LUISS

Dipartimento
di Giurisprudenza

Cattedra di Informatica Giuridica

FRAMEWORK GIURIDICO PER L'INTELLIGENZA ARTIFICIALE

Chiar.mo Prof. Francesco Romeo
RELATORE

Chiar.mo Prof. Stefano Russo
CORRELATORE

Jacopo Cimini, 139163
CANDIDATO

Anno Accademico 2020/2021

Indice

Capitolo Quarto

Prospettive di Attribuzione di Responsabilità

Capitolo Quinto

Attività Ad Alto Rischio. Un Caso Particolare.

Introduzione

Secondo un'analisi effettuata nel 2018, il mercato dell'intelligenza artificiale, valutato in quell'anno a 21.46 miliardi di dollari, avrebbe raggiunto un valore di circa 190 miliardi di dollari nel 2025[1]. Una più recente analisi, ha stimato che per il 2020 il valore di mercato delle IA si sarebbe stanziato sui 156 miliardi dollari, con una previsione per il 2025 di oltre 300 miliardi di dollari[2]. Ancora, come riportato dal *New York Times*, nel 2017 la Cina ha attuato un piano interno del valore di 150 miliardi di dollari per tentare di diventare leader mondiale nel settore delle intelligenze artificiali[3].

Tali dati sono sufficienti per comprendere come l'intelligenza artificiale, che molti ancora ritengono frutto di discorsi fantascientifici, si appresta ad introdursi nella quotidianità dell'essere umano.

Lo sviluppo di questa tecnologia deve essere supportato con entusiasmo, considerati i molteplici benefici che essa può apportare. Tuttavia, accanto ai benefici, è necessario considerare anche i possibili danni: come riportato dalla Commissione Europea, "*while AI can do much good, including by making products and processes safer, it can also do harm. This harm might be both material (safety and health of individuals, including loss of life, damage to property) and immaterial (loss of privacy, limitations to the right of freedom of expression, human dignity, discrimination for instance in access to employment), and can relate to a wide variety of risks. A regulatory framework should concentrate on how to minimise the various risks of potential harm, in particular the most significant ones*"[4].

---

[1] MarketsandMarkets, "*Artificial Intelligence Market by Offering (Hardware, Software, Services), Technology (Machine Learning, Natural Language Processing, Context-Aware Computing, Computer Vision), End-User Industry, and Geography - Global Forecast to 2025*" (febbraio 2018).

[2] International Data Corporation, "*IDC Forecasts Strong 12.3% Growth for AI Market in 2020 Amidst Challenging Circumstances*" (4 agosto 2020), disponibile presso https://www.idc.com/getdoc.jsp?containerId=prUS46757920 (ultimo accesso 25 settembre 2020).

[3] Paul Mozur, "*Beijing Wants A.I. to Be Made in China by 2030*" (New York Times, 20 luglio 2017), disponibile presso https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html?_r=0 (ultimo accesso 25 settembre 2020).

[4] European Commission, "*WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust*" (Bruxelles, 19 febbraio 2020).

Sebbene non possa dirsi che i sistemi di IA operino in un mondo senza leggi - in quanto a livello nazionale, europeo e internazionale è già riscontrabile un *corpus* giuridico[5] - si tratta comunque di discipline non specifiche, ma generali, estendibili solo in via analogica alle IA. In tal senso, un esempio può essere la direttiva europea relativa ai prodotti difettosi, che si presta bene ad essere estesa anche ai sistemi intelligenti; tuttavia, come sottolinea il Parlamento Europeo, "nonostante l'ambito di applicazione della direttiva 85/374/CEE, l'attuale quadro giuridico non sarebbe sufficiente a coprire i danni causati dalla nuova generazione di robot, in quanto questi possono essere dotati di capacità di adattamento e di apprendimento che implicano un certo grado di imprevedibilità nel loro comportamento, dato che imparerebbero in modo autonomo, in base alle esperienze diversificate di ciascuno, e interagirebbero con l'ambiente in modo unico e imprevedibile"[6].

Su tali premesse si articolerà l'analisi di questa dissertazione.

In primo luogo si cercherà di evidenziare gli aspetti critici delle normative europee ed extra-europee correlati all'ingresso di un nuovo potenziale attore nella società umana.

In secondo luogo, una volta individuate le criticità, la ricerca sarà indirizzata alla determinazione di nuove regole specifiche, avendo bene in mente che la loro introduzione non dovrà compromettere lo sviluppo di tali tecnologie.

Considerato l'elevato impatto che le intelligenze artificiali avranno nei vari settori del diritto, sarà privilegiato un approccio multidisciplinare.

Ulteriormente, nel lavoro di ricerca, si seguirà un approccio comparatistico, con particolare riferimento agli ordinamenti giuridici europei e statunitensi, in quanto modelli paradigmatici di *civil law* e *common law*.

---

[5] Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, *Orientamenti Etici per un'IA Affidabile*, istituito dalla Commissione europea nel giugno 2018. Disponibile preso https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[6] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)) (doc. P8_TA(2017)0051).

Capitolo Primo
L'Intelligenza Artificiale

1. Definizione di IA.

L'Intelligenza Artificiale "è quella disciplina, appartenente all'informatica, che studia i fondamenti teorici, le metodologie e le tecniche che permettono di progettare sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico delle prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana"[7]. Questa definizione è, attualmente, la più accreditata a livello internazionale.

Si tratta di una disciplina, *strictu sensu*, molto recente, le cui origini vanno ricercate nella seconda metà del XX secolo; prima di allora si può parlare di IA solo in senso ampio, in quanto lo studio non era focalizzato esclusivamente su di essa, ma ricomprendeva altre discipline, quali la cibernetica e alcune primordiali macchine ad elevata capacità computazionale, come i primi calcolatori elettronici.

