'adempimento dei debiti sorti in occasione dell'esercizio dell'impresa. Per questo motivo, attraverso una *fictionis iuris* il diritto decide di attribuire personalità giuridica a tali enti. Si dice, a questo

⁷² G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, pp. 595-598.

⁷³ G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, p. 598.

⁷⁴ G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, p. 598.

proposito, che la scelta operata dall'ordinamento abbia natura pragmatica, piuttosto che filosofica, non essendo in assoluto correlata alla nozione etica di moralità.⁷⁵ Tornando, quindi, all'interrogativo posto in precedenza, va da sé che la questione più importante non riguardi tanto il se l'ordinamento possa riconoscere personalità ai sistemi di intelligenza artificiale, quanto, piuttosto, l'opportunità di tale decisione. Vale la pena evidenziare come sussista una importante differenza fra le *corporations* e i sistemi di IA, differenza che consiste nella presenza di un substrato umano attraverso il quale le prime sono abilitate ad operare nel mondo delle relazioni giuridiche ed economiche; le seconde, al contrario, sono una creazione dell'uomo, ma non è presente nel processo di decisione e di comunicazione della stessa alcun essere umano.⁷⁶

3.4 La personalità elettronica come approdo finale del processo di oggettivizzazione delle fonti dell'obbligazione

U. Ruffolo sottolinea come “*la personalità elettronica sembrerebbe l'approdo ultimo di quel processo di parallelo oggettivarsi delle due grandi fonti dell'obbligazione, volontà nel contratto e colpa nell'illecito*”. Secondo l'autore, già da tempo sarebbe in corso una progressiva oggettivizzazione, da una parte, del contratto, laddove si privilegia il tenore oggettivo della dichiarazione piuttosto che la volontà soggettiva del dichiarante; dall'altro, dell'illecito, laddove viene meno il primato della colpa nell'ambito della responsabilità extracontrattuale. Con il riconoscimento della personalità elettronica si percorrerebbe l'ultima tappa di questo percorso di oggettivizzazione, poiché sarebbe lo stesso soggetto giuridico a non essere umano. Si potrebbe replicare che anche le società sono soggetti giuridici non umani, ma, come già evidenziato, queste ultime sono costituite da organi composti da esseri umani e ciò comporta che vi sia uno scollamento tra il soggetto decidente e il soggetto dichiarante; nel caso della persona elettronica, invece, la macchina intelligente sarebbe sia l'uno

⁷⁵ S. M. C. AVILA NEGRI, *Robot as Legal Person: Personhood in Robotics and Artificial Intelligence*, in *Frontiers in Robotics and AI*, 2021, p. 6.

⁷⁶ S.M. SOLAIMAN, *Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy*, in *Artificial Intelligence and Law*, 2017 p. 174.

che l'altro. E, partendo da questo presupposto, vi sono teorizzazioni, come quella di Teubner a proposito dei sistemi multiagente,⁷⁷ che si spingono addirittura sino alla spersonalizzazione della stessa macchina: nasce così il paradosso in forza del quale ad essere entificata diviene la decisione comunicata dal soggetto artificiale. Tale paradosso, a parere di U. Ruffolo, è generato dall'equivoco secondo il quale l'obiettivo primario della personificazione dei dispositivi intelligenti è quello di responsabilizzarli direttamente nei confronti dei soggetti lesi, esigenza che l'autore ritiene non essenziale; mentre la necessità di riconoscere loro personalità giuridica al fine di assicurargli diritti e tutele viene del tutto trascurata.⁷⁸ Vi è, infatti, un secondo ordine di ragioni che dovrebbe condurre al riconoscimento della personalità elettronica e che ha a che vedere con la possibilità che i sistemi intelligenti divengano titolari o "autori" di ciò che sono in grado di creare. Ad oggi, invero, solo le persone fisiche possono essere titolari di diritti morali d'autore, tanto che due domande di registrazione di brevetto nelle quali si indicava come inventore un dispositivo intelligente sono state rigettate recentemente dallo *European Patent Office*.⁷⁹ Alla luce di quanto sinora esposto, pare allora che se di una personalità elettronica si possa in qualche misura discutere, ciò debba essere fatto avendo riguardo in primo luogo alla necessità di riconoscere alle macchine intelligenti la titolarità delle opere da esse create, essendo, per contro, la responsabilizzazione diretta delle stesse per i danni cagionati non solo esigenza non essenziale, ma anche strumento inidoneo a perseguire i principali obiettivi della responsabilità extracontrattuale.

3.5 L'esternalizzazione del rischio e le possibili soluzioni

Un'ultima ma non meno importante critica mossa dalla dottrina riguarda, invece, l'aspetto relativo all'incongruenza sussistente tra gli obiettivi perseguiti dalla

⁷⁷ G. TEUBNER, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, 2019.

⁷⁸ U. RUFFOLO, *La personalità elettronica tra "doveri" e "diritti" della macchina*, in *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (a cura di), 2020, pp. 121-122.

⁷⁹ U. RUFFOLO, *Il problema della "personalità elettronica"*, in *Journal of Ethics and Legal Technologies*, 2020, p. 80.

disciplina della responsabilità extracontrattuale e i risultati che si otterrebbero attraverso il riconoscimento della personalità elettronica. Se da un lato, infatti, si mira ad assicurare al soggetto leso il ristoro dei danni subiti, va d'altra parte notato come il dispositivo intelligente non disponga di alcuna somma di denaro con cui poter adempiere a tale obbligo di risarcimento. Si potrebbe, dunque, pensare di dotare il robot di un capitale destinato proprio a riparare i danni cagionati; tale soluzione ricalca inevitabilmente quella adottata dal modello societario, laddove dei danni cagionati dalla società risponde la stessa con il proprio patrimonio, detto perciò "patrimonio di rischio", mentre il patrimonio personale dei soci viene messo al riparo da qualsivoglia pretesa. Come già ricordato, la società funge in questo caso da scudo per i soci, i quali traslano su di essa il rischio di impresa.⁸⁰ Va peraltro rammentato che lo stesso sistema potrebbe essere adottato anche in mancanza di personalità giuridica, come dimostra la storia antica: gli schiavi romani potevano essere dotati di un *peculium* destinato all'esercizio di una attività imprenditoriale e tale somma di denaro costituiva il "capitale di rischio" entro il quale si limitava la responsabilità del *servus*, pur non essendo quest'ultimo considerato persona agli occhi del diritto.⁸¹ Ad ogni modo va da sé che, nel caso dello schiavo, a dotare costui del *peculium* fosse il suo *dominus*, mentre a conferire il capitale sociale provvedono gli stessi soci della società; se si adottasse tale soluzione anche per i moderni schiavi artificiali, allora, dovrebbero essere i produttori a dotare il dispositivo di un proprio patrimonio. La conseguenza di tale soluzione sarebbe, invero, la creazione di un tetto massimo oltre il quale il risarcimento non potrebbe essere riconosciuto, costituito da detto "patrimonio di rischio".⁸² Il secondo grande obiettivo perseguito dalla disciplina sulla responsabilità civile extracontrattuale è la deterrenza, la quale rappresenta una logica conseguenza della previsione dell'obbligazione risarcitoria; il responsabile richiesto di ristorare i danni

⁸⁰ G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, p. 609.

⁸¹ U. RUFFOLO, *La personalità elettronica tra "doveri" e "diritti" della macchina*, in *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (a cura di), 2020, p. 116.

⁸² G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, p. 612.

cagionati viene dissuaso dal porre in essere nuovamente la condotta lesiva. Tuttavia, nessun incentivo a produrre dispositivi più sicuri verrebbe avvertito dai produttori dal momento che a risarcire i danni non sarebbero questi ultimi; dal canto suo, il robot potrebbe certo essere programmato per correggere di volta in volta la propria azione, ma si tratterebbe pur sempre di un intervento effettuato dal creatore dell'algoritmo e non di una scelta del robot dovuta alla forza deterrente della disciplina. Si parla, in questi casi, di esternalizzazione del rischio, poiché il rischio del verificarsi del danno e la relativa sopportazione dei costi non grava più sul produttore, bensì sulla stessa vittima del danno. Ciò comporta che troppi dispositivi vengano prodotti e immessi sul mercato e che quelli già esistenti vengano eccessivamente utilizzati, senza tener conto del fatto che il costo sociale che deriva dal loro utilizzo potrebbe superare l'effettivo valore da questi generato.⁸³ Le soluzioni proposte per fronteggiare la situazione appena descritta consistono, in primo luogo, nel dotare come già visto il dispositivo intelligente di un proprio patrimonio con il quale far fronte alle richieste di risarcimento; in alternativa, nella previsione di una assicurazione obbligatoria di responsabilità civile quale preconditione per il riconoscimento della personalità elettronica della macchina. Si noti come entrambe le soluzioni prospettate presuppongano che vi siano a monte persone fisiche o giuridiche tenute a pagare di tasca propria o per dotare il dispositivo di un capitale di rischio o per adempiere all'obbligazione pecuniaria legata al pagamento del premio assicurativo. È possibile pertanto concludere che, in fin dei conti, a sopportare il rischio del verificarsi del danno continuano ad essere il produttore o l'utilizzatore del dispositivo; con la conseguenza, tuttavia, che il risarcimento sarà assicurato, in questi casi, per un valore non superiore al tetto rappresentato dal capitale o dell'assicurazione obbligatoria. Oltre questo ammontare, il problema dell'esternalizzazione del rischio continua a sussistere. Vero è che tale situazione si presenta anche nel caso delle società; ciò che cambia in tale contesto è che la società ha a che fare con creditori volontari, i quali possono

⁸³ G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, p. 609.

facilmente proteggersi dal rischio di esternalizzazione. Nel caso, invece, dei soggetti danneggiati dai robots, si tratta di creditori involontari sprovvisti di mezzi idonei a fare fronte a simile circostanza.⁸⁴ Ecco allora che, dotare la macchina di personalità elettronica con l'obiettivo di renderla direttamente responsabile dei danni cagionati al fine di incrementare la tutela dei soggetti lesi condurrebbe, paradossalmente, al risultato opposto: una diminuzione della protezione delle vittime, esposte maggiormente al rischio del verificarsi del danno e alla probabilità di non conseguire un risarcimento adeguato. Come rimarcato da U. Ruffolo “la macchina, se e quando personificata, potrà essere presa in considerazione come soggetto cui imputare dirette responsabilità; ma non viceversa”.⁸⁵

⁸⁴ G. WAGNER, *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, p. 610.

⁸⁵ U. RUFFOLO, *Il problema della “personalità elettronica”*, in *Journal of Ethics and Legal Technologies*, 2020, p. 85.

III. Artificial Intelligence Act: l'approccio europeo alla regolazione dell'Intelligenza artificiale

1. Le sfide dell'UE nell'era digitale: un nuovo modello regolatorio. 2. AI Act: la struttura e il modello risk-based. 3. AI Act: il principio di accountability e il confronto con il GDPR. 4. La proposta di direttiva sulla responsabilità dell'IA nel solco della strategia digitale dell'Unione europea.

1. Le sfide dell'UE nell'era digitale: un nuovo modello regolatorio

1.1 L'Agenda Digitale europea: verso il mercato unico digitale

Come illustrato nel capitolo precedente, l'alternativa a cui le Istituzioni dell'Unione europea si trovano di fronte è rappresentata per un verso dalla scelta di adattare il diritto vivente alle nuove sfide che l'evoluzione tecnologica presenta, per altro verso dalla possibilità di comporre un nuovo *framework* normativo in grado di meglio disciplinare il fenomeno in questione. Osserva A. Amidei che l'ordinamento unionale ha già conosciuto la necessità di regolamentare settori che, pur non coincidendo esattamente con quello dell'*artificial intelligence*, si trovano oggi interessati da queste nuove forme di "robotica intelligente", condividendone, sotto certi aspetti, oggetto o caratteristiche. Si pensi, ad esempio, alla Direttiva 89/392/CEE (così detta "prima Direttiva Macchine"), abrogata dalla successiva Direttiva 98/37/CEE, le cui prescrizioni normative sono poi state in parte rielaborate attraverso la Direttiva 2006/42/CEE (così detta "nuova Direttiva Macchine"). Ciò che questi e altri interventi normativi (quali, per citarne uno, la Direttiva 2001/95/CE "*relativa alla sicurezza generale dei prodotti*") cercano di realizzare è la creazione di un *corpus* di norme in grado di rendere uniformi in tutti gli Stati Membri i requisiti e le caratteristiche necessarie a garantire la sicurezza dei macchinari sia per quanto riguarda la fase della progettazione, sia per quanto riguarda la produzione. Tali interventi non si concentrano sulla regolamentazione delle conseguenze di eventuali danni cagionati da un malfunzionamento della macchina o da un difetto di produzione, ma pongono il *focus* principale "a monte", delineando una serie di standard, requisiti e garanzie che gli

operatori sono richiesti di fornire e rispettare al fine di poter immettere il prodotto sul mercato. Si tratta, allora, di una regolamentazione di settore che introduce sistemi di controllo di natura per lo più “amministrativa”.⁸⁶ Tale premessa si rende necessaria qualora, come in questa sede, si voglia esaminare in maniera compiuta e approfondita la più importante legge euro unitaria sull’intelligenza artificiale: si tratta del Regolamento sull’intelligenza artificiale, denominato *Artificial Intelligence Act*.⁸⁷ La Commissione sceglie per la prima volta un modello orizzontale di regolamentazione, distaccandosi perciò dall’approccio settoriale sino a questo momento utilizzato per disciplinare gli ambiti interessati dalle varie applicazioni di IA; questa scelta, come vedremo, avrà delle ricadute in particolare sulla definizione di intelligenza artificiale adottata dalla Commissione, la quale sconta una necessaria genericità. Tornando, però, all’*iter* temporale che ha portato alla presentazione della proposta, va anzitutto ricordato che la medesima si inserisce in un quadro normativo strategico, articolato in una serie di interventi legislativi che toccano fundamentalmente quattro ambiti: quello della protezione dei dati personali, disciplinato attraverso il regolamento 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 “relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati”, noto come “GDPR”⁸⁸ ; quello relativo ai servizi digitali e al mercato digitale, disciplinato rispettivamente dal *Digital Services Act* e dal *Digital Markets Act*; quello concernente l’identità digitale, interessato dalla revisione del

⁸⁶ A. AMIDEI, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in U. RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, 2017, pp. 69-77.

⁸⁷ L’*iter* che porterà all’approvazione del testo definitivo del regolamento da parte del Parlamento europeo ad aprile 2024 è iniziato in data 21 aprile 2021 con la proposta di regolamento della Commissione europea. Allo stato attuale, l’ultimo passo sembra essere stata l’approvazione del testo da parte del Consiglio europeo in data 2 febbraio 2024.

⁸⁸ Il settore della protezione dei dati è stato interessato anche dal *Data Act* e dal *Data Governance Act*. Nel primo caso si tratta del Regolamento 2023/2854 del Parlamento europeo e del Consiglio riguardante norme armonizzate sull’accesso equo ai dati e sul loro utilizzo; nel secondo caso si tratta del Regolamento 2022/868 del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati, il quale modifica il Regolamento 2018/1724.

Regolamento E-IDAS del 2014⁸⁹ e, per concludere, quello che riguarda l'intelligenza artificiale, interessato oggi proprio dall'*Artificial Intelligence Act*. Senza entrare ora nel merito di ciascuno dei provvedimenti sopra menzionati e riservando alla trattazione successiva la comparazione tra il così detto *AI Act* e alcune caratteristiche dei suddetti interventi legislativi, è necessario qui sottolineare come lo scopo ultimo del legislatore europeo sia la costruzione di un mercato unico digitale europeo⁹⁰. Pur essendo questo il più evidente degli obiettivi perseguiti attraverso il disegno strategico appena delineato, si osservi come la stessa Commissione, nella Relazione che accompagna la proposta di Regolamento, definisce altre tre importanti finalità che si aggiungono a quella di “facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato”: nello specifico si parla di “assicurare che i sistemi di IA immessi sul mercato dell’Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e valori dell’Unione”; “assicurare la certezza del diritto per facilitare gli investimenti e l’innovazione nell’intelligenza artificiale” e, infine, “migliorare la governance e l’applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA”. Si tratta di obiettivi che definiscono quello che è l’approccio europeo e che lo contraddistinguono nel panorama internazionale segnandone il distacco, in particolare da Cina e Stati Uniti.

1.2 Il contesto geopolitico: la competizione con Cina e Stati Uniti

Se gli obiettivi indicati sino a questo punto definiscono un approccio tutto europeo alla regolamentazione dell’intelligenza artificiale, va chiarito come vi sia, cionondimeno, un ulteriore obiettivo perseguito dalle Istituzioni che potremmo qualificare quale obiettivo di natura geopolitica. Si legge nella Relazione che accompagna la proposta

⁸⁹ Si tratta della proposta di Regolamento del Parlamento europeo e del Consiglio che riguarda l’istituzione di un quadro normativo per una identità digitale europea, proposta che a sua volta modifica il Regolamento 910/2014.

⁹⁰ 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*, n.2/2022, pp. 309-310.

della Commissione europea che “l’interesse dell’Unione è quello di preservare la *leadership* tecnologica dell’UE”; è una affermazione che la stessa Relazione tenta di chiarire successivamente, aggiungendo che lo scopo è quello di “tutelare la sovranità digitale dell’Unione e sfruttare gli strumenti e i poteri di regolamentazione di quest’ultima per plasmare regole e norme di portata globale”⁹¹. La specifica si rende necessaria dal momento che lo scenario tecnologico e di mercato nel quale la Proposta si inserisce vede Stati Uniti e Cina come leader indiscussi nella produzione di applicazioni di intelligenza artificiale. Proprio da qui è imprescindibile partire per comprendere i diversi approcci alla regolazione dell’intelligenza artificiale che caratterizzano queste potenze, mettendo in luce sostanziali differenze per quanto riguarda le finalità della legislazione, la mentalità con cui ci si accosta alla materia e gli strumenti individuati per meglio conseguire gli obiettivi prefigurati. Come enfatizzato da E. Chiti e B. Marchetti l’avvento dell’intelligenza artificiale viene tematizzato dall’Unione europea come un processo che presenta tutte le caratteristiche tipiche della “crisi” (per quanto il termine esatto non sia mai davvero utilizzato): un evento straordinario, dal momento che comporta una trasformazione rapida e profonda, i cui effetti non sono prevedibili. Da questa rappresentazione discendono gli obiettivi perseguiti dal legislatore unionale, che si possono brevemente riassumere in due punti fondamentali: per un verso l’esigenza di “regolazione e protezione sociale” e di “regolazione etica” che mettono al centro, ad esempio, la tutela del consumatore, la protezione dei dati personali, la tutela dei lavoratori impiegati nelle occupazioni che subiranno le trasformazioni più incisive e, infine, la necessità che l’intervento normativo volto a regolamentare l’IA abbia anche finalità etiche, posto che una delle conseguenze della crisi è proprio la nascita di questioni di natura etica; per altro verso, il desiderio di contribuire, attraverso una apposita normativa, allo sviluppo e all’innovazione dell’intelligenza artificiale, obiettivo che, peraltro, produce un piccolo paradosso rappresentato dal fatto che nonostante l’Unione europea veda l’avvento

⁹¹ G. FINOCCHIARO, *La regolazione dell’intelligenza artificiale*, in *Rivista trimestrale di diritto pubblico*, n.4/2022, p. 1089.

dell'IA come un fattore di crisi da governare, decida poi di sostenerne lo sviluppo.⁹² Cina e Stati Uniti, invero, conferiscono importanza preponderante all'obiettivo di ottenere (nel caso della Cina) o mantenere (nel caso degli Stati Uniti) una *leadership* globale nello sviluppo e nell'impiego delle applicazioni di IA, esigenza avvertita come necessaria al fine di affermare la propria supremazia in campo economico e militare.⁹³ Chiarito questo, va da sé che gli strumenti utilizzati per dare concretezza alle aspirazioni di ciascun attore non possano che essere diversi. Tenuto conto, allora, delle specifiche finalità perseguite da USA e Cina, è possibile ravvisare da parte di questi ultimi un approccio fortemente *innovation-friendly* rispetto alla materia.

1.2.1 Le peculiarità del modello statunitense e del modello cinese

Nel caso degli Stati Uniti tale approccio si traduce in una legislazione per nulla orientata al principio di precauzione, posto che una simile ispirazione comporterebbe uno svantaggio competitivo rispetto a paesi che non seguano una filosofia precauzionale. Il risvolto negativo di tale attitudine si rinviene nello scarso interesse per le possibili minacce ai diritti fondamentali dei cittadini derivanti dall'impiego dell'intelligenza artificiale. Si noti che è in particolare l'azione di governo a propendere per un forte sviluppo dei sistemi di intelligenza artificiale, riconoscendo molta più rilevanza ai vantaggi degli stessi, che ai rischi che ne derivano. Con l'*Executive Order* 13859 dell'11 febbraio 2019 l'amministrazione Trump annuncia una strategia nazionale che per nulla si discosta da quella intrapresa del predecessore Obama ed oggi dall'amministrazione Biden: la preoccupazione principale è costituita dalla *leadership* statunitense nell'intelligenza artificiale, la quale può essere raggiunta solo attraverso il suo sfruttamento economico, politico e militare. Più attenti alla salvaguardia delle libertà individuali si presentano Congresso e legislatori statali, i quali si adoperano per trovare un bilanciamento fra necessità di sviluppo ed esigenza

⁹² E. CHITI, B. MARCHETTI, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della Regolazione dei mercati*, n.1/2020, pp. 31-34.

⁹³ G. RESTA, *Cosa c'è di "europeo" nella proposta di Regolamento UE sull'intelligenza artificiale?*, in *Il diritto dell'informazione e dell'informatica*, n.2/2022, p. 326.

di controllo dei possibili rischi che l'applicazione dell'IA comporta; si tratta pur sempre, tuttavia, di un timido tentativo che si colloca nel solco di una attività di tipo non precauzionale.⁹⁴ Accanto alla regolazione pubblica del Congresso e del potere esecutivo si collocano, poi, le iniziative di *self-regulation* frutto della *partnership* pubblico-privato, che hanno visto coinvolte anche le *big tech* statunitensi quali Amazon, Google, Microsoft ed Apple. Si dubita, tuttavia, della capacità di questa *partnership* e di questo modello di garantire una regolazione effettiva, dal momento che sembrano essersi già verificati vari episodi in cui alla violazione dei principi non è seguita alcuna concreta conseguenza.⁹⁵ Pare si possa dire allora, in virtù di quanto appena esposto, che la strategia adottata dagli Stati Uniti si caratterizza per un approccio *hands off*, per lo meno sul piano domestico: si vuole evitare un *regulatory over-reach* che finirebbe per rallentare eccessivamente la corsa alla primazia in campo tecnologico. Dal canto suo la Repubblica Popolare Cinese, pur allineandosi agli Stati Uniti nella scelta di disciplinare l'intero processo produttivo capitalista, adotta un approccio proattivo sia nella politica industriale che nella regolamentazione, volto a ottenere strumenti che siano in grado di operare un controllo effettivo sulle imprese.⁹⁶ Coerentemente con il proprio indirizzo di governo, la normativa cinese propone un costante richiamo al tema della sicurezza nazionale, dell'ordine pubblico e del controllo delle attività poste in essere dai fornitori e dai gestori di sistemi di intelligenza artificiale.⁹⁷ Il modello di *governance* cinese si distingue dagli altri in analisi, in particolare, per l'accento posto sull'impatto sociale dei sistemi intelligenti; il legislatore sente la necessità di tutelare, attraverso la regolamentazione dell'IA, le categorie sociali più toccate dal fenomeno in questione, mentre meno attenzione è posta sulle ricadute che tale fenomeno può avere sul singolo consociato, o sulle

⁹⁴ E. CHITI, B. MARCHETTI, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della Regolazione dei mercati*, n.1/2020, pp. 34-36.

⁹⁵ E. CHITI, B. MARCHETTI, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della Regolazione dei mercati*, n.1/2020, pp. 40-43.

⁹⁶ G. RESTA, *Cosa c'è di "europeo" nella proposta di Regolamento UE sull'intelligenza artificiale?*, in *Il diritto dell'informazione e dell'informatica*, n.2/2022, p. 326.

⁹⁷ G. CAPUZZO, *Minority Report. Uno studio su intelligenza artificiale e comparazione giuridica tra UE, USA e Cina*, p. 515.

esigenze di produzione di beni e servizi (peculiarità che caratterizzano, rispettivamente, il modello europeo e il modello statunitense).⁹⁸

1.2.2 Il modello europeo e l'effetto Bruxelles

È proprio dalla necessità di garantire tutela ai diritti fondamentali di ciascun individuo che si deve partire, invero, per comprendere l'approccio e l'impostazione del Regolamento della Commissione europea. Formule quali “*human-centric*” o “*trustworthy-AI*”, che ricorrono nel testo, riflettono l'idea che le applicazioni di intelligenza artificiale possano incidere negativamente sul sistema di protezione dei diritti fondamentali, necessitando, pertanto, di un vero e proprio modello di *hard law*, piuttosto che di un sistema guidato dalla *self-regulation*. La linea giuspolitica di fondo che riflette l'agire dell'Unione europea può riassumersi nella massima secondo la quale devono essere i diritti fondamentali a guidare lo sviluppo del mercato e non viceversa.⁹⁹ Questa dimensione, senz'altro coerente con il sistema valoriale interno, va poi bilanciata con l'esigenza di promuovere lo sviluppo dell'intelligenza artificiale; l'ambizioso equilibrio a cui mira la normativa europea si traduce in un approccio aperto alle innovazioni giuridiche, avvertite come necessarie per garantire certezza del diritto, ma anche promozione del progresso scientifico e tecnologico. Tutto questo si traduce, dal punto di vista della produzione normativa, in una proposta di Regolamento che adotta un approccio c.d. *risk-based*, mettendo al centro i possibili rischi di violazione dei diritti fondamentali dell'individuo e tentando di attuare una politica di gestione del rischio. È in quest'ottica che può leggersi il ricorso al principio di precauzione, già da tempo inserito tra i principi fondamentali in materia di politica ambientale europea e del quale oggi si accetta una interpretazione estensiva volta ad ampliarne l'operatività a settori quali la sicurezza sul lavoro o la tutela dei

⁹⁸ G. CAPUZZO, *Minority Report. Uno studio su intelligenza artificiale e comparazione giuridica tra UE, USA e Cina*, p. 491.

⁹⁹ H. ROBERTS, *Achieving a “Good AI Society: Comparing the Aims and Progress of the EU and US*, p. 67.

consumatori.¹⁰⁰ L'analisi sin qui condotta dell'assetto geopolitico in cui si colloca la corsa mondiale all'IA e le distinzioni che intercorrono tra i vari modelli di regolamentazione esige un ultimo, ma imprescindibile riferimento, fondamentale ai fini della comprensione dell'approccio europeo: ci si riferisce alla tecnica normativa della “*territorial extension*”, differenziata da Joanne Scott dal più generale paradigma della extraterritorialità.¹⁰¹ Si tratta di una strategia posta in essere dalle Istituzioni dell'Unione europea in una pluralità di discipline che punta ad estendere in modo particolarmente ampio e flessibile l'ambito territoriale di applicazione delle norme. L'*Artificial Intelligence Act* contiene, per l'appunto, una clausola di applicazione territoriale ampia a tal punto da dispiegare forme di *territorial extension* della normativa interna, clausola peraltro analogamente contenuta all'interno del GDPR, del *Digital Services Act* e del *Digital Markets Act*. In particolare, l'art. 2, 1 co., lettera c) dispone che i doveri di condotta stabiliti dalla proposta e le relative sanzioni si applichino non solo ai fornitori di un dispositivo intelligente direttamente immesso nel mercato UE, ma anche a fornitori e utilizzatori situati in un paese terzo “allorché l'*output* prodotto dal sistema sia utilizzato nell'Unione”.¹⁰² Il legislatore europeo argomenta, nel considerando n. 11, che tale soluzione ovvia al problema dell'elusione del Regolamento e garantisce una protezione efficace delle persone fisiche che si trovano nell'Unione. Come evidenziato da G. Resta non vi è dubbio che un problema di elusione e di de-localizzazione si presenti allorquando si debba regolare la tecnologia, tanto più nel caso di tecnologie digitali quali l'IA che si contraddistinguono per il loro carattere incorporale e, dunque, “strutturalmente a-territoriale”.¹⁰³ L'autore, tuttavia, si chiede anche se la Proposta, così strutturata, non dia vita ad una forma di *underregulation* per l'ipotesi specifica in cui il dispositivo intelligente venga sì

¹⁰⁰ E. CIBELLA, *Il principio di precauzione nell'ambiente digitale*, in *P.A. Persona e Amministrazione*, n.1/2023, pp. 521-523.

¹⁰¹ J. SCOTT, *The Global Reach of EU Law*, in M. CREMONA – J. SCOTT (a cura di) *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, 2019, p. 21.

¹⁰² G. RESTA, *Cosa c'è di “europeo” nella proposta di Regolamento UE sull'intelligenza artificiale?*, in *Il diritto dell'informazione e dell'informatica*, n.2/2022, p. 331.

¹⁰³ G. RESTA, *Cosa c'è di “europeo” nella proposta di Regolamento UE sull'intelligenza artificiale?*, in *Il diritto dell'informazione e dell'informatica*, n.2/2022, p. 332.

prodotto all'interno dell'UE, ma sia poi destinato ad essere commercializzato od utilizzato in un paese terzo. Una clausola così predisposta impone di estendere gli obblighi, ma non le tutele verso l'esterno, dando vita ad una soluzione poco coerente con il carattere universalistico delle situazioni giuridiche in oggetto. Non a caso, sotto questo specifico profilo la scelta effettuata dal Regolamento 2016/679 è stata diversa: il legislatore, in coerenza con la finalità di protezione dei diritti e della dignità umana, ha stabilito che fossero assoggettate ai requisiti previsti dalla normativa tutte le ipotesi di trattamento dei dati personali effettuate da parte di titolari stabiliti nell'Unione, a prescindere dal fatto che i dati si riferissero a cittadini UE o domiciliati all'interno dei confini dell'Unione.¹⁰⁴ Osserva poi G. Resta che, per altro verso, potremmo trovarci di fronte ad una ipotesi di una *regulatory overreach* o, come pare più probabile stante le verosimili difficoltà di applicazione, ad una disposizione “meramente declamatoria”, avendo la stessa un raggio di azione talmente allargato da risultare inapplicabile e, quindi, puramente simbolica.

Per comprendere fino in fondo il significato della clausola di “*territorial extension*” è però necessario percorrere qualche passo a ritroso e tornare al ruolo che gioca l'Unione europea nel panorama internazionale. Come accennato in precedenza, non vi è dubbio che non vi sia al momento alcuna possibilità per l'UE di competere con superpotenze quali Stati Uniti e Cina dal punto di vista dello sviluppo e della produzione di applicazioni di intelligenza artificiale; cionondimeno, il modello regolatorio europeo assurge a vero e proprio *gold standard* globale per quanto riguarda la protezione dei diritti fondamentali nel contesto di utilizzo delle applicazioni di IA. Particolarmente efficace risulta l'immagine di una Unione europea fondata sul diritto e non sul potere, laddove tuttavia il diritto può rappresentare, nelle relazioni internazionali, una fonte di potere.¹⁰⁵ Con l'espressione “Effetto Bruxelles” ci si riferisce, secondo A. Bradford, alla “capacità unilaterale dell'Unione di regolare i mercati globali stabilendo gli

¹⁰⁴ G. RESTA, *Cosa c'è di “europeo” nella proposta di Regolamento UE sull'intelligenza artificiale?*, in *Il diritto dell'informazione e dell'informatica*, n.2/2022, p. 333.

¹⁰⁵ Questa riflessione si trova in M. CREMONA - J. SCOT, *Introduction. EU Law Beyond EU Borders*, in M. CREMONA – J. SCOTT (a cura di) *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, p. 21.

standard nella politica della concorrenza, la protezione ambientale, la sicurezza alimentare, la protezione della privacy, o la regolamentazione dei discorsi di odio nei social media”.¹⁰⁶ Bradford parte dal presupposto che l’UE non abbia bisogno di imporre coercitivamente a nessuno i suoi standard, essendo sufficienti le sole forze di mercato: sono infatti poche le aziende globali che possono permettersi di non intraprendere relazioni commerciali con questo paese. Il mercato di consumo europeo è talmente ampio ed omogeneo da poter essere considerato una destinazione commerciale inevitabile; ciò solo, tuttavia, non è di per sé sufficiente a far emergere il c.d. Effetto Bruxelles. Quello che rende l’UE una superpotenza in grado di esportare i propri modelli normativi è la presenza di istituzioni dotate di vera e propria capacità regolamentare e una volontà politica di utilizzare questa capacità al fine di produrre regole rigorose: solo così il potere di mercato si potrà tradurre in influenza normativa. Si parla di Effetto Bruxelles *de facto* quando le aziende globali non solo decidano di continuare a commercializzare i loro prodotti nel mercato europeo, ma pervengano alla conclusione che è nel loro interesse conformarsi agli standard di produzione europei senza ricorrere alla così detta “differenziazione”, vale a dire senza offrire diversi prodotti per diverse giurisdizioni. Le ragioni che possono condurre alla decisione di adottare uno standard uniforme sono varie: la volontà di mantenere un marchio globale o di mandare ai consumatori un segnale importante di adesione ai valori che guidano il loro comportamento, ottenendo così un beneficio in termini di reputazione; la non divisibilità tecnica della produzione e, anche laddove fosse possibile produrre una certa varietà di dispositivi per altrettanti mercati, qualora le economie di scala rendessero il costo della differenziazione maggiore rispetto al costo della non differenziazione. L’Effetto Bruxelles *de facto* si completa, poi, con l’Effetto Bruxelles *de jure*, il quale si verifica allorquando una giurisdizione straniera adotti regolamenti ispirati alla legislazione unionale. Tale fenomeno si verifica in virtù del fatto che l’UE viene

¹⁰⁶ A. BRADFORD, *The Brussels Effect, How the European Union Rules the World*, Oxford University Press, 2021.

considerata come un modello per l'esperienza nella predisposizione di regole, per il potere di contrattazione e per l'influenza politica generale che esercita.

Ecco allora che la scelta dell'Unione europea di disciplinare l'intelligenza artificiale attraverso una cornice normativa *ad hoc* avente efficacia orizzontale, si colloca, grazie al meccanismo appena illustrato, all'interno di un disegno più ampio volto a consolidare la sua posizione di "*leadship by example*".¹⁰⁷

2. AI Act: la struttura e il modello risk-based

2.1 La definizione di IA e le critiche che solleva

Come già accennato, l'impianto normativo in materia di IA predisposto dal legislatore europeo mira a garantire certezza del diritto e protezione della dignità umana e dei diritti fondamentali, cercando nondimeno di contemperare siffatte esigenze con la necessità di favorire l'innovazione in campo tecnologico. In questa chiave va letta la definizione che il testo dell'art. 3 della proposta di Regolamento offre a proposito di cosa debba intendersi per intelligenza artificiale: "un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni, o decisioni che influenzano gli ambienti con cui interagiscono".¹⁰⁸ Non vi è dubbio che il compito definitorio del legislatore sia di per sé particolarmente difficile, dal momento che il fenomeno IA si caratterizza per la sua rapida evoluzione, tanto da essere descritto in modo efficace come *moving target*.¹⁰⁹ L'ambizione di una definizione così generica è quella di resistere ai possibili sviluppi delle applicazioni di intelligenza artificiale che, come ben noto, tendono a correre molto più velocemente del diritto, ma anche di estenderne il campo di applicazione a quelle più tradizionali

¹⁰⁷ G. LO SAPIO, *Intelligenza artificiale: rischi, modelli regolatori, metafore, in federalismi.it – ISSN 1826-3534*, n. 27/2022, p. 242.

¹⁰⁸ Art. 3 della proposta di Regolamento della Commissione europea (AI Act)

¹⁰⁹ G. MAZZINI, S. SCLAZO, *Relazione al convegno organizzato dall'Università degli Studi di Trento, su "Diritto e potere nell'era dell'intelligenza artificiale"*, 25 febbraio 2022.

che non presentino i caratteri del *machine learning*.¹¹⁰ In particolare, il meccanismo dell'aggiornamento si rende possibile grazie al riferimento all'allegato I, del quale fa menzione anche il successivo art. 4 laddove si tenta di stabilire i confini della definizione di IA proposta attraverso l'elencazione delle tecniche e degli approcci al campo dell'intelligenza artificiale che si considerano interessati dall'applicazione del Regolamento. Tra questi si ritrovano: a) le tecniche di *machine learning*, incluso l'apprendimento supervisionato, non supervisionato e per rinforzo, attraverso l'utilizzo di vari metodi, tra cui anche il *deep learning*; b) gli approcci basati sulla logica e sulla conoscenza, tra i quali i sistemi simbolici; c) gli approcci statistici, di ricerca e i metodi di ottimizzazione. Una delle critiche che viene mossa a proposito di questo riferimento riguarda l'assenza di distinzioni che, in realtà, risultano essere rilevanti; Swedsoft afferma che la definizione non coglie e non dà la necessaria rilevanza alla differenza, da un lato, fra algoritmi e dati e dall'altro fra modelli costruiti attraverso combinazioni di algoritmi e modelli costruiti attraverso combinazioni di dati e nemmeno fra diversi tipi di algoritmi e diversi tipi di dati. Anche questo, per l'appunto, rinforza l'idea di una definizione di IA particolarmente ampia.¹¹¹ E proprio il carattere di ampiezza della definizione di IA è, d'altra parte, il bersaglio delle maggiori critiche rivolte alla stessa: si ritiene, segnatamente, che trattandosi di una definizione di gran lunga più ampia rispetto alla maggior parte delle definizioni di IA, indurrà a ritenere che anche applicazioni tradizionalmente non considerate di intelligenza artificiale ricadano nel campo di applicazione dell'*AI Act*. Inoltre, vi è il sospetto che la genericità sia tale da rendere concretamente inapplicabile la normativa a qualsiasi sistema specifico di IA.¹¹²

¹¹⁰ D. PIANA, G. VICICONTE, *Considerazioni critiche sulla proposta regolativa europea in materia di intelligenza artificiale con attenzione ai profili attuativi*, in *Rivista Corte dei conti*, n. 4/2022, p. 9.

¹¹¹ Swedsoft, *Comments Regarding the European Commission's Proposal for an Artificial Intelligence Act*, 2021, p.3.

¹¹² V. L. RAPOSO, *Ex Machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, n.30/2022, pp. 90-91.

2.2 Il modello risk-oriented: una breve analisi dell'impostazione seguita dal legislatore europeo

Come è già stato più volte ricordato, uno degli obiettivi principali perseguiti dal legislatore europeo nel difficile compito di disciplinare la materia è stato quello di dare priorità alla costruzione del mercato unico; questa specifica rende comprensibile la scelta di adottare quale base giuridica della proposta l'art. 114 TFUE che, come noto, concerne l'adozione di "misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno". Si spiega in questi termini una delle "dimensioni" che è possibile attribuire alla regolazione dell'IA con particolare riferimento all'*AI Act*: una dimensione europea, avvertita come necessaria al fine di evitare che limiti e divieti differenti tra i vari Stati membri possano restringere la libera circolazione dei prodotti e dei servizi.¹¹³ All'originaria base giuridica il Parlamento europeo ha poi recentemente aggiunto¹¹⁴, attraverso degli emendamenti parlamentari, l'art. 16 TFUE, il quale riconosce a qualsiasi persona il diritto alla protezione dei dati di carattere personale. Ciò, tuttavia, come osserva A. Alaimo non è sufficiente a smantellare l'impianto originario della proposta che si presenta poco coerente rispetto alla direzione etico-valoriale paventata attraverso il proprio *memorandum* esplicativo; più incisivo sarebbe stato il riferimento all'art. 119 TFUE, che consente alle Istituzioni di adottare i provvedimenti idonei a contrastare le discriminazioni fondate sui fattori ivi elencati.¹¹⁵ La scelta dello strumento giuridico del regolamento piuttosto che della direttiva, analogamente a quanto accaduto con il GDPR, nonché con il *Digital Services Act* e il *Digital Markets Act*, pare poi la più

¹¹³ C. SCHEPISI, *Le "dimensioni della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *Quaderni AISDUE*, ISSN 2723-9969, Sezione "Atti convegni AISDUE", n. 16/2022, p. 334.

¹¹⁴ Il Parlamento europeo ha approvato in data 14 giugno 2023 il testo dell'*AI Act*, apportando allo stesso alcune modifiche attraverso emendamenti parlamentari.

¹¹⁵ A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in *federalistmi.it - ISSN 1826-3534*, n. 25/2023, p. 138.

idonea a garantire sia la salvaguardia della salute, della sicurezza e dei diritti fondamentali (finalità dichiarata ripetutamente nel testo della proposta) sia ad armonizzare le regole previste per lo sviluppo, l'immissione sul mercato e l'utilizzo dei sistemi di intelligenza artificiale, esplicitando il regolamento efficace diretta negli ordinamento degli Stati membri.¹¹⁶ Ma ciò che più ha catalizzato l'attenzione dei commentatori e che costituisce la caratteristica fondamentale di tale provvedimento è, senz'altro, il modello di regolamentazione fondato sul rischio. In virtù del principio di proporzionalità, il legislatore europeo individua tre categorie di rischio connaturato nell'utilizzo di un determinato tipo di sistema di IA e, sulla base di questa previsione, dispone una serie di divieti o obblighi di natura tecnico-procedimentale diversamente graduati a seconda della gravità del rischio stesso. Tali obblighi gravano, in misura maggiore sui fornitori di sistemi di IA o di servizi IA (i così detti *providers*), in misura minore anche sull'utente o operatore del sistema. La ragione di questa ripartizione viene opportunamente messa in luce da A. Alaimo, la quale lega tale scelta alla base giuridica e al buon funzionamento del mercato interno; secondo l'autrice anche la vigente normativa europea in materia di immissione e circolazione nel mercato dei prodotti di consumo si fonda sulle stesse premesse e così come in quest'ultima normativa, anche nella proposta di Regolamento della Commissione prevale la prospettiva della sicurezza. Si individuano, così, tre livelli di rischio: a) rischio inaccettabile, al quale consegue la proibizione delle pratiche di impiego dei sistemi intelligenti; b) rischio alto, al quale fa seguito l'accertamento di determinati criteri e requisiti necessari affinché il sistema possa essere immesso sul mercato; c) rischio limitato e minimo, che comporta principalmente obblighi di trasparenza. Si procederà ora ad una sintetica analisi ricognitiva di ciò che il legislatore europeo dispone per ciascun tipo di rischio.

¹¹⁶ G. LO SAPIO, *Intelligenza artificiale: rischi, modelli regolatori, metafore*, in *federalismi.it* – ISSN 1826-3534, n. 27/2022, pp. 237-238.

2.2.1 Rischio inaccettabile e pratiche di intelligenza artificiale proibite

Le ipotesi a) e b) dell'art. 5 comma 1 della proposta disciplinano rispettivamente una forma di manipolazione e una forma di manipolazione con aggiunta di *micro-targeting*. La Commissione europea utilizza, quali esempi per chiarire cosa si intenda per manipolazione, il caso di un dispositivo che emetta un suono in grado di agire sulla soglia di attenzione di un camionista, in modo da indurlo a guidare per un tempo maggiore rispetto a quanto si considera umanamente ragionevole (ipotesi sub. a); il caso di un giocattolo dotato di un dispositivo di assistenza vocale attraverso il quale si incoraggia il bambino ad adottare un comportamento pericoloso (ipotesi sub. b). Per determinare l'esistenza di manipolazione si richiede in entrambe le ipotesi il requisito dell'intenzione manipolativa, il quale si somma nell'ipotesi a) alle tecniche subliminali nascoste, mentre nell'ipotesi b) ad una certa vulnerabilità della vittima. Infine, è necessario che il risultato dell'impiego di tali tecniche manipolative sia la causazione effettiva o la mera possibilità di cagionare un danno fisico o psicologico. Si noti che non viene richiesta la prova dell'esistenza di un nesso causale fra le pratiche di manipolazione e il danno, dal momento che anche la mera possibilità del danno rileva ai fini della manipolazione. La norma richiede che l'intenzione manipolativa si ravvisi in capo a chi sviluppa, immette sul mercato o utilizza questi sistemi di IA. La criticità legata a tale requisito è dovuta al fatto che risulta complicato indagare se sussista una intenzione manipolativa, laddove il soggetto in questione non l'abbia espressamente dichiarato. Inoltre, risulta poco chiaro se il danno richiesto dalla normativa debba essere stato cagionato da un unico evento o se sia sufficiente una concomitanza di avvenimenti, che presi singolarmente non sarebbero in grado di causare alcun danno, ma che messi insieme e ripetuti nel tempo conducano a tale effetto.¹¹⁷

Infine, la lettera c) e la lettera d) dell'art. 5 comma 1 stabiliscono che sia proibito l'impiego di sistemi, rispettivamente, di *social scoring* e di identificazione biometrica remota. Merita attenzione, in particolare, questa ultima ipotesi. In via generale la

¹¹⁷ V. L. RAPOSO, *Ex Machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, n.30/2022, p. 92-93.

normativa vieta l'immissione sul mercato, la messa in servizio e l'uso di sistemi di identificazione biometrica (che comportino, quindi, riconoscimento facciale e vocale) a distanza in tempo reale. Sono tuttavia previste una serie di eccezioni, tra le quali alcune riguardanti l'applicazione dei sistemi di IA in campo penale segnatamente per: i) la ricerca mirata di vittime potenziali di reato, compresi bambini scomparsi; ii) la prevenzione di una minaccia sostanziale e imminente alla vita o all'incolumità delle persone fisiche o di un atto terroristico; iii) l'individuazione, la localizzazione, l'identificazione o il perseguimento dell'autore o sospetto autore di una serie di reati.¹¹⁸ Si tratta di una regolamentazione dettagliata, ma al tempo stesso vaga per quanto riguarda il concetto di "identificazione"; si proibiscono i sistemi finalizzati all'identificazione (volti cioè ad identificare nome e cognome dell'individuo), quando in realtà molti sistemi biometrici sono utilizzati per il "riconoscimento" (ossia per categorizzare gli individui in distinte classi o per valutare il loro comportamento). Si presenta, dunque, un problema di *privacy*.¹¹⁹

2.2.2 Rischio alto

I sistemi di IA ad alto rischio sono quelli descritti dall'art. 6. Si tratta essenzialmente di due categorie di prodotti: i prodotti o le componenti di prodotti che richiedono una valutazione di conformità ai fini dell'immissione sul mercato secondo la legislazione UE armonizzata citata nell'allegato II al Regolamento e i sistemi di IA indipendenti (così detti *stand alone systems*) che rappresentano una minaccia per la salute, la sicurezza o i diritti fondamentali e che sono elencanti nell'allegato III. Come previsto dall'art. 7 del Regolamento tale lista dovrà essere aggiornata dalla Commissione europea in concomitanza con i più recenti sviluppi tecnologici. È interessante notare come il rischio alto a cui si fa riferimento non sia legato solo allo specifico

¹¹⁸ Specificamente i reati di cui all'art. 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibili nello Stato Membro interessato con una pena detentiva della durata massima di almeno tre anni come previsto dalla legislazione interna dello Stato interessato.

¹¹⁹ G. CONTISSA, F. GALLI, F. GORDANO, G. SARTOR, *Il Regolamento europeo sull'intelligenza artificiale*, in *i-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale, Rivista semestrale online*: www.i-lex.it, n. 2/2021, pp. 17-18.

funzionamento del sistema, ma anche allo scopo che quest'ultimo persegue. L'uso di questi sistemi di IA è soggetto a una serie di limiti e di requisiti, in particolare aventi a che fare con procedure di controllo e di monitoraggio che possono essere suddivise in due fasi: una prima fase ha luogo prima della immissione sul mercato del sistema e richiede la designazione obbligatoria, da parte degli Stati membri, di una autorità nazionale di notifica, la quale a sua volta dovrà designare gli organismi preposti alla valutazione della conformità del sistema di IA ai requisiti richiesti dal Regolamento; tale valutazione, se positiva, condurrà all'emissione del marchio di conformità CE. Tali organismi sono considerati alla stregua di una terza parte indipendente rispetto ai soggetti coinvolti nel ciclo produttivo del sistema. Una seconda fase che consiste in un meccanismo di monitoraggio *ex post* attuato dalle autorità di sorveglianza del mercato. La marcatura CE si rende necessaria ai fini della libera circolazione del sistema all'interno del territorio dell'Unione europea. I requisiti che il legislatore pone a fondamento del rilascio del marchio di conformità CE fanno riferimento: a) all'alta qualità dei dati utilizzati per il “*training*” del sistema (laddove per dati di alta qualità si intende dati che siano privi di errore, completi, rilevanti e rappresentativi); b) alla trasparenza, in quanto si richiede che il *provider* del sistema renda note tutte le informazioni necessarie affinché il sistema possa essere utilizzato correttamente (caratteristiche, capacità e limiti del sistema, nonché scopo e cure necessarie per la corretta manutenzione); c) alla possibilità che il sistema di IA sia soggetto a supervisione da parte dell'uomo; d) alla precisione, robustezza e cybersicurezza, il cui livello deve essere commisurato allo scopo perseguito dal sistema. Qualora il sistema di IA ad alto rischio già immesso sul mercato fosse poi modificato, sarà necessario sottoporlo ad un nuovo giudizio di conformità. Vi sono poi dei casi in cui il legislatore europeo riconosce la possibilità per i fornitori stessi di auto-certificare la conformità del sistema di IA alla normativa; la giustificazione di simile scelta risiede nella constatazione che i *providers* dovrebbero conoscere meglio di chiunque altro il loro prodotto e, pertanto, sarebbero i più idonei a certificarne la conformità. Si dubita, invero, dell'efficacia di tale impostazione, dal momento che anche il giudizio affidato alle autorità indipendenti suscita perplessità: il timore è che queste autorità si limitino

a verificare che il sistema di IA soddisfi i requisiti formali richiesti dal Regolamento, senza soffermarsi sul rispetto dei diritti fondamentali.

Un ultimo problema è rappresentato dalla circostanza per cui molti sistemi di IA sono, in realtà, componenti di un prodotto già di per sé soggetto ad un giudizio di conformità. Il Regolamento stabilisce in questi casi che la componente IA sia assoggettata al solo giudizio relativo al prodotto finale, giudizio che però andrà effettuato anche alla luce di quei requisiti richiesti dall'*AI Act* che non siano integrati nella normativa di settore in questione.¹²⁰

2.2.3 Rischio limitato e rischio minimo

I sistemi che non rientrano nelle già menzionate categorie si considerano sistemi a rischio limitato o minimo. In questi casi il legislatore non assoggetta i dispositivi di IA alle due fasi di controllo e monitoraggio appena descritte, ma lascia libero il fornitore di creare il proprio codice di condotta al quale attenersi (per quanto riguarda i sistemi a rischio minimo). I pochi requisiti che incontrano i fornitori di sistemi a rischio limitato sono soprattutto obblighi di trasparenza. In questa categoria rientrano, ad esempio, i sistemi la cui funzione è interagire con gli umani, vale a dire i così detti *chatbots* o, più semplicemente, *bots*: com'è noto tali sistemi devono essere progettati in modo tale che gli esseri umani che interagiscono con loro siano messi a conoscenza della loro natura di macchine, a meno che il contesto di utilizzo non renda superflua tale informazione.¹²¹

2.3 Il bilanciamento ex ante nella prospettiva della valutazione del rischio

Di particolare interesse risulta essere l'approfondimento di C. Schepisi con riguardo al peso che assume, nell'ottica di una predisposizione a monte dei vari livelli di rischio sottesi all'utilizzo dei sistemi di IA, il bilanciamento tra i diritti che potrebbero essere

¹²⁰ V. L. RAPOSO, *Ex Machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, n.30/2022, p. 96-99.

¹²¹ V. L. RAPOSO, *Ex Machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, n.30/2022, p. 99-100.

lesi dal comportamento della macchina. Se l'obiettivo del legislatore è quello non solo di non frammentare il mercato unico europeo, ma anche di non frammentare i diritti nella medesima dimensione, la via prescelta per conseguire tale risultato è la definizione a monte della irrinunciabilità di un determinato diritto fondamentale, piuttosto che della sua maggiore o minore rilevanza in un ambito o in una determinata applicazione di IA. Si parte dal presupposto che vi sono danni in grado di cagionare una lesione di un diritto fondamentale talmente grave da non poter essere in alcun modo riparata o compensata a posteriori: per fare un esempio su tutti, i danni arrecati all'integrità fisica o psichica della persona. Si tratta dell'applicazione di un principio riconosciuto sia a livello nazionale che internazionale e richiamato anche dal Consiglio d'Europa nell'ambito della regolazione dell'intelligenza artificiale¹²²: il principio di prevenzione del danno.

È in questo senso che va letta la scelta di costituire la categoria del rischio inaccettabile e il conseguente divieto di sviluppo e di immissione nel mercato di varie categorie di sistemi di IA; la tutela della vita, della salute e della dignità della persona sono avvertite come essenziali dal legislatore europeo, irrinunciabili rispetto a esigenze di carattere economico e prevalenti nel bilanciamento con altri diritti. Vi è poi un'ulteriore operazione che sta alla base della creazione di una tutela multilivello; ci si rende conto che vi sono casi in cui l'applicazione del sistema di IA può sì comportare il rischio di ledere un diritto, ma al contempo può offrire un notevole contributo alla protezione e al rafforzamento di altri diritti (si pensi alle tecnologie impiegate per le diagnosi sanitarie o la ricerca di persone scomparse). È quindi importante comprendere come ai fini dell'immissione nel mercato e dell'utilizzo di un sistema di IA non solo

¹²² Report CAHAI(2020)23 *Ad hoc Committee on artificial intelligence*: "The prevention of harm is a fundamental principle that should be upheld, in both the individual and collective dimension, especially when such harm concerns the negative impact on human rights, democracy and the rule of law. The physical and mental integrity of human beings must be adequately protected, with additional safeguards for persons and groups who are more vulnerable. Particular attention must also be paid to situations where the use of AI systems can cause or exacerbate adverse impacts due to asymmetries of power or information, such as between employers and employees, businesses and consumers or governments and citizens".

venga considerato il bilanciamento tra esigenze di mercato e di protezione dei diritti fondamentali, bensì anche tra diritti diversi; e dal momento che la prevalenza di un diritto sull'altro consegue all'impostazione valoriale che caratterizza ciascun ordinamento giuridico, le scelte effettuate dal Regolamento rispecchiano indubbiamente quello europeo.

Una dimostrazione di quanto appena detto è fornita dalla regolazione dei sistemi di riconoscimento biometrico in *real time* da parte delle autorità pubbliche a fini di contrasto, vietate proprio perché lesive del diritto fondamentale della vita privata e della tutela dei dati personali; qualora tuttavia questi sistemi fossero usati nella ricerca tesa ad individuare potenziali vittime di reato, persone scomparse, minacce di attacchi terroristici, localizzazione e individuazione di presunti autori di una serie di reati elencati nell'allegato II, ecco allora che il diritto alla vita privata e alla tutela dei dati personali cederebbe davanti alla necessità di proteggere l'integrità fisica delle persone. Davanti all'opportunità di perseguire un obiettivo legittimo si considera giustificabile una compressione, sebbene limitata nel tempo, di un diritto fondamentale. Contraddittoria appare, in questo senso, la scelta del legislatore di considerare i sistemi di *deepfake* quali sistemi a rischio lieve soggetti quindi soltanto ad un obbligo informativo, nonostante il Parlamento europeo avesse consigliato di limitarne l'uso, in quanto lesivi della dignità umana e del diritto all'informazione.¹²³ Come se non bastasse, mentre per gli altri sistemi di cui all'art. 52 dell'*AI Act* (come, ad esempio, i sistemi che interagiscono con le persona) la deroga a tale obbligo di informazione è prevista solo qualora vi sia una autorizzazione della legge al fine di accertare, prevenire, indagare e perseguire reati, per i sistemi di *deepfake* si aggiunge un'ulteriore motivo di deroga, rappresentato dal fatto che il loro utilizzo sia "necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele

¹²³ Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI)).

adeguate per i diritti e le libertà dei terzi”. La libertà di espressione, in questo caso, prevale sugli altri diritti considerati dalla norma; questa impostazione pare stridere, tuttavia, con la rilevanza che l’Unione riserva alla protezione della dignità della persona.¹²⁴

3. AI Act: il principio di accountability e il confronto con il GDPR

3.1 La premessa per una analisi comparata

Chiarito brevemente in cosa consiste l’approccio fondato sul rischio adottato dal legislatore europeo, conviene ora riportare l’attenzione sul problema giuridico dal quale siamo partiti e che costituisce il *focus* principale di questa analisi: quale responsabilità per i danni cagionati dai sistemi di IA?

Prima di entrare nel merito dell’*AI Act* e di vedere quale strada si è scelto di percorrere per disciplinare questo aspetto, occorre fare una premessa che porterà ad un esame comparato tra il Regolamento della Commissione europea sull’intelligenza artificiale e il Regolamento generale sulla protezione dei dati personali.¹²⁵ La connessione esistente tra i due provvedimenti si spiega se si pensa che alla base del funzionamento dei sistemi di IA vi sono i dati, per quanto non sempre e non solo dati personali; sempre di più, del resto, si sente parlare di tecnologie *data-driven*. E proprio questa connessione viene presa in considerazione per creare un regolamento che si ispiri, nei suoi tratti principali e in particolare nella sua struttura al GDPR. Ciò che più interessa ai fini di questa disamina è sicuramente l’aspetto legato alla regolazione della responsabilità, che nel testo del Regolamento 2016/679 assume i connotati dell’*accountability*. Si vedrà come lo stesso modello venga mutuato dal campo della protezione dei dati personali a quello della regolazione dell’intelligenza artificiale, sollevando tuttavia una serie di considerazioni critiche.

¹²⁴ Il contenuto di questo paragrafo è tratto da C. SCHEPISI, *Le “dimensioni” della regolazione dell’intelligenza artificiale nella proposta di regolamento della Commissione*, in *Quaderni AISDUE*, ISSN 2723-9969, Sezione “Atti convegni AISDUE”, n. 16/2022, pp. 339-345.

¹²⁵ Regolamento UE 2016/679 in materia di trattamento dei dati personali e di privacy (GDPR).

3.2 La responsabilità del titolare del trattamento nel GDPR: fra liability e accountability

Conviene innanzitutto chiarire che l'art. 82 del GDPR prevede in capo al soggetto leso da un illecito trattamento dei dati personali un vero e proprio diritto al risarcimento del danno, sia patrimoniale che non patrimoniale.¹²⁶ Si introduce, così, una disciplina che differenzia la posizione del titolare del trattamento da quella del responsabile del trattamento, per i quali si prevede un diverso criterio di imputazione della responsabilità: mentre il titolare risponde per il danno cagionato dal trattamento in violazione del regolamento, il responsabile risponde solo allorquando non abbia correttamente adempiuto ai suoi obblighi specifici, o se abbia agito in maniera difforme dalle istruzioni impartitegli dal titolare. Grava, in questo senso, in capo al titolare del trattamento una responsabilità oggettiva per qualunque danno derivante dal trattamento al quale ha dato avvio, da solo o in solido con altri.¹²⁷ Va da sé, tuttavia, che questa impostazione non costituisca una rilevante novità della disciplina sostanziale. Decisamente più significativa risulta essere la scelta di predisporre un sistema di tutele organizzato sulla base del rischio e basato sul principio di *accountability*. Con il termine *accountability* ci si riferisce a un meccanismo di responsabilizzazione, o meglio, ad un principio di responsabilità¹²⁸, in virtù del quale l'accento della disciplina viene posto sull'aspetto della protezione e della sicurezza del trattamento e sulle misure che si rendono necessarie ad evitare o a ridurre i rischi di accesso e divulgazione dei dati non autorizzati o di perdita e distruzione degli stessi. Il legislatore parte dal presupposto che solo attraverso una visione integrata (informatica, giuridica e organizzativa) si possa rispondere efficacemente al problema

¹²⁶ Il testo dell'art. 82 utilizza la locuzione "danni materiali e immateriali", la quale si ritiene solitamente che corrisponda a quella di danno patrimoniale e non patrimoniale; è lo stesso Regolamento che in sede di considerando specificava che "il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento" (considerando n. 146).

¹²⁷ M. COCUCCIO, *Dimensione "patrimoniale" del dato personale e tutele risarcitorie*, in *Diritto di Famiglia e delle Persone*, n.1/2022, pp. 241-243.

¹²⁸ Così viene definito dal Gruppo di lavoro articolo 29 per la protezione dei dati nel parere 3/2010

della sicurezza. Viene individuato nel titolare del trattamento il soggetto al quale affidare l'individuazione e l'adozione delle misure di sicurezza, non prima di una attenta valutazione, sempre affidata a quest'ultimo, della natura dei dati, del contesto, dei rischi e dei costi; inoltre, si richiede allo stesso titolare una successiva attività di monitoraggio continuo al fine di verificare che le misure adottate continuino ad essere proporzionate ai rischi, soggetti a continuo cambiamento. Non solo: al titolare viene anche richiesto di dimostrare di aver adottato le necessarie misure giuridiche, tecniche e organizzative necessarie ad assicurare la protezione dei dati personali.

Si evidenziano due livelli di *accountability*, uno obbligatorio ed uno volontario: il primo è costituito da un obbligo di base che vincola tutti i responsabili del trattamento, ossia l'obbligo di attuare le misure e conservare le relative prove; al contrario, il secondo livello prevede "sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure (norme di attuazione eccedenti il livello minimo".¹²⁹ Non vi sono più indicazioni precise dettate dalla normativa di riferimento; la legge impone ai titolari del trattamento di modulare la concreta attuazione dei principi che la stessa normativa sancisce in astratto.¹³⁰ Riassumendo, quindi, gli elementi essenziali che contribuiscono a costruire il concetto di *accountability* sono: a) la necessità che il titolare del trattamento adotti misure efficaci e proporzionate affinché i principi di protezione dei dati e di sicurezza trovino effettiva attuazione; b) la necessità che lo stesso titolare sia in grado di dimostrare attraverso delle prove che misure efficaci sono in concreto state adottate. Si collega dunque al principio di *accountability* la previsione di meccanismi attraverso i quali si certifica la conformità alle norme delle misure adottate. Appaiono come applicazione del principio di responsabilità e al tempo stesso limitazioni alla discrezionalità del titolare nel decidere come implementare le garanzie di protezione dei dati anche i

¹²⁹ Parere 3/2010 del Gruppo di lavoro articolo 29

¹³⁰ M. COCUCIO, *Dimensione "patrimoniale" del dato personale e tutele risarcitorie*, in *Diritto di Famiglia e delle Persone*, n.1/2022, p. 251.

principi di *privacy by design* e *privacy by default*¹³¹, fondamentali nell'architettura normativa del GDPR.¹³² Come sottolinea D. Barbierato il principio di *accountability* configura un modello di "responsabilità volto alla prevenzione del danno". Vi è dunque una differenza ontologica tra *accountability* e responsabilità civile, poiché la responsabilizzazione *ex ante* si declina come responsabilità *ex post* solo nel momento in cui la componente dell'affidabilità e della conformità viene meno e ciò comporta la causazione di un danno. La versione inglese del considerando 74 rende perfettamente questa distinzione contrapponendo all'espressione "*accountability*" l'espressione "*liability*", che nella versione italiana è riportata con la poco convincente formula di "responsabilità generale".¹³³

3.3 Il principio di accountability nel Regolamento sull'intelligenza artificiale e altre considerazioni critiche

È stata già evidenziata la centralità del legame tra le tecnologie di intelligenza artificiale e i dati nella scelta del legislatore europeo di adottare un modello fondato sul rischio per disciplinare i sistemi di IA. Sia il GDPR che l'AI Act adottano un approccio orientato al rischio fondato su un modello di responsabilità che non contempla solo l'osservanza di disposizioni che impongono obblighi e riconoscono diritti (modello *rights-based*), ma che prevede la diretta responsabilizzazione a monte dei soggetti coinvolti (modello *risk-based*).¹³⁴ Come si è avuto modo di osservare precedentemente, il Regolamento sull'intelligenza artificiale prevede una serie di

¹³¹ L'art. 25 del GDPR prevede, per quanto riguarda il principio di *privacy by design*, che fin dal momento della loro progettazione i sistemi di gestione dei dati devono adottare tutti gli accorgimenti necessari ad assicurare la tutela dei diritti dell'interessato; mentre, per quanto riguarda il principio di *privacy by default*, che tali sistemi per impostazione predefinita debbano utilizzare solo i dati strettamente necessari e sufficienti al raggiungimento della finalità prevista e solo per il tempo necessario a tale finalità.

¹³² Il contenuto del sub-capitolo è prevalentemente tratto da G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Le nuove leggi civili commentate*, n.1/2017, pp. 10-14.

¹³³ D. BARBIERATO, *Trattamento dei dati personali e "nuova" e responsabilità civile*, in *Responsabilità civile e previdenza*, n.6/2019.

¹³⁴ O. POLLICINO, G. DE GREGORIO, *Intelligenza artificiale, data protection e responsabilità*, in F. DONATI, A. PERRUCCI, A. PAJNO (a cura di) *Intelligenza artificiale e diritto*, Il Mulino, volume 2, 2022.

compiti e di obblighi di conformarsi alla disciplina che riguardano produttori, fornitori e utilizzatori, in particolare, di sistemi di IA che presentano un rischio alto. Anche in questo caso, dunque, è possibile parlare di un principio di *accountability*: si richiede a determinati soggetti coinvolti nella progettazione, nella distribuzione e nell'utilizzo di queste tecnologie di adottare delle misure volte a ridurre al minimo il rischio e di provare il rispetto delle stesse.

Il principio di *accountability* così come concepito nel GDPR presenta un connotato che salta subito all'occhio: al titolare del trattamento è lasciata grande discrezionalità nella valutazione del rischio che comporta il procedimento in questione e, per di più, nella scelta delle misure che costituiranno lo standard di protezione dei dati personali. A ben vedere questa flessibilità manca, invece, nel modello *risk-based* presente nel Regolamento sull'intelligenza artificiale. Pur essendo l'*AI Act* orientato alla tutela dei valori europei, non si rintraccia al suo interno quella versatilità che deriva dall'applicare il principio di *accountability* in modo tale per cui si lasciano al titolare del trattamento le scelte riguardanti il rischio e le concrete misure da adottare al fine di ridurlo, come invece accade per il GDPR. Così, mentre il sistema di tutele costruito dal GDPR appare idoneo a modificarsi nel tempo in seguito ai cambiamenti sociali e tecnologici, mantenendo centrale la protezione dei diritti dell'interessato, l'*Artificial Intelligence Act* introduce un approccio fondato sul rischio molto più rigido poiché definito dall'alto dalla Commissione.¹³⁵ Secondo O. Pollicino e G. De Gregorio questo tipo di approccio porta ad una frammentazione del regime di responsabilità, dal momento che la presenza di regole generali e astratte che limitano gli spazi di discrezionalità potrebbe comportare la proliferazione di linee-guida che perseguano l'obiettivo di definire "i limiti applicativi nell'implementazione delle tecnologie di intelligenza artificiale".¹³⁶ Il rigido sistema di *compliance* a cui è sottoposto il

¹³⁵ O. POLLICINO, G. DE GREGORIO, *Intelligenza artificiale, data protection e responsabilità*, in F. DONATI, A. PERRUCCI, A. PAJNO (a cura di) *Intelligenza artificiale e diritto*, Il Mulino, volume 2, 2022.

¹³⁶ O. POLLICINO, G. DE GREGORIO, *Intelligenza artificiale, data protection e responsabilità*, in F. DONATI, A. PERRUCCI, A. PAJNO (a cura di) *Intelligenza artificiale e diritto*, Il Mulino, volume 2, 2022.

provider, pertanto, rischia di frenare il mercato. Gli stessi autori ritengono che l'approccio così detto *top-down* adottato dal Regolamento sull'intelligenza artificiale (contrapposto all'approccio *bottom-up* adottato dal GDPR) renda la normativa incapace di tenere in considerazione il contesto in cui deve operare, al contrario di quanto accade nel GDPR.

Allontanandosi per un attimo dalla logica comparata con il GDPR vi è poi un ulteriore interessante aspetto relativo agli obblighi di *compliance* previsti dall'*AI Act* messo in luce da G. Finocchiaro. Tali obblighi comportano naturalmente un costo che dovrà essere sostenuto dalla società che riveste il ruolo di *provider*; pare evidente che non tutte le società abbiano le stesse dimensioni e le stesse possibilità di conformarsi alla normativa. Si presume che le società di grandi dimensioni non avranno grandi difficoltà a gestire gli oneri relativi alla documentazione, alla certificazione, alla marcatura e tutto il resto; per le piccole imprese e, in particolare, per le *start-up* si profila invece una maggiore difficoltà. Gli obblighi di *compliance*, dunque, si rendono oggetto anche di una critica che riguarda l'adozione di un approccio formale e indifferenziato da parte del Regolamento.¹³⁷

Tornando invece alla dimensione comparata, resta da analizzare ora uno degli aspetti forse più significativi della disciplina con riferimento al tema che costituisce l'oggetto di questo approfondimento: il rapporto fra *accountability* e *liability* nel testo dell'*Artificial Intelligence Act*. Una delle grandi speranze che ruotavano attorno alla creazione di un testo che si pone l'obiettivo di disciplinare orizzontalmente l'IA era sicuramente quella di vedere la nascita di un nuovo modello di responsabilità che meglio rispondesse alle esigenze delle vittime di danni cagionati da sistemi di IA, spesso svantaggiate dalla mancanza, a livello europeo, di una disciplina che tenga conto delle specificità del caso. L'*AI Act*, invero, è silente con riferimento a due importanti aspetti relativi al fondamentale tema della responsabilità. In primo luogo, non prevede alcun diritto di azione nei confronti di *suppliers* o *users* dei sistemi di IA

¹³⁷ G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Rivista trimestrale di diritto pubblico*, n.4/2022, pp. 1096-1097.

per non essersi conformati alla disciplina; l'assenza di specifici meccanismi di compensazione è stata ripetutamente sottolineata sia da autorità dell'Unione europea quali l'EDPB e l'EDPS¹³⁸, sia da gruppi privati a sostegno dei diritti civili.¹³⁹ Come è stato già osservato, l'unica fonte normativa europea che disciplina la così detta *liability* è la Direttiva 85/374/CEE, attualmente oggetto di revisione in vista di una sua possibile applicazione anche ai danni cagionati da sistemi di IA. Ci si aspettava pertanto che la nuova disciplina offrisse uno strumento ulteriore e più adatto a risolvere un problema la cui soluzione, invece, è stata rinviata.

In questa prospettiva si legge una delle principali obiezioni mosse dalla dottrina al testo di legge: non sono previsti rimedi a favore di coloro che si ritengano lesi dall'impiego dei sistemi di intelligenza artificiale. G. Capuzzo nota come da questo punto di vista vi sia allora uno scollamento tra l'approccio "umano-centrico" e le finalità che il Regolamento si prefigge di perseguire (tra le quali la creazione di IA che si possano considerare *trustworthy*) e l'articolato che, al contrario, non prevede a favore degli interessati alcun rimedio o diritto da poter esercitare nei confronti dei soggetti gravati dalla così detta "responsabilizzazione".¹⁴⁰ Ancora una volta il paragone con il GDPR fa emergere una differenza sostanziale: come già si è visto il Regolamento generale sulla protezione dei dati personali appronta un vero e proprio meccanismo di tutela per i singoli individui coinvolti dall'utilizzo dei sistemi di IA, riconoscendo loro non solo un diritto al risarcimento del danno, di cui all'art.82, ma anche altre situazioni giuridiche soggettive tra le quali, ad esempio, il diritto di contestare decisioni che siano il risultato di un processo decisionale completamente automatizzato di cui all'art. 22 del GDPR.¹⁴¹ Sottolinea G. Capuzzo come, in realtà, il

¹³⁸ European Data Protection Board, European Data Protection Supervisor

¹³⁹ V. L. RAPOSO, *Ex Machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, n.30/2022, p. 102.

¹⁴⁰ G. CAPUZZO, *Minority Report. Uno studio su intelligenza artificiale e comparazione giuridica tra UE, USA e Cina*, p. 493.

¹⁴¹ Il diritto di contestazione è stato oggetto di acceso dibattito segnatamente con riferimento al suo contenuto. In C. SARRA, *Put Dialectics into the Machine: Protection against Automatic-decision-making through a Deeper Understanding of Contestability by Design*, in *Global Jurist*, 2020, l'autore individua nel diritto di contestazione la vera chiave di volta del sistema di tutele offerte a colui che subisce una decisione automatizzata; il diritto all'intervento umano e ad esprimere la propria

paragone con il GDPR da questo punto di vista possa risultare improprio. I dati di cui si nutrono i sistemi di IA per poter funzionare sono solo in minima parte dati personali e questo conduce a ritenere che, se diversa è la natura dei dati oggetto delle due discipline, necessariamente diversa sarà anche la natura della protezione giuridica; in questo senso tale protezione non andrà più accordata solo a livello individuale, ma andrà riconosciuta ai gruppi sociali a cui i dati in questione si riferiscono.¹⁴² Va tuttavia constatato anche il mancato riconoscimento di una tutela collettiva all'interno dell'*Artificial Intelligence Act*.

GDPR e *Artificial Intelligence Act* convergono invece nella previsione di sanzioni amministrative pecuniarie laddove vi sia il mancato rispetto delle regole previste nei rispettivi testi di legge.

Per concludere questo tema pare degna di nota l'impostazione che ne viene data da G. Comandè, a parere del quale l'*accountability* sarebbe la risposta corretta alla domanda di regolamentazione dei nuovi sistemi di IA, non potendo la sola liability farsi carico di una soluzione olistica. La responsabilità civile è certo in grado di svolgere un ruolo di riallocazione della perdita dal soggetto leso ad altro soggetto, senza però far sorgere gli incentivi di prevenzione. Sarebbe dunque più corretto adottare la logica della responsabilizzazione e, di volta in volta, integrare questa scelta con la regola di

opinione sarebbero, infatti, ricompresi a loro volta nel diritto di contestare la decisione, diritto quest'ultimo che, se interpretato come avente contenuto procedurale, presuppone la sussistenza di una serie di altri diritti che il titolare del trattamento dovrebbe garantire al destinatario della decisione. Nel testo si prospetta, inoltre, l'adesione alla corrente dottrinale per cui il destinatario del trattamento avrebbe anche, nel contesto delle decisioni automatizzate, un diritto ad ottenere una spiegazione. Ne fa menzione il Considerando 71, ma nel testo del GDPR non se ne trova traccia; ebbene, nonostante vi sia chi, adottando un approccio formalistico e una interpretazione letterale, afferma che la sua assenza nel testo del GDPR sia frutto di una precisa scelta del legislatore, si ritiene di condividere un diverso orientamento alla luce del quale tale diritto esisterebbe e sarebbe legato proprio al diritto a contestare la decisione; meglio, il contenuto di tale diritto sarebbe di volta in volta legato al concreto uso di simile tutela. Ecco allora che il GDPR riconosce in capo al destinatario del trattamento persino più diritti di quelli che si possono identificare sulla scorta di una rapida lettura del testo.

¹⁴² G. CAPUZZO, *Minority Report. Uno studio su intelligenza artificiale e comparazione giuridica tra UE, USA e Cina*, p. 494.

responsabilità civile che risulta più opportuna, a seconda della finalità che ci si prefigga (risarcimento o deterrenza).¹⁴³

4. La proposta di direttiva sulla responsabilità dell'IA nel solco della strategia digitale dell'Unione europea

4.1 IA Liability Directive: brevi cenni introduttivi

Si è fin qui avuto modo di osservare, pur avvertendo la necessità di predisporre un sistema di tutele in grado di rispondere alle esigenze di protezione proprie di chi si ritiene leso dai danni cagionati dai sistemi di IA, il legislatore non sia stato in grado fino ad ora di introdurre un sistema di norme armonizzate in materia di responsabilità civile extracontrattuale capace di colmare simile lacuna nell'ordinamento europeo. Lo stesso *Artificial Intelligence Act* rinvia la questione concentrandosi sull'aspetto della responsabilizzazione del *provider* e dello *user* e avendo quindi riguardo a una tutela *ex ante* in un'ottica di prevenzione del rischio, piuttosto che a una tutela risarcitoria *ex post*. Vi sono, tuttavia, due importanti proposte della Commissione europea che si inseriscono nel complesso pacchetto normativo volto a regolare l'IA in modo unitario e che puntano i riflettori sulla necessità di adeguare le norme sulla responsabilità civile all'era digitale. Si tratta della proposta di revisione della direttiva sulla responsabilità da prodotto difettoso e della proposta di direttiva sulla responsabilità dell'IA (*IA Liability Directive*), entrambe presentate dalla Commissione europea in data 28 settembre 2022. Si noti che è già stata condotta una breve analisi relativa alla prima, la quale verrà qui menzionata al solo fine di mettere a confronto alcuni aspetti fondamentali che la contraddistinguono dalla proposta di direttiva sulla responsabilità dell'IA. Innanzitutto, mentre l'AILD si propone di disciplinare direttamente i sistemi di intelligenza artificiale, la così detta "*PLD proposal*" presenta un ambito di

¹⁴³ G. COMANDE', *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, ISSN 1720-951X, n.1/2019, pp.186-186.

applicazione più esteso, disciplinando i danni cagionati in generarle da qualsiasi *software*. Per questo motivo si ritiene che gli ambiti di applicazione di ciascuna proposta non si dovrebbero sovrapporre tra loro. A questo proposito P. Hacker sottolinea come, invero, molte società affermino di utilizzare sistemi di IA, quando in realtà si limitino a fare uso di *software* standard o algoritmi leggermente più complessi, comunque non riconducibili all'IA *stricto sensu*; questo potrebbe condurre i soggetti lesi a scegliere il regime normativo scorretto.¹⁴⁴ Ancora, mentre la *PLD Proposal* contiene sia norme sostanziali che norme procedurali, l'AILD adotta un approccio puramente procedurale disciplinando l'armonizzazione delle sole regole relative all'onere della prova e alla divulgazione di informazioni; ciò nonostante entrambe perseguono l'obiettivo di assicurare una compensazione effettiva alla persona lesa e di colmare i vuoti di responsabilità che sorgono in conseguenza delle peculiarità delle nuove tecnologie (*responsibility gaps*).¹⁴⁵ Altra differenza fondamentale è rappresentata dal grado di armonizzazione che le due proposte intendono porre in essere: da una parte (*PLD Proposal*) un'armonizzazione piena, dall'altra (*AI Liability Directive*) un'armonizzazione minima e riguardante le sole regole procedurali; ciò significa che residua in capo agli Stati membri la possibilità di adottare misure più favorevoli per il danneggiato. Cambiano anche i legittimati passivi, poiché mentre ai sensi della *PLD Proposal* è possibile agire solo nei confronti dei così detti "operatori economici" (categoria che comprende i produttori e i soggetti coinvolti nel ciclo produttivo), ai sensi della AILD è possibile agire anche nei confronti degli utilizzatori professionali e non professionali (i consumatori).¹⁴⁶ Le definizioni di *providers* e di *users* che la AILD prende in considerazione ai fini dell'individuazione dei legittimati passivi fanno riferimento alle stesse categorie di cui all'*AI Act*; sussiste quindi una fondamentale coordinazione tra i due provvedimenti attraverso la quale viene anche

¹⁴⁴ P. HACKER, *The European AI liability directives - Critique of a half-hearted approach and lessons for the future*, in *Computer Law and Security Review*, n. 51/2023, p. 6.

¹⁴⁵ P. HACKER, *The European AI liability directives - Critique of a half-hearted approach and lessons for the future*, in *Computer Law and Security Review*, n. 51/2023, p. 6.

¹⁴⁶ P. HACKER, *The European AI liability directives - Critique of a half-hearted approach and lessons for the future*, in *Computer Law and Security Review*, n. 51/2023, p. 7.

definito il perimetro di applicazione della proposta; al contrario, molti meno riferimenti all'*AI Act* si possono scorgere nella *PLD Proposal*.¹⁴⁷ Infine, una differenza sostanziale riguarda il tipo di responsabilità sanzionabile ai sensi delle due proposte: nel caso della *PLD Proposal* il riferimento continua ad essere ad una responsabilità oggettiva dell'operatore economico, mentre la AILD disciplina una responsabilità fondata sulla colpa e, segnatamente, originante dalla violazione di un dovere di diligenza. Anche in questo caso il collegamento con l'*AI Act* e con il regime di responsabilizzazione *ex ante* è evidente; ci troviamo di fronte ad una normativa che si pone con quest'ultimo in un rapporto di complementarità.

4.2 Le regole procedurali in breve

L'*AI Liability Directive* rappresenta uno strumento giuridico attraverso il quale si consente a qualunque soggetto, pubblico o privato che sia, di promuovere un giudizio davanti ai giudici nazionali per far valere l'inosservanza della diligenza dovuta da parte di sviluppatori, fornitori o utenti (compresi, come già visto, i consumatori) nel caso in cui tale inosservanza abbia comportato la lesione di situazioni giuridiche soggettive ritenute meritevoli di tutela dalla legge nazionale. Come sottolineato in precedenza, si tratta di un regime di armonizzazione minima, poiché dopo aver definito il dovere di diligenza, le uniche regole comuni che vengono dettate dalla proposta riguardano l'onere della prova; si lascia, invece, agli Stati membri la possibilità di applicare la normativa interna con riguardo ad alcuni aspetti generali della responsabilità civile, fra i quali la definizione di colpa, di causalità e i tipi di danno che determinano le richieste di risarcimento.¹⁴⁸ Tale regime costituisce per questo oggetto di critiche secondo le quali si favorirebbe in questo modo una frammentazione della disciplina.

La proposta mira ad alleggerire la posizione probatoria del soggetto leso da un danno cagionato da un sistema di IA in ragione delle caratteristiche, già esaminate in questa

¹⁴⁷ P. HACKER, *The European AI liability directives - Critique of a half-hearted approach and lessons for the future*, in *Computer Law and Security Review*, n. 51/2023, p. 11.

¹⁴⁸ G. D'ALFONSO, *Intelligenza artificiale e responsabilità civile. Prospettive europee*, in *Revista de Estudios Juridicos y Criminologicos*, ISSN-e 2345-3456, n.6/2022, p. 187.

sede, che contraddistinguono tali tecnologie. Il legislatore ricorre, a questo fine, all'individuazione di strumenti quali: a) l'applicazione della così detta presunzione relativa; b) la divulgazione di informazioni relative. Si individuano tre regimi in tema di onere probatorio che pur non comportando un'inversione tra presunto danneggiato e danneggiante, agevolano le parti lese nel provare la fondatezza delle loro pretese.¹⁴⁹ In particolare, l'art. 4 elenca tre condizioni che, se soddisfatte, comportano che gli organi giurisdizionali nazionali debbano presumere l'esistenza di un nesso di causalità tra la colpa del convenuto e l'output del sistema di IA o la sua mancata produzione. Un secondo regime si applica invece alle domande di risarcimento proposte contro un fornitore di IA ad alto rischio (così come definite dall'*AI Act*): in questo caso si prevede un'eccezione alla presunzione di causalità allorché il convenuto dimostri che l'attore è in grado di accedere a elementi di prova, potendo così dimostrare da sé l'esistenza del nesso causale; di contro, per i sistemi non ad alto rischio la presunzione di causalità opera soltanto laddove l'organo giurisdizionale accerti che per l'attore sia eccessivamente difficile e gravoso provare il nesso causale. Un ultimo regime probatorio riguarda l'utilizzo di un sistema di IA nel corso di una attività personale non professionale; l'art. 4 stabilisce che la presunzione di causalità si applica qui solo quando il convenuto abbia interferito materialmente con le condizioni di funzionamento del sistema di IA oppure quando abbia l'obbligo e sia in grado di determinare le condizioni di funzionamento del sistema e non l'abbia fatto.

4.3 Riflessioni conclusive sulla proposta di AI Liability Directive

Anche se si tratta, allo stato attuale, di una mera proposta, l'*AI Liability Directive* rappresenta una buona occasione per il legislatore europeo di costruire un sistema multilivello di distribuzione di responsabilità tra i diversi operatori del settore, in grado di coprire l'intero processo di produzione e applicazione dell'intelligenza artificiale.¹⁵⁰

¹⁴⁹ C. DEL FEDERICO, *Intelligenza artificiale e responsabilità civile. Alcune osservazioni sulle attuali proposte europee*, in *Jus Civile*, ISSN 2281-3818/2421-2563, n. 5/2023, pp. 1039-1040.

¹⁵⁰ C. DEL FEDERICO, *Intelligenza artificiale e responsabilità civile. Alcune osservazioni sulle attuali proposte europee*, in *Jus Civile* ISSN 2281-3818/2421-2563, n. 5/2023, p. 1043.

Se con l'*AI Act* si perseguono fini di tutela dei diritti fondamentali attraverso meccanismi preventivi volti a minimizzare il rischio, con questa proposta si cerca di incidere sui meccanismi procedurali con l'obiettivo di rendere più agevole la posizione dell'attore presumibilmente leso da un sistema di IA. In questo contesto una delle speranze degli studiosi pare essere la realizzazione di un perfetto allineamento tra le due normative, di tal modo che la violazione dei precetti dell'*AI Act* sia condizione necessaria e sufficiente per l'attivazione della tutela processuale riconosciuta dalla direttiva.¹⁵¹ Vi sono tuttavia anche delle criticità riguardanti la normativa così come attualmente concepita; una fra tutte è quella che riguarda l'eccessiva discrezionalità riconosciuta ai singoli Stati membri sul profilo della responsabilità, che rischia di rendere inutile i tentativi di uniformità che le Istituzioni europee stanno cercando di portare avanti.

Si partirà proprio dalla considerazione che ogni Stato presenta un diverso regime di responsabilità extracontrattuale applicabile ai casi di cui ci si occupa per analizzare, nel successivo capitolo, quale possibile applicazione della normativa italiana risulti più opportuna a dirimere le controversie aventi ad oggetto il risarcimento del danno da sistema intelligente.

¹⁵¹ P. HACKER, *The European AI liability directives - Critique of a half-hearted approach and lessons for the future*, in *Computer Law and Security Review*, n. 51/2023, p. 33.

IV. Il modello interno della responsabilità extracontrattuale: gli strumenti del diritto civile italiano come risposta ai “nuovi” danni da sistemi di IA

1. Le tradizionali ipotesi di responsabilità vicaria: il robot come essere senziente; 2. L'applicabilità degli artt. 2050 e 2051 c.c.: il robot come prodotto; 3. L'art. 2054 c.c. e il futuro della r.c.a.

1. Le tradizionali ipotesi di responsabilità vicaria: il robot come essere senziente

1.1 Una breve ricognizione degli strumenti sin qui analizzati

Si è dato spazio fino a questo momento all'analisi delle soluzioni al problema di stampo europeo, concentrandosi in particolare sugli strumenti normativi esistenti e, in linea di principio, applicabili estensivamente al caso dei danni da sistemi intelligenti, da un lato, e agli strumenti normativi che si propongono di disciplinare la materia ma che ancora non sono entrati in vigore, dall'altro. Segnatamente, si fa riferimento alla Direttiva 84/375/CEE e all'*AI Act*, provvedimenti delle Istituzioni europee che già trovano o troveranno presto attuazione negli ordinamenti giuridici nazionali degli Stati membri. Come si è già osservato, le previsioni della Direttiva *Product Liability* sono confluite nel Codice del consumo italiano e trovano oggi applicazione in tutti quei casi in cui ad essere lesa sia un soggetto qualificabile come consumatore. La normativa individua, infatti, in modo assai circoscritto, i casi interessati dall'applicazione della stessa: oltre alla qualifica del soggetto lesa, occorre che il danno sia stato cagionato da un dispositivo che presenti un difetto di progettazione o di fabbricazione. Si intuisce immediatamente come vi siano danni che non potranno essere interessati dal rimedio riparatorio di cui alla normativa in questione. Ci si domanda allora se - anche alla luce di questa considerazione e tenuto conto del fatto che vi sono strumenti che ancora non possono essere invocati in quanto non ancora vigenti - vi siano norme di diritto interno capaci di dare risposta all'esigenza di regolamentazione del fenomeno di cui si discute.

Si chiarisce fin da ora che non sono oggetto di questa trattazione i casi in cui il danneggiato può agire in giudizio ai sensi dell'art. 1218 c.c., vale a dire quando vi sia una relazione contrattuale che lo leghi ai soggetti coinvolti nel ciclo di produzione e immissione sul mercato del sistema intelligente; tale eventualità gli consentirà di ottenere ristoro per il danno subito invocando l'inadempimento di una o più obbligazioni contrattuali.

Se, quindi, oggetto dell'indagine è la sola responsabilità aquiliana, non vi è dubbio che la prima norma che si dovrebbe prendere in considerazione quale strumento per regolamentare i danni causati dagli *smart devices* è l'art. 2043 c.c.; invero, pur essendo previsione generale e atipica, connotata dal principio di neutralità tecnologica, tale norma appare inidonea a disciplinare i suddetti danni. In primo luogo, il danneggiato incontrerebbe l'ostacolo della prova dell'elemento soggettivo della colpevolezza del danneggiante;¹⁵² inoltre, come già visto precedentemente, nel caso dei sistemi di IA risulta particolarmente complesso risalire all'autore materiale dal danno, essendo le tecniche di progettazione e produzione del sistema molto complesse e coinvolgendo una pluralità di attori. In virtù di queste considerazioni, si è ritenuto che l'applicazione dell'art. 2043 c.c. sia inappropriata nei casi in cui si verifichi un così detto "danno anonimo", considerando più opportuno il ricorso a norme che permettano di individuare un soggetto al quale imputare la responsabilità a prescindere dall'accertamento dell'elemento soggettivo della colpa.¹⁵³

Ci si concentrerà, *in primis*, sulle norme di cui agli articoli 2047, 2048 e 2049 del Codice civile, che disciplinano ipotesi di responsabilità vicaria.

¹⁵² G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e "responsabilità da algoritmo"*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 103.

¹⁵³ G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e "responsabilità da algoritmo"*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 103.

1.2 La responsabilità per danno cagionato dall'incapace e la sua applicazione analogica

Si è già avuto modo di vedere come, seppur vi siano orientamenti dottrinali che riconoscono la possibilità e addirittura auspicano che i sistemi intelligenti siano riconosciuti quali soggetti di diritto al fine di poter loro imputare una responsabilità diretta per i danni da questi cagionati, la maggior parte degli studiosi neghi che tale riconoscimento possa di fatto raggiungere l'obiettivo che si pone, ovvero sia incrementare la tutela nei confronti dei soggetti lesi. Al contrario, si sottolinea come attraverso la creazione di una personalità giuridica *ad hoc* la protezione delle vittime di danno diminuirebbe sensibilmente. Ecco allora che, se si volesse comunque abbracciare, secondo una prospettiva antropomorfica, la teoria secondo la quale i sistemi di IA sono esseri senzienti dotati di intelligenza (seppure non umana), si dovrebbe far ricorso all'applicazione analogica degli art. 2047, 2048 e 2049 del Codice civile.

Ai sensi dell'art. 2047 c.c.¹⁵⁴, qualora il fatto dannoso sia commesso da persona non imputabile ex art. 2046 c.c., tenuto a riparare il pregiudizio è colui su cui grava un dovere di sorveglianza dell'incapace; presupposto applicativo è, dunque, che il danno sia cagionato da persona incapace di intendere e di volere e alla quale, pertanto, non sia direttamente imputabile la responsabilità per il fatto commesso. Il sorvegliante potrà liberarsi, tuttavia, dimostrando di non aver potuto impedire il fatto. La norma fa riferimento alla mancanza di capacità di intendere e di volere, così che interessati dall'applicazione dell'art. 2047 c.c. sono, ad esempio, gli illeciti commessi dal minore in tenera età, per i quali risponderanno i genitori non già nella veste di esercenti la patria potestà, bensì quali sorveglianti del soggetto non imputabile.¹⁵⁵ Il dovere di

¹⁵⁴ Art. 2047 c.c.: *"In caso di danno cagionato da persona incapace di intendere o di volere, il risarcimento è dovuto da chi è tenuto alla sorveglianza dell'incapace, salvo che provi di non aver potuto impedire il fatto."*

Nel caso in cui il danneggiato non abbia potuto ottenere il risarcimento da chi è tenuto alla sorveglianza, il giudice, in considerazione delle condizioni economiche delle parti, può condannare l'autore del danno a un'equa indennità".

¹⁵⁵ Cass., 15.1.1980, n. 369, in *Giur. it.*, 1980, I, 1, c. 597.

sorveglianza può trovare la sua fonte nella legge (come nel caso dei genitori, dei tutori e degli affidatari nei confronti dei figli), nel contratto o in una libera scelta. Per quanto concerne la responsabilità gravante sul soggetto tenuto alla sorveglianza, sebbene ancora vi sia una parte della dottrina che la ritiene qualificabile come responsabilità per fatto altrui¹⁵⁶ (non essendo il sorvegliante l'autore materiale dell'illecito), la giurisprudenza ha chiarito che si tratta di responsabilità diretta derivante dalla violazione del dovere di custodia in capo al sorvegliante (*culpa in vigilando*).¹⁵⁷ Secondo questa ricostruzione ci troveremmo di fronte, allora, non ad una ipotesi di responsabilità oggettiva, bensì ad una ipotesi di responsabilità aggravata; spetterebbe al sorvegliante provare di non aver potuto impedire il fatto per poter vincere la presunzione relativa alla propria colpa. Infine, il secondo comma dell'art. 2047 c.c. prevede che qualora il sorvegliante riesca a fornire la prova liberatoria, il giudice potrà valutare se condannare o meno l'incapace al pagamento di un'equa indennità, avuto riguardo alle condizioni economiche delle parti.

Orbene, qualora si volesse creare un parallelo fra il soggetto incapace di intendere e di volere e il sistema di IA "senziente", ma privo della stessa capacità, si potrebbe pensare di ricorrere all'applicazione analogica dell'art. 2047 c.c. ogni qual volta il comportamento della macchina intelligente tenga un comportamento lesivo della sfera giuridica del terzo. Bisognerebbe prima di tutto individuare, in questo caso, il soggetto su cui grava il dovere di vigilanza del sistema di IA; sulla scorta di quanto detto precedentemente a proposito della fonte di tale dovere, si potrebbe pensare al "proprietario" del dispositivo o, quanto meno, al soggetto che trae i maggiori benefici dall'attività del sistema. Per contro, al produttore del dispositivo, al creatore dell'algoritmo o all'addestratore non potrebbe imputarsi alcuna responsabilità,

¹⁵⁶ M. FRANZONI, *L'illecito I*, in *Tratt. Franzoni*, Milano, 2010, p. 692.

¹⁵⁷ Cass. Civ., sez. III, sentenza n. 12965/2005: "*La responsabilità civile del soggetto tenuto alla sorveglianza di una persona incapace, la quale abbia cagionato danni a terzi, deriva dall'art. 2047 c.c., che dà luogo ad una responsabilità diretta e propria di coloro che sono tenuti alla sorveglianza, per inosservanza dell'obbligo di custodia, ponendo a carico di essi una presunzione di responsabilità, che può essere vinta solo dalla prova di non avere potuto impedire il fatto malgrado il diligente esercizio della sorveglianza impiegata*".

essendo il sistema uscito dalla loro sfera di vigilanza. Si noti inoltre che, a questo punto, onerato di fornire la prova liberatoria sarebbe proprio il “proprietario” del dispositivo intelligente, tenuto pertanto a dimostrare l’esistenza di un nesso di causalità tra l’omessa sorveglianza e il danno cagionato dal dispositivo stesso; tale prova risulterebbe senz’altro difficile da produrre in giudizio, con la conseguenza che nella maggior parte dei casi il danneggiato godrebbe di un regime di assoluto favore. Infine, nella rara ipotesi in cui il sorvegliante riuscisse a fornire la prova di cui sopra, diverrebbe inapplicabile il secondo comma dell’art. 2047 c.c., poiché il giudice non potrebbe disporre del suo potere equitativo a meno di non riconoscere soggettività giuridica al sistema intelligente, dotandolo quindi di un patrimonio proprio. Si arriva dunque alla conclusione, condivisa da gran parte della dottrina,¹⁵⁸ per la quale l’applicazione analogica dell’art. 2047 c.c. non sarebbe opportuna.

1.3 La responsabilità dei precettori e la sua applicazione analogica

Pur se collegato all’art. 2047 c.c., l’art. 2048 c.c.¹⁵⁹ disciplina una fattispecie che si discosta da quella appena descritta in alcuni punti fondamentali. Segnatamente, si stabilisce che i genitori o i tutori, i precettori e i maestri d’arte siano tenuti a rispondere del danno cagionato dal fatto illecito commesso, rispettivamente, dai figli minori che con essi convivano, dagli allievi e dagli apprendisti (anch’essi minori¹⁶⁰) per tutto il tempo in cui siano sottoposti alla loro vigilanza.

¹⁵⁸ Per una opinione contraria si veda A. SANTOSUOSSO, M. TOMASI, *Diritto, scienza, nuove tecnologie*, Wolters Kluwer, 2021, pp. 338 ss.

¹⁵⁹ Art. 2048 c.c.: *“Il padre e la madre, o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi. La stessa disposizione si applica all'affiliante.*

I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza.

Le persone indicate dai commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto.”

¹⁶⁰ Cass. Civ., sez. III, sentenza n. 7387/2001: *“La presunzione di colpa di cui all'art. 2048, comma 2, c.c. non può ritenersi applicabile [...] nel caso in cui l'allievo sia persona maggiore d'età, dovendosi presumere che, all'interno della stessa disposizione, il legislatore non abbia voluto riservare ai precettori e maestri d'arte un trattamento peggiore rispetto a quello dei genitori di cui al comma 1, dilatando la loro responsabilità oltre il limite temporale della minore età del danneggiante.”*

La dottrina si è soffermata, in particolar modo, sull'elemento dell'incapacità di intendere e di volere del minore, vero e proprio discrimine fra l'art. 2047 e l'art. 2048 c.c.; qualora il minore difetti della capacità di intendere e di volere sarà applicabile l'art. 2047 c.c., mentre nel caso in cui quest'ultimo sia dotato di tale capacità invocabile sarà, allora, l'art. 2048 c.c. Nello specifico, il dibattito generatosi sul punto riguarda la possibilità che proprio la capacità di intendere e di volere del minore che commette il fatto illecito dannoso possa far sorgere ai sensi dell'art. 2048 c.c. una responsabilità diretta del genitore, del precettore o del maestro d'arte, la quale si aggiunge in via cumulativa a quella dell'autore materiale del fatto.¹⁶¹ Vi è tuttavia chi, sulla base di una interpretazione letterale del testo dell'art. 2048 c.c., ritiene invocabile la sola responsabilità delle figure sopra citate.¹⁶²

Per terminare la disamina della fattispecie, va infine sottolineato come, anche in questo caso, dottrina e giurisprudenza inquadrino la responsabilità ex art. 2048 c.c. come responsabilità aggravata, con la conseguenza che saranno i genitori, precettori e maestri d'arte a dover fornire la prova liberatoria al fine di superare la presunzione di colpevolezza che grava su di loro. Qui, come per l'art. 2047 c.c., l'*onus probandi* consiste nel dimostrare di non aver potuto impedire il fatto, ma la giurisprudenza ha individuato un contenuto differente di tale onere a seconda che esso gravi sui genitori, da un lato, ovvero sui precettori e maestri d'arte, dall'altro. Se di *culpa in vigilando* risponderanno tutti i soggetti di cui al disposto dell'art. 2048 c.c., soltanto i genitori, al contrario, saranno tenuti a far fronte anche all'eventuale presenza di *culpa in educando*. Si tratta di un concetto elaborato dalla giurisprudenza che esplica notevoli ripercussioni in materia di onere della prova. Se ai sensi dell'art. 147 c.c.¹⁶³ i genitori

¹⁶¹ Così, Cass. Civ., sez. III, sentenza n. 8470/2001: "L'art. 2048 c.c. postula l'esistenza di un fatto illecito compiuto da un minore capace di intendere e di volere, in relazione al quale soltanto è configurabile la "culpa in educando" e la "culpa in vigilando". Pertanto, la responsabilità dei genitori o precettori ex art. 2048 cit. viene a concorrere con la responsabilità del minore."

¹⁶² F. FRIGIDA, *Responsabilità del sorvegliante dell'incapace, dei genitori e tutori, dei padroni e Committenti*, in *La Responsabilità Civile*, Giuffrè, 2018, pp. 1798 e ss.

¹⁶³ Art. 147 c.c.: "Il matrimonio impone ad ambedue i coniugi l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni, secondo quanto previsto dall'articolo 315 bis."

hanno, fra gli altri, il dovere di educare i figli, ecco che allora per superare la presunzione di responsabilità in caso di danno cagionato dal figlio minore saranno non solo tenuti a fornire la prova positiva di avere esercitato una adeguata vigilanza sullo stesso, ma anche quella di avergli impartito una buona educazione.¹⁶⁴

Cercando ora, ancora una volta, di capire se sia possibile applicare l'art. 2048 c.c. analogicamente ai danni cagionati dai sistemi di IA, va prima di tutto tenuto conto del fatto che risulta particolarmente difficile l'adeguamento laddove si disciplini la responsabilità dei genitori; il "proprietario" del dispositivo o comunque, colui che beneficia della sua attività, non svolge alcun ruolo in tal senso.

Tuttalpiù si potrebbe pensare alla possibilità di imputare simile responsabilità al programmatore del sistema, il quale sarebbe paragonabile al precettore nel momento in cui insegna alla macchina a tenere un certo comportamento. Anche qui, invero, si renderebbe necessario un correttivo laddove la norma richiede, ai fini dell'imputazione della responsabilità, che il danno sia stato cagionato nel tempo in cui l'allievo era sottoposto alla vigilanza del precettore. Il programmatore della macchina, una volta svolto il suo compito, non ha più la possibilità di esercitare un controllo sulla stessa e di impedire, dunque, il verificarsi del danno.¹⁶⁵

Sarebbe allora opportuno superare il concetto di *culpa in vigilando* quale criterio di imputazione della responsabilità e introdurre un nuovo concetto di *culpa in educando*, il cui contenuto si adatti alle peculiarità del rapporto programmatore-macchina.

Rimarrebbe tuttavia problematica la questione della prova liberatoria. Si dà infatti la possibilità che il programmatore "educi" moltissimi sistemi intelligenti distinti fra loro, rimanendo così esposto al rischio di essere chiamato a risarcire tutti i danni cagionati dagli stessi; in tal caso non solo il patrimonio a cui attingere per i ristori dei danni sarebbe limitato, ma tale impostazione produrrebbe conseguenze negative anche sul piano dello sviluppo tecnologico, scoraggiando la produzione dei sistemi di IA. Sarebbe dunque necessario alleggerire l'*onus probandi* in capo al programmatore. A

¹⁶⁴ Cass. Civ., sez. III, sentenza n. 24475/2014.

¹⁶⁵ A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *La Nuova Giurisprudenza Commentata*, 2012.

tal proposito U. Pagallo prospetta l'ipotesi di una prova liberatoria che consista nel dimostrare di non aver potuto prevenire il danno a causa della condotta (negligente o intenzionale) del danneggiato.¹⁶⁶

Al netto dell'analisi e delle proposte sin qui illustrate, può dunque concludersi che anche l'applicazione analogica dell'art. 2048 c.c. risulta insuscettibile di risolvere i problemi posti dall'intelligenza artificiale.

1.4 La responsabilità dei committenti e la sua applicazione analogica

L'art. 2049 c.c.¹⁶⁷ chiude la disamina delle ipotesi di responsabilità vicaria discostandosi tuttavia da quelle precedentemente esaminate. La norma disciplina la responsabilità dei committenti per i danni cagionati dalla condotta illecita dei propri commessi nello svolgimento delle attività cui sono adibiti.

Contrariamente alle norme viste sin qui, l'art. 2049 c.c. describe, secondo la dottrina maggioritaria, un'ipotesi di responsabilità oggettiva;¹⁶⁸ l'obiettivo del legislatore pare essere quello di responsabilizzare il committente per l'errore del suo commesso, a prescindere dal fatto che sussista o meno la colpa dell'imprenditore e senza offrire pertanto a quest'ultimo la possibilità di fornire una prova liberatoria. Tra gli elementi costitutivi della fattispecie, dottrina e giurisprudenza individuano: a) l'esistenza di un rapporto di preposizione tra committente e commesso; b) una condotta illecita del commesso, perlomeno colposa; c) un nesso di occasionalità necessaria tra il danno e la condotta del commesso nell'esercizio dell'attività che è tenuto a svolgere.¹⁶⁹ A ben vedere, qualora il committente riuscisse a provare l'inesistenza di uno di questi requisiti potrebbe liberarsi dalla responsabilità.

Delineati i punti fondamentali della fattispecie, ci si deve concentrare ora sul ruolo che questa norma potrebbe svolgere nel disciplinare i danni da sistemi di IA.

¹⁶⁶ U. PAGALLO, *The Laws of Robots: Crimes, Contracts and Torts*, Springer, 2013, p. 128.

¹⁶⁷ Art. 2049 c.c.: *"I padroni e i committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti."*

¹⁶⁸ M. COMPARTI, *Fatti illeciti: le responsabilità oggettive*, Giuffrè, 2009, p. 88.

¹⁶⁹ Cass. Civ., sez. III, sentenza n. 6756/2001.

Sul punto gli studiosi si dividono fra chi ritiene possibile una applicazione analogica dell'articolo 2049 c.c. e chi nega che ciò sia conciliabile con il nostro ordinamento. Segnatamente, i sostenitori della prima corrente¹⁷⁰ propongono l'applicazione analogica dell'art. 2049 c.c. laddove il danno sia stato cagionato da un sistema intelligente preposto allo svolgimento di mansioni connesse all'attività imprenditoriale; in tal caso sorgerebbe, appunto, la responsabilità dell'imprenditore.¹⁷¹ M. Costanza premette, a questo riguardo, che affinché possa discutersi di possibile applicazione della norma si deve escludere il caso in cui il robot sia semplicemente una macchina nelle mani del lavoratore umano, restringendosi il campo alle sole eventualità in cui il robot sia a tutti gli effetti un sostituto del lavoratore. Dal momento che si tratta di una ipotesi di responsabilità oggettiva risulta agevole imputare la responsabilità per le disfunzioni dei robot alle scelte operate dall'imprenditore. Si tratterebbe solo di mutare l'oggetto sul quale cade la scelta: non più il lavoratore, bensì il robot. I dubbi sorgono allorché si guardi all'elemento del fatto illecito, per il quale si richiede che vi sia colpa o intenzionalità nell'azione proveniente dall'uomo e l'allegazione di tali circostanze. Come osserva M. Costanza, invero, una volta superato il principio "nessuna responsabilità senza colpa" e ritenuto più congruo il criterio del rischio ai fini dell'imputazione della responsabilità, ecco che l'art. 2049 c.c. ben si potrebbe prestare ad una applicazione analogica nei casi qui descritti.¹⁷²

Di diverso avviso risulta essere invece la corrente dottrinale secondo la quale una simile applicazione dell'art. 2049 c.c. sarebbe da escludersi. Secondo U. Ruffolo la condotta illecita del commesso appare ricollegata al censurabile uso del suo "libero arbitrio"; e se è vero che ciò che caratterizza la responsabilità aquiliana oggi non è più l'elemento soggettivo dell'illecito, ma il danno ingiusto, è pur sempre vero anche che l'art. 2049 c.c. responsabilizza il committente per il compimento di un fatto illecito il

¹⁷⁰ M. COSTANZA, *Robot e impresa*, in U. RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, Milano, 2017, p. 112.

¹⁷¹ G. D'ALFONSO, *Intelligenza artificiale e responsabilità civile. Prospettive europee*, in *Revista de Estudios Jurídicos y Criminológicos*, ISSN-e: 2345-3456, 2022, p. 172.

¹⁷² M. COSTANZA, *Robot e impresa*, in U. RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, Milano, 2017, pp. 112-113.

cui elemento soggettivo è da ravvisarsi nella coscienza o volontà di una intelligenza tutta umana.¹⁷³ Per contro, i sistemi di IA, seppur “personificati”, non paiono in grado di porre in essere condotte colpose o dolose in senso stretto. Vi è poi un’ulteriore corrente dottrinale, soprattutto germanica, che in virtù di una determinata concezione di “personalità elettronica” e dell’illecito oggettivato riconnesso alla stessa qualifica gli agenti software come “commessi digitali”, giungendo a teorizzare l’invocabilità di una responsabilità vicaria omologa a quella dell’art. 2049 c.c.¹⁷⁴

Si può dunque concludere l’analisi delle ipotesi di responsabilità vicaria notando come sino a quando i sistemi di IA non saranno animati da una vera e propria coscienza sulla scorta della quale qualificarli come “persone” e non più come “cose”, l’applicazione analogica degli artt. 2047, 2048 e 2049 c.c. pare essere non agevole. Trattasi, infatti, di fattispecie “tarate sulla specificità della natura umana dell’essere (e dell’intelligenza) del cui illecito si risponde”.¹⁷⁵ Si esclude così sia una loro applicazione estensiva o sistematica al campo dei danni cagionati dai sistemi intelligenti, sia una loro applicazione analogica, in quanto a mancare sarebbe proprio l’*eadem ratio* su cui si fonda l’analogia giuridica.

2. L’applicabilità degli artt. 2050 e 2051 c.c.: il robot come prodotto

2.1 Le evoluzioni storiche della responsabilità da cose in custodia e da attività pericolosa, dal Code Napoleon al Codice civile del 1942

Qualora si qualifichi il sistema di IA come prodotto (pur con tutte le criticità di cui si è già fatta menzione nei capitoli precedenti), occorrerà volgere lo sguardo agli artt.

¹⁷³ U. RUFFOLO, *La responsabilità da algoritmo*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell’Intelligenza Artificiale*, G. Giappichelli Editore, 2020, p. 141.

¹⁷⁴ G. TEUBNER, *I soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, Napoli, 2019.

¹⁷⁵ U. RUFFOLO, *La responsabilità da algoritmo*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell’Intelligenza Artificiale*, G. Giappichelli Editore, 2020, p. 141.

2050, 2051 e, con particolare riferimento ai veicoli che incorporano sistemi intelligenti, 2054 c.c.

Per meglio comprendere il significato delle norme in esame conviene analizzarne le radici storiche e l'evoluzione nel corso del tempo partendo proprio dal *Code Napoleon*, matrice dei codici continentali. Grande spazio era riservato nel testo francese - accanto alla responsabilità soggettiva per negligenza, imprudenza e imperizia - alle ipotesi di responsabilità aquiliana derivata da errori correlati all'intelligenza umana o animale; in particolare, si dava rilievo alle ipotesi di responsabilità per "fatti altrui" commessi da persona dotata di minorate capacità intellettive e di responsabilità per danni cagionati da animali, quali beni intelligenti e, spesso, strumentali rispetto all'uomo. Il nostro art. 2052 c.c., che disciplina la responsabilità per danno cagionato da animali, costituisce traduzione letterale dell'allora art. 1385, confluito nell'attuale art. 1242. Invero, l'art. 2051 c.c. che oggi presenta nel nostro codice una formulazione speculare a quella dell'art. 2052 c.c., trova anch'esso origine nel *Code Napoleon*, ma rappresenta l'approdo di una attività interpretativa che prende le mosse dalla previsione della responsabilità da animale (cosa intelligente). Il *Code Napoleon*, difatti, prevedeva solo un breve e decisamente meno articolato inciso all'art. 1384, laddove, nel disciplinare la responsabilità per fatto proprio, e specificato che si è responsabili anche del "fatto" delle persone delle quali si risponde, accennava in modo conciso ad una responsabilità per fatto "*des choses que l'on a sous sa garde*". È solo attraverso un'attività interpretativa creativa che, partendo da quell'inciso, si giunge quindi ad adeguare l'ordinamento giuridico a una realtà produttiva nuova e di dimensioni crescenti. Si parte dal presupposto che l'azione della cosa sia distinta dall'attività del suo custode e che quest'ultimo risponda dei danni cagionati dalla cosa non più per *culpa in custodiendo*, bensì per qualsivoglia evento dannoso che sia conseguenza dell'azione della cosa. Si perviene, in questo modo, ad individuare una responsabilità per fatto delle cose "seagenti" attribuita parallelamente a quella per fatto dell'animale e si estende poi tale responsabilità anche alle cose che per loro natura non presentino la caratteristica suddetta, ma che siano potenzialmente dannose in relazione all'attività cui sono adibite. Si giunge così all'introduzione degli artt. 2050 e 2054 nel Codice

civile italiano, accanto naturalmente all'art. 2051 c.c., formulato nel Codice del 1942 in maniera simmetrica all'art. 2052 c.c.

La stessa formula, pertanto, viene utilizzata sia per disciplinare la responsabilità da cosa intelligente (l'animale), sia per disciplinare la responsabilità da cose non intelligenti.

La breve ricostruzione sin qui delineata mostra come si sia arrivati alle nuove responsabilità da rischio d'impresa attraverso un'intensa attività interpretativa che trova il suo fondamento nella responsabilità "da cosa", alla quale si affianca la responsabilità per l'utilizzo dell'intelligenza animale in funzione strumentale.

Ci si chiede, allora, se la medesima strategia possa condurre a individuare già nello stesso *corpus* normativo criteri di imputazione della responsabilità idonei a regolare anche quella derivante dall'attività dei sistemi di intelligenza artificiale.¹⁷⁶

2.2 La responsabilità ex art. 2050 c.c. e la sua cumulabilità con quella da prodotto difettoso

L'applicazione dell'art. 2050 c.c.¹⁷⁷ quale criterio di imputazione della responsabilità per i danni cagionati dai sistemi intelligenti si fonda sulla presunzione che il ricorso all'intelligenza artificiale sia suscettibile di rendere pericolose attività che non sarebbero tali in assenza dell'utilizzo di sistemi intelligenti. Gli esempi più citati, in tal senso, dalla letteratura giuridica sono quelli che riguardano la produzione di macchine ad elevata automazione così come la produzione di farmaci. Segnatamente con riferimento alla produzione di veicoli, osserva U. Ruffolo come sia ben possibile che si generino "pericolosità asimmetriche" dovute al fatto che l'intelligenza artificiale rende per un verso e in generale più sicuro il prodotto connotato da IA, andando però,

¹⁷⁶ L'analisi svolta è tratta da U. RUFFOLO, *Le responsabilità da produzione e gestione di intelligenza artificiale self-learning*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, G. Giappichelli Editore, 2020, pp. 134-137.

¹⁷⁷ Art. 2050 c.c.: "*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.*"

per altro verso, a creare nuovi pericoli in determinate situazioni circoscritte.¹⁷⁸ E indice di pericolosità diviene, ad esempio, la presenza del rischio di sviluppo, il quale come già visto costituisce limite esterno all'applicazione della disciplina della responsabilità per prodotto difettoso; così, qualora l'incidenza di tale rischio fosse significativa si potrebbe andare a qualificare l'attività di produzione di alcuni beni dotati di IA come pericolosa. E al tempo stesso, qualora l'evoluzione tecnologica corra più veloce del ciclo di vita del prodotto si darà il caso in cui sul mercato convivano prodotti più avanzati dal punto di vista della tecnica e prodotti tecnicamente superati e divenuti, di conseguenza, meno sicuri; anche in questo caso il rischio di sviluppo sarebbe indice di elevata pericolosità dell'attività di produzione. Anche avendo riguardo alla formulazione letterale della norma si può notare come il suddetto rischio possa giocare un ruolo fondamentale nell'applicazione dell'art. 2050 c.c.: il legislatore pone in capo all'esercente l'attività pericolosa i costi relativi all'adozione delle misure di sicurezza idonee a prevenire il danno, imponendogli, laddove non adottasse dette misure, di sostenere i costi per il risarcimento degli eventi dannosi in seguito verificatisi. Si noti, però, che l'idoneità ad evitare il danno delle misure adottate potrà essere valutata soltanto sulla base delle conoscenze tecniche del momento in cui si produce; se, da un lato, questo giudizio di idoneità *ex ante* esclude l'invocabilità a posteriori della responsabilità da prodotto difettoso, dall'altro il rischio che successivamente, alla luce delle nuove conoscenze della tecnica, quel prodotto risulti pericoloso e cagioni un danno sembra ammettere l'applicabilità dell'art. 2050 c.c., poiché qualifica l'attività produttiva come pericolosa.¹⁷⁹

¹⁷⁸ U. RUFFOLO, *Le responsabilità da produzione e gestione di intelligenza artificiale self-learning*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, G. Giappichelli Editore, 2020, p. 138. Così anche L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, 2018, p. 735 che afferma che anche l'attività di produzione di veicoli autonomi si può considerare pericolosa "in funzione dei nuovi pericoli di fallibilità del prodotto", consentendo quindi l'applicazione dell'art. 2050 c.c. e imputando in tal caso la responsabilità in capo allo sviluppatore dell'intelligenza artificiale.

¹⁷⁹ U. RUFFOLO, *Le responsabilità da produzione e gestione di intelligenza artificiale self-learning*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, G. Giappichelli Editore, 2020, pp. 138-139.

Proprio il rapporto fra la tutela offerta dall'art. 2050 c.c. e quella offerta dalla disciplina di *product liability* merita un breve approfondimento. All'interrogativo riguardante la cumulabilità delle due responsabilità gli studiosi rispondono dividendosi fra chi ritiene che siano concorrentemente invocabili e che esclude tale possibilità. In particolare, i fautori della non cumulabilità fondano la loro tesi sulla lettura della disciplina comunitaria quale *lex specialis* che introduce vincoli di disciplina uniforme; ciò precluderebbe agli Stati membri di introdurre o applicare nei confronti della vittima del danno una disciplina diversa e più favorevole. Secondo U. Ruffolo si tratterebbe di una erronea interpretazione della disciplina comunitaria che genererebbe un falso problema dovuto alla mancata distinzione fra la *ratio* della normativa specifica in materia di responsabilità da prodotto difettoso e quella delle generali previsioni che individuano i criteri di imputazione della responsabilità extracontrattuale. La stessa Corte di Giustizia ha affermato che sia cumulabile la disciplina di *product liability* con “*i regimi di responsabilità contrattuale o extracontrattuale che si basano su elementi diversi, come la garanzia dei vizi occulti o la colpa*”.¹⁸⁰ Sulla scorta di quanto dichiarato dalla Corte si può allora ribadire che, nel settore di cui si discute, il campo di applicazione dell'art. 2050 c.c. non coinciderebbe totalmente con quello della responsabilità da prodotto difettoso, dal momento che andrebbe a disciplinare la responsabilità per danni cagionati da prodotti che presentino una potenzialità lesiva, seppur privi di difetti. Come si è già precedentemente avuto modo di chiarire, infatti, non necessariamente il concetto di “prodotto pericoloso” coincide con quello di “prodotto difettoso” e viceversa. Risulta differente anche la prova liberatoria gravante sul convenuto: ai sensi dell'art. 2050 c.c. l'aver adottato tutte le misure idonee ad evitare il danno; ai sensi dell'art. 118 cod. cons., una serie di ipotesi che dimostrano, in generale, che il difetto non sia causalmente imputabile al produttore. A ben vedere, inoltre, la non cumulabilità delle due tutele porterebbe anche ad accordare in alcuni casi al consumatore - notoriamente soggetto debole - una minore protezione rispetto a quella accordata al professionista, il primo potendo invocare solo

¹⁸⁰ Corte di Giustizia, sentenza del 21 dicembre 2011, C-495/10.

l'applicazione della disciplina di *product liability*, la quale offre una tutela evidentemente minore rispetto a quella di cui all'art. 2050 c.c., invocabile invece dal secondo in occasione di un evento dannoso lesivo di un bene strumentale.

In virtù di questo ragionamento si giunge pertanto ad ammettere che il soggetto leso da un evento plurioffensivo possa invocare alternativamente o cumulativamente sia la responsabilità per prodotto difettoso sia quella da attività pericolose.¹⁸¹

Un'ultima specifica pare opportuna segnatamente con riferimento al concetto di pericolosità. Vi è chi, fra gli studiosi, pur ammettendo l'applicabilità in via interpretativa della responsabilità di cui all'art. 2050 c.c. e la sua cumulabilità con quella di *product liability*, non condivide la soluzione per cui l'impiego di intelligenza artificiale rappresenta un'attività intrinsecamente pericolosa. Sarebbe, invece, più sicura dell'attività svolta dall'uomo, in quanto costituente spesso e volentieri uno strumento di correzione o integrazione delle imprecisioni umane.¹⁸² La pericolosità potrebbe invero riferirsi alle interazioni dei sistemi intelligenti con il mondo esterno, trasformando così in pericolosa un'attività fino a quel momento non considerata tale.

2.3 Il regime di cui all'art. 2051 c.c. e la qualificazione giuridica della responsabilità da cose in custodia

L'art. 2051 c.c.¹⁸³ disciplina la responsabilità del custode per i danni provocati dalla cosa oggetto della custodia e rappresenta la norma nella quale la letteratura giuridica ha identificato la possibilità di applicazione forse più calzante al caso dei danni provati dai sistemi intelligenti.

Affinché sorga la responsabilità del custode occorre che siano soddisfatte le seguenti condizioni: i) che sussista una relazione di custodia tra la cosa che cagiona il danno e

¹⁸¹ U. RUFFOLO, *Le responsabilità da produzione e gestione di intelligenza artificiale self-learning*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, G. Giappichelli Editore, 2020, pp. 139-140.

¹⁸² M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giurisprudenza italiana*, 2019, p. 1688.

¹⁸³ Art. 2051 c.c.: "Ciascuno è responsabile del danno cagionato dalle cose che ha in custodia, salvo che provi il caso fortuito".

il soggetto che si pretende responsabile per tale danno; ii) che la cosa oggetto della custodia sia causa diretta del danno; iii) che vi sia un nesso di causalità fra la cosa e l'evento dannoso.

Per quanto concerne la prima condizione si ritiene che la relazione di custodia, ossia il rapporto qualificato con la *res*, si realizzi attraverso l'esercizio di un "potere di governo" che il custode esercita sulla cosa al fine di controllarla e di evitare o quantomeno ridurre il possibile insorgere di situazioni pericolose.¹⁸⁴ Le classiche categorie del diritto di proprietà non esauriscono le ipotesi di custodia rilevanti ai fini dell'applicazione dell'art. 2051 c.c., dal momento che ciò che conta è la disponibilità di fatto e giuridica della cosa, a prescindere da qualsiasi utilità che dalla stessa si tragga; così potranno essere qualificati come custode non solo il proprietario, il possessore o il detentore, ma anche l'usufruttuario, il conduttore e il titolare di un diritto di godimento sul bene altrui.¹⁸⁵

Il secondo presupposto per l'insorgere della responsabilità consiste nell'idoneità della *res* a cagionare un danno, idoneità intrinseca o sviluppata successivamente a causa delle condizioni in cui la cosa viene a trovarsi.¹⁸⁶ Non si richiede, invece, una sua pericolosità connaturata, a differenza di quanto visto per l'art. 2050 c.c.

Si noti che la fattispecie in esame non riguarda il caso in cui la cosa produca un danno quando utilizzata come strumento dell'agire di una persona; in quel caso sarà applicabile l'art. 2043 c.c. A norma dell'art. 2051 c.c., invece, si richiede che la cosa abbia, di fatto, "un ruolo attivo nella produzione dell'evento".¹⁸⁷

Per quanto riguarda l'onere probatorio, sarà il danneggiato a dover fornire la prova del rapporto di custodia e del nesso di causalità fra la cosa oggetto della custodia e l'evento

¹⁸⁴ M. COZZI, *La responsabilità civile per danno da cose (diritto italiano e francese)*, Padova, 1935, p.333.

¹⁸⁵ G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e "responsabilità da algoritmo"*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 84.

¹⁸⁶ C. DAINI, *La responsabilità da cose in custodia*, in *Danno e responsabilità*, 2019, p. 193.

¹⁸⁷ L. CORSARO, voce "Responsabilità da cose", in *Dig.disc.priv.*, sez. civ., XVII, Torino, 1998, p. 105.

dannoso, mentre per liberarsi il convenuto sarà tenuto a provare l'esistenza del "caso fortuito", quale elemento idoneo ad interrompere la relazione causale.¹⁸⁸

Largamente dibattuta è stata poi la questione relativa alla qualificazione giuridica della responsabilità da cose in custodia: la letteratura giuridica ha elaborato due principali ricostruzioni a riguardo, le quali sono state accolte con orientamenti oscillanti dalla Corte di legittimità.¹⁸⁹

La dottrina maggioritaria ha qualificato la responsabilità da cose in custodia come responsabilità oggettiva, individuando la *ratio* dell'art. 2051 c.c. nell'obiettivo di responsabilizzare il soggetto che si trovi in una posizione che gli consenta di gestire i rischi connessi alla res; viene puntualizzato, a tal proposito, che la funzione della responsabilità oggettiva è quella di imputare a chiunque il "rischio oggettivamente creato" dalla propria attività.¹⁹⁰ Anche la giurisprudenza maggioritaria pare aver riconosciuto già da tempo la natura oggettiva della responsabilità da cose in custodia.

¹⁹¹ Alla luce di questa impostazione, il "caso fortuito" di cui all'art. 2051 c.c. assume il significato di eccezione alla normale sequenza causale, un fattore in astratto ed *ex ante* imprevedibile che comporta l'inevitabilità dell'evento.¹⁹²

Se la tesi della responsabilità oggettiva è quella sposata dalla dottrina prevalente e dalla giurisprudenza più recente, non bisogna dimenticare tuttavia che l'insegnamento giurisprudenziale più risalente ha qualificato la responsabilità da cose in custodia come responsabilità aggravata. Come già osservato a proposito di alcune delle ipotesi di responsabilità vicaria, si tratta di una responsabilità che si fonda sulla colpa, ma per la quale si prevede un'inversione dell'onere della prova liberatoria, posto a carico del convenuto (in questo caso il custode). Si presume, dunque, che il custode sia colpevole

¹⁸⁸ Cass.civ., sez. III, ord., 1° febbraio 2018, n. 2477, in *Giustizia civile*, 2018.

¹⁸⁹ G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e "responsabilità da algoritmo"*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 87.

¹⁹⁰ P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 193 ss.

¹⁹¹ Cass.civ., sez.un., 11 novembre 1991, n. 12019; Cass.civ., sez. III, 20 maggio 1998, n. 5031.

¹⁹² D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e "responsabilità da algoritmo"*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 88.

fin tanto che non provi di non essere “in colpa”, superando così la presunzione *iuris tantum*. La prova del caso fortuito acquisisce, in base a tale ricostruzione, una valenza soggettiva e consiste nel dimostrare sia di aver tenuto un comportamento diligente, sia che sia intervenuto un fattore idoneo a causare o a concorrere a cagionare il danno.¹⁹³ Si segnala che, sebbene l’orientamento della responsabilità aggravata sia stato superato da quello della responsabilità oggettiva, la giurisprudenza si mostra tutt’ora altalenante nell’inquadramento della responsabilità di cui all’art. 2051 c.c.

2.4 L’art. 2051 c.c. e l’intelligenza artificiale

L’art. 2051 c.c. così interpretato pare potersi adattare meglio di altre fattispecie al caso dei danni cagionati dai sistemi di IA. Come ricordato precedentemente, la storia della sua nascita dimostra come si sia partiti dalla responsabilità “per fatto” dell’animale per poi giungere a quella da cose in custodia, e non viceversa. Di qui la definizione di “norma fotocopia” utilizzata da U. Ruffolo¹⁹⁴ per descrivere il peculiare rapporto fra l’art. 2051 c.c. e l’art. 2052 c.c., concernente la responsabilità per i danni cagionati da animali. Entrambe le ipotesi, dunque, individuano nella custodia il criterio di imputazione della responsabilità e nel caso fortuito il limite della stessa. La stretta relazione sussistente tra le due norme ha spinto parte della dottrina¹⁹⁵ a ritenere che l’interprete possa scegliere se applicare l’una o l’altra a seconda di come configuri il sistema di IA: se entità dinamica ed evolutiva come un animale, l’art. 2052 c.c.; se, in una logica naturalistica, come cosa in senso proprio, l’art. 2051 c.c.¹⁹⁶

¹⁹³ D’ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e “responsabilità da algoritmo”*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 90.

¹⁹⁴ U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giur.it.*, 2019, p. 1699.

¹⁹⁵ A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *La Nuova Giurisprudenza Commentata*, 2012, p. 495; U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giur.it.*, 2019, p. 1699; L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, 2018, p. 734.

¹⁹⁶ D’ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e “responsabilità da algoritmo”*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 105.

Vi è, tuttavia, altra parte della dottrina¹⁹⁷ che respinge il richiamo all'art. 2052 c.c., ritenendo che pur essendo l'imprevedibilità della condotta caratteristica che contraddistingue tanto l'animale quanto il dispositivo intelligente, nel primo caso il proprietario abbia comunque la possibilità di esercitare un controllo su tale condotta attraverso l'addomesticamento dell'animale, mentre nel secondo caso il titolare, l'utilizzatore o il custode della cosa non possa in alcun modo incidere sulla condotta della stessa.¹⁹⁸

Sono poi state presentate alcune critiche alla possibilità di applicare l'art. 2051 c.c. al fenomeno di cui si discute. In particolare, si è affermato che: i) mentre la cosa oggetto della custodia ai sensi dell'art. 2051 c.c. sarebbe "inanimata", il dispositivo intelligente è capace di decisioni autonome e di agire senza necessità di controllo da parte dell'uomo;¹⁹⁹ ii) il parametro della custodia risulterebbe inidoneo, dal momento che sarebbe particolarmente complicato per il custode controllare il dispositivo intelligente, soprattutto qualora quest'ultimo godesse di elevata autonomia; iii) la prova liberatoria del caso fortuito che riguarda l'imprevedibilità del comportamento della macchina potrebbe rivelarsi molto complicata, stante l'insondabilità del comportamento del sistema di IA.²⁰⁰

A fronte dei rilievi critici appena esposti, si evidenziano tuttavia una serie di ragioni alla luce delle quali l'applicazione dell'art. 2051 c.c. parrebbe opportuna, come, ad esempio, il fatto che la norma richiede che la cosa oggetto della custodia sia fonte essa stessa di danno e non mero strumento dell'agire del custode; ovvero il fatto che tale

¹⁹⁷ F. NADDEO, *Intelligenza artificiale: profili di responsabilità*, in *Comparazione e diritto civile*, 2020, p. 1158; M. SCIALDONE, *Il diritto dei robot: la regolamentazione giuridica dei comportamenti non umani*, in E. PIETRAFESA, F. MARZANO, T. MEDICI (a cura di), *La rete e il fattore C: Cultura, Complessità, Collaborazione*, Volume II, Roma, Stati Generali dell'Innovazione, 2016, p. 79.

¹⁹⁸ D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e "responsabilità da algoritmo"*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, pp. 105-106.

¹⁹⁹ M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giurisprudenza italiana*, 2019, p. 1687; G SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Dir.Inf.*, 2003, pp. 55 ss.

²⁰⁰ L. FORT, V. IEVA, *Intelligenza artificiale, responsabilità civile e interpretazione analogica*, in www.biodiritto.org, 2020, p. 15.

norma disciplinerebbe una fattispecie complementare rispetto a quella di cui all'art. 2050 c.c. A questo riguardo vi è anche chi prospetta la facoltà per il danneggiato di proporre il “concorso” fra gli artt. 2050 e 2051 c.c., lasciando poi al giudice la decisione circa la qualificazione della fattispecie avuto riguardo al caso concreto.²⁰¹ È necessario poi distinguere fra sistema chiuso e sistema aperto. Nel primo caso l'applicazione dell'art. 2051 c.c. sarà preclusa, poiché il titolare, utilizzatore o custode del dispositivo di IA non esercita alcun controllo sui rischi connessi al sistema; in tale situazione si potrebbe pensare ad un aggravamento della responsabilità in capo al produttore del dispositivo, essendo quest'ultimo il soggetto che si trova nella posizione di poter minimizzare i rischi. Nel secondo caso, al contrario, il titolare, l'utilizzatore o il custode si trovano nella condizione di poter controllare e modificare i rischi connessi al dispositivo; di conseguenza, l'applicazione della norma è considerata idonea a disciplinare la fattispecie concreta.²⁰²

2.4.1 Le figure del produttore e del trainer: quale responsabilità?

Un'ultima puntualizzazione va fatta, infine, relativamente ai soggetti diversi dal titolare/utilizzatore/custode ai quali si possa imputare la responsabilità da cose in custodia per i danni cagionati dai dispositivi intelligenti. La dottrina ha individuato nel *trainer* che addestra il sistema di IA la persona in capo alla quale potrebbe gravare una responsabilità a norma dell'art. 2051 c.c., giustificando tale possibilità con l'assunto che si tratta del soggetto incaricato di utilizzare o gestire la “cosa” intelligente e di indirizzarla verso una *mentalità*, potenzialmente in grado di sfociare in condotte lesive, senza prevedere meccanismi capaci di limitare tali condotte.²⁰³

In questo caso la responsabilità dell'addestratore si presenterebbe come concorrente rispetto a quella del gestore o del custode. La responsabilità del produttore e dell'autore

²⁰¹ A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, in A. PROCIDA MIRABELLI DI LAURO, M. FEOLA (a cura di), *Diritto delle obbligazioni*, Napoli, 2020, p. 520.

²⁰² D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e “responsabilità da algoritmo”*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 107.

²⁰³ D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizioni e “responsabilità da algoritmo”*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 107.

dell'algoritmo di autoapprendimento, invece, sarebbero meglio normate attraverso il ricorso alla disciplina di *product liability*, nonché dell'art. 2050 c.c. (qualora si dimostrasse la presenza del requisito della pericolosità), ovvero dell'art. 2051 c.c., laddove invocabile.²⁰⁴

3. L'art. 2054 c.c. e il futuro della r.c.a.

3.1 La disciplina dell'art. 2054 c.c.

L'art. 2054 c.c.²⁰⁵ disciplina la responsabilità per i danni cagionati dalla circolazione di veicoli e individua una figura di illecito connotata dal carattere della specialità, introdotta dal legislatore del 1942 per sottrarre la regolamentazione di tali danni ai criteri generali di imputazione della responsabilità di cui all'art. 2043 c.c.; l'obiettivo era quello di predisporre una regolamentazione più severa per poter accordare ai terzi danneggiati dal fenomeno della circolazione stradale una tutela più incisiva.

Per comprendere come il mutato panorama tecnologico possa condizionare l'assetto giuridico che il legislatore ha tradizionalmente predisposto, va sottolineato che il criterio di imputazione della responsabilità per questa fattispecie di danni si è fondato, fino a questo momento, sul tradizionale fattore di rischio che la circolazione dei veicoli introduce, costituito dalla fallibilità della condotta umana.²⁰⁶ Fin dal principio,

²⁰⁴ U. RUFFOLO, *Le responsabilità da produzione e gestione di intelligenza artificiale self-learning*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, G. Giappichelli Editore, 2020, pp. 140-141.

²⁰⁵ Art. 2054 c.c.: *“Il conducente di un veicolo senza guida di rotaie è obbligato a risarcire il danno prodotto a persone o a cose dalla circolazione del veicolo, se non prova di aver fatto tutto il possibile per evitare il danno.*

Nel caso di scontro tra veicoli si presume, fino a prova contraria, che ciascuno dei conducenti abbia concorso ugualmente a produrre il danno subito dai singoli veicoli.

Il proprietario del veicolo, o, in sua vece, l'usufruttuario o l'acquirente con patto di riservato dominio, è responsabile in solido col conducente, se non prova che la circolazione del veicolo è avvenuta contro la sua volontà.

In ogni caso le persone indicate dai commi precedenti sono responsabili dei danni derivati da vizi di costruzione o da difetto di manutenzione del veicolo.”

²⁰⁶ G. CALABRESI, A. AL MUREDEN, *Driverless cars, Intelligenza artificiale e futuro della mobilità*, Il Mulino, 2021, p. 12.

pertanto, si è individuato nel conducente il soggetto responsabile per i danni cagionati dalla circolazione dei veicoli e nella colpa il criterio di imputazione di tale responsabilità (art. 2054 c.c. comma 1). Non solo, si sono previsti ulteriori meccanismi di allocazione del costo dei danni che fungono da contrappeso alla responsabilità del conducente e che forniscono una garanzia ulteriore, rispetto al solo patrimonio di quest'ultimo, per il soggetto leso; così, il terzo e il quarto comma dell'art. 2054 c.c. prevedono, rispettivamente, la responsabilità solidale del proprietario del veicolo tanto per la condotta colposa del conducente, quanto per eventuali vizi di costruzione o difetti di manutenzione del veicolo. Questa decisione si spiega anche tenendo conto del fatto che all'epoca l'automobile era considerata ancora un bene di lusso, riservato a chi avesse le risorse economiche per potersi permettere il suo acquisto e il suo mantenimento; il proprietario, allora, era ritenuto soggetto più solvibile rispetto al conducente dell'automobile.²⁰⁷ La successiva diffusione esponenziale dell'automobile dovuta a una maggiore accessibilità dal punto di vista economico non solo aumentava il numero degli incidenti e la necessità di garantire alle vittime un risarcimento, ma rendeva meno efficace dal punto di vista della tutela la soluzione normativa per cui era il proprietario il soggetto sicuramente in grado di assicurare il risarcimento. È questo lo scenario socioeconomico che rappresenta la *ratio* dell'introduzione dell'assicurazione obbligatoria ad opera della legge 24 dicembre 1969, n. 990, attraverso la quale si proseguiva il processo di così detta socializzazione della responsabilità civile automobilista (r.c.a.).²⁰⁸

La prima osservazione che può farsi circa la disciplina dell'art. 2054 c.c. è, perciò, che all'aumentare del livello di rischio dato dalla circolazione dei veicoli si realizza un'espansione di quel processo di socializzazione dei costi dovuti alla verifica degli incidenti che ha la finalità sia di distribuire tali costi tra più soggetti (diversi dai danneggiati), sia di meglio tutelare questi ultimi garantendogli la possibilità di

²⁰⁷ S. POLLASTRELLI, *Circolazione di veicoli*, in P. SCHLESINGER (diretto da), *Il Codice civile. Commentario*, Milano, 2022, p. 179.

²⁰⁸ E. AL MUREDEN, *Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo*, in *Contratto e impresa*, 2019, pp. 896-897.

accedere allo strumento assicurativo. Ci si chiede, quindi, come il mutare del rischio dovuto all'avvento dei veicoli a guida autonoma possa incidere sul processo di socializzazione del costo dei danni a cui si è appena accennato.²⁰⁹

3.1.1 Le nozioni di “circolazione”, “veicolo” e “conducente”

Si noti come sussista una stretta relazione tra la disciplina privatistica in esame e la normativa pubblicistica, data dal fatto che le nozioni che fondano i presupposti applicativi dell'art. 2054 c.c. non trovano una compiuta descrizione all'interno della norma e vanno quindi riempite di contenuto alla luce della normativa contenuta nel codice della strada. Sono quindi i concetti di “circolazione”, “veicolo” e “conducente”, così come descritti dal codice della strada, a perimetrare il campo di applicazione della norma in esame.²¹⁰

Il primo presupposto applicativo è che il danno sia cagionato “dal veicolo in circolazione”. Dottrina e giurisprudenza hanno fornito una definizione di “circolazione” particolarmente ampia, tale da ricomprendere non solo la fase in cui il veicolo è in movimento, ma anche quella dell'arresto e della sosta, purché si trovi in una zona adibita alla pubblica viabilità. A ben vedere, dunque, il concetto di “circolazione” non ostacolerebbe l'applicazione delle norme al caso dei danni cagionati da veicoli a guida autonoma, ricomprendendo anche i casi in cui il conducente non è propriamente alla guida del mezzo.

Per “veicolo” si intendono, ai sensi del codice della strada, le macchine di qualsiasi specie, che circolano sulle strade “guidate dall'uomo” (art. 46 cds). Affiora in questo caso una nozione di veicolo che difficilmente si concilia con le *driverless car*, in particolare con i livelli di automazione più elevati (livello 4 e 5). E lo stesso vale per la nozione di conducente di cui al comma 1 dell'art. 2054 c.c., che contrasta nettamente con il significato stesso del termine “*driverless car*”, letteralmente “auto senza

²⁰⁹T. DE MARI CASARETO DAL VERME, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma*, in *BioLaw Journal – Rivista di BioDiritto*, n.3/2023.

²¹⁰T. DE MARI CASARETO DAL VERME, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma*, in *BioLaw Journal – Rivista di BioDiritto*, n.3/2023.

conducente”. Se la lettura della disciplina dell’art. 2054 c.c. alla luce della normativa pubblicistica ci rimanda un quadro che poco si conforma ai nuovi scenari, è altrettanto vero che la norma in esame mostra una certa flessibilità che permette a dottrina e giurisprudenza di specificare il contenuto di quei concetti al variare della normativa *ex ante* (la quale dovrebbe a sua volta riflettere le caratteristiche della tecnologia esistente).²¹¹

3.1.2 I criteri di imputazione della responsabilità

Escluso l’ultimo comma dell’art. 2054 c.c. che costituisce una fattispecie autonoma, la condotta del conducente risulta essere centrale nella disciplina della norma ed è per questo che, secondo l’opinione dominante in dottrina, l’imputazione della responsabilità in capo a tale soggetto si fonda sul criterio della colpa. Pertanto, mentre il danneggiato dovrà dimostrare il nesso di causalità fra la circolazione del veicolo e il danno, il conducente potrà liberarsi provando l’assenza di colpa.²¹² Si ritiene che lo stesso accada nel caso di scontro fra due veicoli di cui al comma 2, laddove la colpa dei conducenti giustifica la distribuzione tra gli stessi dei costi del danno. E tale criterio si ravvisa anche nel comma 3, dal momento che la responsabilità solidale del proprietario è una responsabilità vicaria, che presuppone quindi la sussistenza della colpa del conducente. Trattasi pertanto in tutti questi casi di responsabilità fondata sulla colpa.²¹³ Ciò che cambia, invero, pare essere il livello di diligenza che viene richiesto al conducente. La giurisprudenza individua uno *standard* molto più elevato per il conducente che cagiona un danno al pedone, rispetto al conducente che si scontra con altri veicoli. Si potrebbe allora affermare che nei casi di cui al comma 1 si impone al conducente un dovere di prevenzione unilaterale, tale da far sorgere una responsabilità quasi-oggettiva in caso di violazione di detto dovere; così quest’ultimo

²¹¹ T. DE MARI CASARETO DAL VERME, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma*, in *BioLaw Journal – Rivista di BioDiritto*, n.3/2023.

²¹² C. SALVI, *La responsabilità civile*, Giuffrè Francis Lefebvre, 2019, p.216.

²¹³ T. DE MARI CASARETO DAL VERME, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma*, in *BioLaw Journal – Rivista di BioDiritto*, n.3/2023.

è tenuto a prevedere anche una condotta particolarmente imprudente dei pedoni. Per quanto concerne il comma 2, invece, lo standard di diligenza si affievolisce e la presunzione di colpa non grava interamente su un conducente, come nel comma 1, ma su entrambi in egual misura.

Il comma 4, come già anticipato, costituisce una fattispecie autonoma rispetto alle precedenti e individua una responsabilità solidale (non vicaria) del conducente e del proprietario nel caso di danno causato da un vizio di costruzione o da un difetto di manutenzione del veicolo. Secondo l'opinione prevalente, la responsabilità, in questo caso, ha natura oggettiva.²¹⁴

3.2 Livelli di automazione e applicazione dell'art. 2054 c.c.

Sulla scorta di quanto sinora detto, ci si chiede allora se sarà ancora possibile fare ricorso all'applicazione dell'art. 2054 c.c. al fine di disciplinare i danni cagionati dai veicoli autonomi. È bene specificare, a questo proposito, che quando si parla di veicoli distinti da quelli "tradizionali", non si allude ad una categoria unitaria, bensì a diverse categorie corrispondenti ad altrettanti livelli di automazione. In particolare, se con il livello 0 si individua l'assenza totale di automazione, con i livelli 1 e 2 ci si riferisce ai veicoli dotati dei così detti ADAS (*Advanced Driver Assistance Service*), mentre ai livelli dal 3 al 5 corrispondono i sistemi così detti ADS (*Automated Driving System*). Rilevano dunque, in questo caso, gli ultimi tre livelli. In particolare, il livello 3 corrisponde ad una automazione parziale, in cui il conducente umano svolge ancora un ruolo attivo; risulta dunque agevole un'applicazione dell'art. 2054 c.c. così come formulato ora, dal momento che la fonte del rischio del danno sta ancora nella fallibilità umana.

²¹⁴ C. CASTRONOVO, *La nuova responsabilità civile*, Milano, 2006, pp. 438 ss., il quale osserva che l'introduzione nel Codice del consumo della disciplina di product liability che individua nel produttore il soggetto responsabile in caso di prodotto difettoso, rende forse anacronistica la previsione di responsabilità in capo a conducente e proprietario, non essendo questi ultimi i soggetti in grado di gestire il rischio relativo ai difetti di progettazione e costruzione.

Il livello 4, pur comprendendo già i veicoli ad alta automazione, prevede che vi sia ancora un soggetto tenuto alla supervisione della macchina autonoma, il quale tuttavia non svolge un ruolo preponderante nella circolazione della stessa; gli viene richiesto di intervenire solo in particolari situazioni di emergenza. Se si guarda alla definizione di conducente elaborata dalla giurisprudenza, pare potersi ricomprendere anche il soggetto adibito alla supervisione nei veicoli del livello in esame; mentre, avuto riguardo dei criteri di imputazione della responsabilità, solo il primo e il terzo comma sembrano applicabili, data la severità con cui il criterio della colpa è stato interpretato. Si dubita, invero, che arrivati a questo livello di automazione sia ancora opportuno parlare di dover di prevenzione unilaterale in capo al conducente, posto che quest'ultimo potrebbe non essere più nella condizione di prevenire o ridurre il rischio dell'evento lesivo; e altrettanto incerto è che la causa del rischio di verificazione del danno continui ad essere la fallibilità umana.

Gli stessi rilievi critici valgono, a maggior ragione, quando si arrivi al livello massimo di automazione.

Se queste considerazioni valgono a proposito dei primi tre commi dell'art. 2054 c.c., non va però dimenticato che il criterio oggettivo di imputazione della responsabilità di cui all'ultimo comma ben si concilia anche con i più alti livelli di automazione; orbene, la sua operatività rimane comunque limitata ai casi in cui il danno è cagionato da vizi di costruzione o difetti di manutenzione.

Si può quindi prevedere che, quando in futuro si arriverà all'ingresso nel mercato di veicoli a guida autonoma corrispondenti ai livelli di autonomia più alti, vi sarà un corrispondente spostamento del *focus* della responsabilità dal conducente al produttore del veicolo, non rispondendo l'attuale formulazione dei primi tre commi dell'art. 2054 c.c. alle esigenze di disciplina dei danni cagionati dalle *driverless car*.²¹⁵

²¹⁵ L'intero paragrafo è tratto da T. DE MARI CASARETO DAL VERME, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma*, in *BioLaw Journal – Rivista di BioDiritto*, n.3/2023.

Conclusioni

Arrivati al termine di questo percorso, vale la pena di rivedere brevemente i punti fondamentali del lavoro sino a qui svolto, al fine di riordinare le idee e restituire un quadro d'insieme dal quale sia più agevole trarre delle conclusioni.

In primis, si è cercato di inquadrare il problema del così detto “*responsibility gap*” e di valorizzare il collegamento che sussiste fra questo e alcune delle caratteristiche che qualificano le più avanzate applicazioni di intelligenza artificiale, cioè quelle che fondano il proprio metodo di apprendimento sul meccanismo del *machine learning*. All'opacità e alla complessità tecnologica che caratterizza tali tecnologie, consegue, per ciò che in questa sede interessa, la difficoltà di risalire alla ragione che ha portato la macchina a comportarsi in quel modo e, di conseguenza, anche alla causa del danno, la quale rischia di rimanere ignota. Tali considerazioni portano quindi a ritenere che il criterio di imputazione della responsabilità, in questi casi, dovrebbe essere oggettivo, di modo tale che sia identificabile a priori il soggetto ritenuto responsabile del danno cagionato dai sistemi di IA; ancora, la responsabilità oggettiva (e questo, forse, il punto più importante) permette al danneggiato di non essere gravato dall'onere di provare la colpa del danneggiante, il quale sarà tenuto a risarcire il danno a prescindere dal fatto che la sua condotta rispondesse o meno ai canoni della diligenza. Se questo è vero, pare allora opportuna l'applicazione, in simili casi, della Direttiva 85/374/CEE in materia di responsabilità da prodotto difettoso, secondo la quale la responsabilità per il danno cagionato dal prodotto difettoso è da imputarsi al produttore sulla base di un criterio oggettivo. Fermo restando che l'analisi delle esimenti mostra come, nella maggior parte dei casi, il produttore si liberi dimostrando la propria diligenza, si è tuttavia osservato come, in particolare la nozione di prodotto, la nozione di difetto e la necessità per il danneggiato di provare il nesso di causalità tra il difetto e il danno risultino poco aderenti alla realtà dei sistemi intelligenti, richiedendo sul punto un intervento del legislatore. La proposta di una nuova direttiva in materia di responsabilità da prodotto difettoso non ha tardato ad arrivare, anche se per il momento si tratta ancora, appunto, solo di una proposta.

Si è volto poi lo sguardo al nuovo Regolamento sull'intelligenza artificiale, destinato a influire profondamente nel campo dell'IA, anche se probabilmente non altrettanto incisivo per quanto riguarda la necessità di regolamentazione della responsabilità extracontrattuale per i danni di cui trattasi. Come si è osservato, l'approccio seguito dall'Unione europea ricalca quello adottato in tema di protezione dei dati personali, discostandosene, invero, in alcuni tratti fondamentali. Ciò che più interessa di simile approccio è la volontà del legislatore europeo di porre l'accento sulla fase anteriore all'immissione nel mercato del sistema intelligente, prevenendo una serie di adempimenti che variano a seconda della pericolosità del sistema; il legislatore individua a monte diverse categorie di sistemi distinte sulla base del rischio che possano cagionare un danno. L'obiettivo perseguito è chiaramente quello di minimizzare il rischio attraverso le prescrizioni di obblighi il cui inadempimento porta all'applicazione di sanzioni amministrative.

Se ne deduce che, preso atto del fatto che per alcuni sistemi di IA vi è un ineliminabile rischio che l'agire del sistema cagioni un danno, il legislatore ritiene opportuno intervenire a monte delineando un sistema di *accountability* (o principio di responsabilità) che dovrebbe avere l'effetto di ridurre l'incidenza dei danni.

Se dovessimo tracciare un collegamento fra quanto detto precedentemente con riferimento alla responsabilità oggettiva e l'approccio *risk-based* scelto dal legislatore si potrebbe giungere alla conclusione che si tratti di due impostazioni che non si escludono a vicenda, ma che anzi costituiscono due momenti diversi di uno stesso percorso volto a disciplinare il fenomeno dei danni cagionati dai sistemi di IA. Da un lato è possibile incidere sul numero dei danni cercando di minimizzare il rischio della loro verifica (come cerca di fare l'*AI Act*); dall'altro, qualora il danno ciononostante si verifichi, la responsabilità andrà imputata al soggetto tenuto alla gestione del rischio. Va sottolineato, tuttavia, che il Regolamento sull'intelligenza artificiale è deficitario in questi termini, non prevedendo alcun diritto al risarcimento in favore del soggetto leso. Come ipotizzato da parte della dottrina, allora, si potrebbe pensare ad un ulteriore provvedimento europeo che si proponga di disciplinare proprio questa seconda fase dedicata al ristoro dei soggetti danneggiati. Volendo fare un

parallelo con il prodotto tradizionalmente inteso, si pensi alla normativa in materia di sicurezza generale dei prodotti (Direttiva 2001/95/CE), che detta una disciplina che si colloca a monte del processo produttivo e il cui destinatario è il produttore; e poi si pensi alla già citata Direttiva 85/374/CEE, dedicata alla regolamentazione dei danni cagionati da prodotti difettosi, che riconosce al danneggiato il diritto di agire per ottenere il risarcimento del danno.

Lo stesso schema si potrebbe adottare per i nuovi “prodotti” tecnologici.

Tornando alla descrizione del percorso qui intrapreso, ci si è chiesti infine se vi fosse la possibilità per il diritto interno di risolvere efficacemente la questione oggetto di disamina. Le fattispecie ritenute più idonee a tal fine sono risultate essere quelle di cui all’art. 2050 e 2051 c.c., le quali a ben vedere offrono maggior protezione al soggetto leso della concorrente disciplina contenuta nella Direttiva *Product Liability*.

La proposta potrebbe allora essere quella di predisporre una normativa europea che sia in grado di armonizzare le regole applicabili dagli Stati membri e che preveda una tutela minima per il danneggiato, il quale sia poi messo nelle condizioni di agire a norma di regole di diritto interno più favorevoli.

Si tenga presente, tuttavia, che attualmente le uniche opzioni a disposizione del danneggiato sono rappresentate dall’applicazione delle norme del Codice civile sopra menzionate, qualora la fattispecie concreta sia sussumibile nella fattispecie astratta, e dall’applicazione delle norme del Codice del consumo nelle quali è confluita la disciplina di *Product Liability*, con tutti i limiti che ne derivano. E si presume che anche con l’entrata in vigore dell’*AI Act* la situazione rimanga immutata.

Si auspica, perciò, un ulteriore intervento del legislatore europeo incentrato sulla creazione di una disciplina *ad hoc* che sia in grado di allocare efficacemente la responsabilità aquiliana.

Bibliografia

ALAIMO A., *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in *federalistmi.it* - ISSN 1826-3534, n. 25/2023, p. 138.

AL MUREDEN A., *Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo*, in *Contratto e impresa*, 2019, pp. 896-897.

ALPA G., *Responsabilità extracontrattuale ed elaboratore elettronico*, in *Diritto dell'informazione e dell'informatica*, 1986, p. 385.

AL MUREDEN E., *Autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense*, in *GIURISPRUDENZA ITALIANA*, 2019, p. 1706.

AMIDEI A., *Robotica intelligente e Responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Intelligenza Artificiale e Responsabilità*, a cura di Ugo Ruffolo, 2017, pp. 82-88.

AMIDEI A., *Intelligenza Artificiale e responsabilità da prodotto*, in RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti l'etica*, 2020, p. 137.

AMIDEI A., *La responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in U. RUFFOLO, *XXVI Lezioni di diritto dell'intelligenza artificiale* (a cura di), 2020, p. 156.

AMIDEI A., *Le responsabilità da intelligenza artificiale tra product liability e sicurezza del prodotto*, in *XXVI Lezioni di diritto dell'intelligenza artificiale*, Ugo Ruffolo (a cura di), 2021, pp. 153-154.

AVILA NEGRI S. M. C., *Robot as Legal Person: Personhood in Robotics and Artificial Intelligence*, in *Frontiers in Robotics and AI*, 2021, p. 5.

BALDASSARRE C., *Responsabilità del produttore: danno risarcibile, onere della prova e logica giuridica*, in *Danno e resp.*, 2014, pp. 1444 e ss.

- BARBIERATO D., *Trattamento dei dati personali e “nuova” e responsabilità civile*, in *Responsabilità civile e previdenza*, n.6/2019.
- BELLISARIO E., *Il danno da prodotto conforme tra regole preventive e regole risarcitorie*, in *Europa e diritto privato*, 2016, p. 34.
- BRADFORD A., *The Brussels Effect, How the European Union Rules the World*, Oxford University Press, 2021.
- BRUSAMOLIN MANTOVANI A., *Elementi di informatica*, Cedam, p. 69.
- CALABRESI G., AL MUREDEN A., *Driverless cars, Intelligenza artificiale e futuro della mobilità*, Il Mulino, 2021, p. 12.
- CAPUZZO G., *Minority Report. Uno studio su intelligenza artificiale e comparazione giuridica tra UE, USA e Cina*, p. 515.
- CASTRONOVO C., *La nuova responsabilità civile*, Milano, 2006, pp. 438 e ss.
- CHITI E., MARCHETTI B., *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della Regolazione dei mercati*, n.1/2020, pp. 31-34.
- CIBELLA E., *Il principio di precauzione nell’ambiente digitale*, in *P.A. Persona e Amministrazione*, n.1/2023, pp. 521-523.
- CIONI A., *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*, n.2/2023, pp. 656 e ss.
- CHATZIPANAGIOTOIS M., *Product Liability Directive and Software Updates on Automated Vehicles*, in *Proceedings of SETN 2020, 11th Hellenic Conference on Artificial Intelligence*, SETN, 2020.
- COCUCCIO M., *Dimensione “patrimoniale” del dato personale e tutele risarcitorie*, in *Diritto di Famiglia e delle Persone*, n.1/2022, pp. 241-243.

- COMANDE' G., *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, ISSN 1720-951X, n.1/2019, pp.186-186.
- COMPORTE M., *Fatti illeciti: le responsabilità oggettive*, Giuffrè, 2009, p. 88.
- COPPINI L., *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, 2018, p. 734.
- CORSARO L., voce "Responsabilità da cose", in *Dig.disc.priv.*, sez. civ., XVII, Torino, 1998, p. 105.
- COSTANZA M., *Robot e impresa*, in U. RUFFOLO (a cura di) *Intelligenza artificiale e responsabilità*, Milano, 2017, p. 112.
- COSTANZA M., *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giurisprudenza italiana*, 2019, p. 1688.
- COZZI M., *La responsabilità civile per danno da cose (diritto italiano e francese)*, Padova, 1935, p. 333.
- D'ALFONSO G., *Intelligenza artificiale e responsabilità civile. Prospettive europee*, in *Revista de Estudios Juridicos y Criminologicos*, ISSN-e 2345-3456, n.6/2022, p. 187.
- D'ALFONSO G., *Il regime di responsabilità da cose in custodia tra questioni tradizioni e "responsabilità da algoritmo"*, in *European Journal of Privacy Law and Technologies*, ISSN 2704-8012, 2022, p. 103.
- DAINI C., *La responsabilità da cose in custodia*, in *Danno e responsabilità*, 2019, p. 193.
- DE CONCA S., *Bridging the Liability Gaps: Why AI Challenges the Existing Rules on Liability and How to Design Human-empowering Solutions*, in *Law and Artificial Intelligence*, Springer, v. 35, 2022, pp. 239-256.

DEL FEDERICO C., *Intelligenza artificiale e responsabilità civile. Alcune osservazioni sulle attuali proposte europee*, in *Jus Civile*, ISSN 2281-3818/2421-2563, n. 5/2023, pp. 1039-1040.

DE MARI CASARETO DAL VERME T., *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma*, in *BioLaw Journal – Rivista di BioDiritto*, n.3/2023.

DI DONNA L., *La controversa soggettività giuridica dei robot*, in *Intelligenza artificiale e rimedi risarcitori*, 2022.

DI DONNA L., *Software intelligenti e responsabilità del produttore*, in *Intelligenza artificiale e rimedi risarcitori*, 2022, pp. 91-93.

FINOCCHIARO G., *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Le nuove leggi civili commentate*, n.1/2017, pp. 10-14.

FINOCCHIARO G., *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Il diritto dell'informazione e dell'informatica*, n.2/2022, pp. 309-310.

FINOCCHIARO F., *La regolazione dell'intelligenza artificiale*, in *Rivista trimestrale di diritto pubblico*, n.4/2022, p. 1089.

FRANZONI M., *L'illecito I*, in *Tratt. Franzoni*, Milano, 2010, p. 692.

FRIGIDA F., *Responsabilità del sorvegliante dell'incapace, dei genitori e tutori, dei padroni e Committenti*, in *La Responsabilità Civile*, Giuffrè, 2018, pp. 1798 e ss.

HACKER P., *The European AI liability directives - Critique of a half-hearted approach and lessons for the future*, in *Computer Law and Security Review*, n. 51/2023, p. 6.

HAUSELMANN A., *Disciplines of AI: An Overview of Approaches and Techniques*, in *Law and Artificial Intelligence*, Springer, 2022, pp. 46 e ss.

KONIGS P., *Artificial intelligence and responsibility gaps: what is the problem?*, in *Ethics and information Technology*, 2022.

LO SAPIO G., *Intelligenza artificiale: rischi, modelli regolatori, metafore*, in *federalismi.it – ISSN 1826-3534*, n. 27/2022, p. 242.

MATTHIAS A., *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics and Information Technology*, 2004, p. 178.

MAZZINI G., SCLAZO S., *Relazione al convegno organizzato dall'Università degli Studi di Trento, su "Diritto e potere nell'era dell'intelligenza artificiale"*, 25 febbraio 2022.

MONTINARO R., *Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law*, in *Persona e Mercato*, n.4/2020, pp. 366-368.

NADDEO F., *Intelligenza artificiale: profili di responsabilità*, in *Comparazione e diritto civile*, 2020, p. 1158.

NEWELL A., SIMON H.A., *Computer Science as Empirical Inquiry: Symbols and Search*, in *Communications of the ACM*, 1976, pp. 113 e ss..

PAGALLO U., *The Laws of Robots: Crimes, Contracts and Torts*, Springer, 2013, p. 128.

PAPAKONSTANTINO V., DE HERT P., *Refusing to award legal personality to AI: why the European Parliament got it wrong*, in *European Law blog*, 2020.

PIANA D., VICICONTE G., *Considerazioni critiche sulla proposta regolativa europea in materia di intelligenza artificiale con attenzione ai profili attuativi*, in *Rivista Corte dei conti*, n. 4/2022, p. 9.

POLLASTRELLI S., *Circolazione di veicoli*, in P. SCHLESINGER (diretto da), *Il Codice civile. Commentario*, Milano, 2022, p. 179.

POLLICINO O., DE GREGORIO G., *Intelligenza artificiale, data protection e responsabilità*, in F. DONATI, A. PERRUCCI, A. PAJNO (a cura di) *Intelligenza artificiale e diritto*, Il Mulino, volume 2, 2022.

PONZANELLI G., *Responsabilità per danno da computer: alcune considerazioni comparative*, in *Resp. civ. prev.*, 1991, p. 653.

PIETRAFESA, F. MARZANO, T. MEDICI (a cura di), *La rete e il fattore C: Cultura, Complessità, Collaborazione*, Volume II, Roma, Stati Generali dell'Innovazione, 2016, p. 79.

PROCIDA MIRABELLI DI LAURO A., *Intelligenze artificiali e responsabilità civile*, in A. PROCIDA MIRABELLI DI LAURO, M. FEOLA (a cura di), *Diritto delle obbligazioni*, Napoli, 2020, p. 520.

RAPOSO V. L., *Ex Machina: preliminary critical assessment of the European Draft Act on artificial intelligence*, in *International Journal of Law and Information Technology*, n.30/2022, pp. 90-91.

RESTA G., *Cosa c'è di "europeo" nella proposta di Regolamento UE sull'intelligenza artificiale?*, in *Il diritto dell'informazione e dell'informatica*, n.2/2022, p. 326.

ROBERTS H., *Achieving a "Good AI Society: Comparing the Aims and Progress of the EU and US*, p. 67.

RODOLFI L., *Appunti sparsi di Machine learning. Un vademecum per comprendere uno degli argomenti più affascinanti dei nostri giorni*, 2019, p. 19.

RUFFOLO U., *Per i fondamenti di un diritto della robotica self-learning; dalla Machinery produttiva all'auto driverless: verso una "responsabilità da algoritmo?"*, in *Intelligenza Artificiale e Responsabilità*, a cura di Ugo Ruffolo, 2017, p. 14.

RUFFOLO U., *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giur.it.*, 2019, p. 1699.

RUFFOLO U., *La responsabilità da algoritmo*, in *XXVI lezioni di diritto dell'Intelligenza Artificiale* (a cura di), 2020, pp. 132-133.

RUFFOLO U., *Le responsabilità da produzione e gestione di intelligenza artificiale self-learning*, in U. RUFFOLO (a cura di) *XXVI Lezioni di Diritto dell'Intelligenza Artificiale*, G. Giappichelli Editore, 2020, p. 138.

- RUFFOLO U., *La personalità elettronica tra “doveri” e “diritti” della macchina*, in *XXVI Lezioni di Diritto dell’Intelligenza Artificiale* (a cura di), 2020, pp. 121-122.
- RUFFOLO U., *Il problema della “personalità elettronica”*, in *Journal of Ethics and Legal Technologies*, 2020, p. 80.
- SALANTIRO U., *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Rivista di diritto civile*, n.6/2020, p. 1247.
- SAMUEL A.L., *Some studies in machine learning using the game of checkers*, in *IBM Journal of Research and Development*, 1959, pp. 210 e ss.
- SANTOSUOSSO A., BOSCARATO C., CAROLEO F., *Robot e diritto: una prima ricognizione*, in *La Nuova Giurisprudenza Commentata*, 2012, p. 495.
- SANTOSUOSSO A., TOMASI M., *Diritto, scienza, nuove tecnologie*, Wolters Kluwer, 2021, pp. 338 e ss.
- SALVI C., *La responsabilità civile*, Giuffrè Francis Lefebvre, 2019, p. 216.
- SARTOR G., LAGIOIA F., *Le decisioni algoritmiche tra etica e diritto*, in *Intelligenza artificiale: il diritto, i diritti e l’etica*, in U. Ruffolo (a cura di) *Intelligenza artificiale. Il diritto, i diritti, l’etica*, 2020, pp.63-88.
- SARTOR G., *L’intelligenza artificiale e il diritto*, Giappicchelli, 2022, p. 46.
- SCHEPISI C., *Le “dimensioni della regolazione dell’intelligenza artificiale nella proposta di regolamento della Commissione*, in *Quaderni AISDUE*, ISSN 2723-9969, Sezione “Atti convegni AISDUE”, n. 16/2022, p. 334.
- SCIALDONE M., *Il diritto dei robot: la regolamentazione giuridica dei comportamenti non umani*, in Emma Pietrafesa, Flavia Marzano e Tiziana Medici (a cura di) *La rete e il fattore C: Cultura, Complessità, Collaborazione*, Volume II, Roma, Stati Generali dell’Innovazione, 2016.
- SCOTT J., *The Global Reach of EU Law*, in M. CREMONA – J. SCOTT (a cura di) *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, 2019, p. 21.

SEARLE J.R., *Minds, Brains and Programs*, in *The Behavioural and Brain Science*, 1980, pp. 417 e ss.

SOLAIMAN S. M., *Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy*, in *Artificial Intelligence and Law*, 2017 p. 174.

STELLA G., *Causa ignota del danno derivante dall'uso del prodotto e responsabilità del produttore per prodotto difettoso*, in *Responsabilità civile e previdenza*, n. 5/2017, pp. 1445-1447.

TAMPIERI M., *L'intelligenza Artificiale tra storia e utopia per il futuro*, in *L'Intelligenza Artificiale e le sue evoluzioni*, CEDAM, 2022, pp. 9 e ss.

TEUBNER G., *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, 2019.

TRIMARCHI P., *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 193 ss.

WAGNER G., *Robot Liability*, 2018, p. 11.

WAGNER G., *Robot, Inc.: Personhood for Autonomous System?*, in *Fordam Law Review*, 2019, pp. 594-595.

ZACCARIA A., *La responsabilità del "produttore" di software*, p. 303.

Sitografia

CONTISSA G., GALLI F., GORDANO F., SARTOR G., *Il Regolamento europeo sull'intelligenza artificiale*, in *i-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale*, *Rivista semestrale online*: www.i-lex.it, n. 2/2021, pp. 17-18.

FORT L., IEVA V., *Intelligenza artificiale, responsabilità civile e interpretazione analogica*, in www.biodiritto.org, 2020, p. 15.

RICCIARDELLI U., *Automazione self-learning e responsabilità civile: note a margine di una riflessione europea*, in *Cammino Diritto*, <https://rivista.camminodiritto.it>, n.5/2020, p. 34.