Nella prima metà del XX secolo, infatti, si parlava non tanto di intelligenza artificiale quanto di "macchine pensanti", termine cui si riferisce Alan Turing, matematico e filosofo del XX secolo, ritenuto uno dei padri fondatori del ramo dell'intelligenza artificiale. Turing stesso, si pone il seguente quesito: possono le macchine pensare? Invece di rispondere alla domanda, formulando una definizione formale di "macchina pensante", dà nuova forma al problema, creando un gioco in grado di giungere allo stesso risultato in maniera deduttiva, il c.d. *Imitation Game*: si prendono 3 soggetti, un uomo A, una donna B e un interrogatore C, il cui sesso è irrilevante; l'interrogatore, posto in una stanza separata rispetto agli altri due, dovrà determinare, mediante domande, quale dei due sia l'uomo, dunque A, e quale dei due sia la donna, dunque B. L'obiettivo di A è portare C ad effettuare una scelta sbagliata, mentre l'obiettivo di B è aiutare C a compiere la scelta corretta. Cosa accade però se A viene sostituito da una macchina? L'interrogatore verrà indotto in errore sia che si giochi in presenza di una

[7] Marco Somalvico, Amigoni, F., & Schiaffonati, V. (n.d.), "INTELLIGENZA ARTIFICIALE".

macchina o in assenza di essa? Quest'ultimo interrogativo sostituisce la domanda iniziale ("possono le macchine pensare?"), fornendo non tanto una definizione, ma un metodo di determinazione dell'esistenza di una macchina pensante: se l'interrogatore, portato all'errore, non è in grado di distinguere fra la macchina e l'essere umano, si è in presenza di una "macchina pensante", ovvero di una intelligenza artificiale.

Al di là del fondamentale contributo apportato da Turing e dal suo test, convenzionalmente la data di nascita dell'intelligenza artificiale si colloca tra il 1955 ed il 1956; tale termine fu coniato da John McCarty, *Assistant Professor* presso la facoltà di Matematica al *Dartmouth College*, nel momento in cui, assieme ad altri colleghi, propose l'istituzione di una conferenza mediamente un documento informale noto come "Proposta di Dartmouth". Tale documento, oltre ad introdurre per la prima volta il termine di intelligenza artificiale[8], motiva la necessità della conferenza con la seguente asserzione: "Lo studio procederà sulla base della congettura per cui, in linea di principio, ogni aspetto dell'apprendimento o una qualsiasi altra caratteristica dell'intelligenza possano essere descritte così precisamente da poter costruire una macchina che le simuli"[9].

I dizionari moderni presentano diversi approcci alla definizione di intelligenza artificiale.

L'*English Oxford Living Dictionary* definisce l'IA come la teoria e lo sviluppo di sistemi informatici in grado di svolgere compiti che normalmente richiedono intelligenza umana, come la percezione visiva, il riconoscimento vocale, il processo decisionale e la traduzione tra le lingue[10].

---

8 Si ritiene che questo nome sia stato scelto, almeno in parte, per la sua neutralità; con tale termine McCarty ha voluto isolare e focalizzare la disciplina, evitando, ad esempio, qualunque confusione con la scienza cibernetica.

9 John McCarthy, Marvin Minsky, Claude Elwood Shannon, and Nathaniel Rochester, "*A proposal for the Dartmouth Summer Research Project on Artificial Intelligence*", trad. it. di G. Paronitti, disponibile presso https://web.archive.org/web/20150112124045/http://www.dif.unige.it/epi/hp/frixione/dartmouth_proposal_ital.pdf (ultimo accesso 25 settembre 2020).

10 *Lexico.com*, s.v., "artificial intelligence", disponibile presso https://www.lexico.com/definition/artificial_intelligence (ultimo accesso 25 settembre 2020).

Il *Cambridge Dictionary*, invece, parla di macchine che hanno alcune delle qualità presenti nella mente umana, quali l'abilità di comprendere il linguaggio, riconoscere immagini, risolvere problemi e imparare[11].

Ancora, il *White Paper on AI* della Commissione Europea più semplicemente parla di IA come un insieme di tecnologie che combinano dati, algoritmi e potenza di calcolo.

Nel cercare di rendere una definizione generale ed onnicomprensiva, si può dire che l'intelligenza artificiale è quella parte della scienza informatica che studia, progetta e mira a realizzare sistemi hardware e software che, mediante il combinato uso di preesistenti dati ed algoritmi, simulino l'intelligenza umana, emulandone caratteristiche e qualità, e che siano in grado di svolgere compiti che si ritiene possano essere svolti solo ed esclusivamente da un essere umano.

Ciò posto, occorre individuare quali siano le caratteristiche umane che, una volta emulate, possano farci ritenere di essere in presenza di una IA e, in tal senso, soccorre nuovamente il *Turing Test:* per fare in modo di ingannare l'interrogatore, la "macchina" deve essere in grado di comunicare in una lingua intelligibile; deve possedere delle nozioni, essere in grado di conservarle e riuscire ad estrapolarle quando necessario, mediante ragionamenti autonomi; deve essere in grado di imparare dall'ambiente che la circonda in modo tale da ampliare il suo "pacchetto" di conoscenze (c.d. *machine learning*).

2. Funzionamento dell'IA.

Atecnicamente parlando, l'intelligenza artificiale "funziona combinando grandi quantità di dati con un'elaborazione veloce e iterativa e algoritmi intelligenti, consentendo al software di imparare automaticamente dai modelli o dalle caratteristiche dei dati"[12]. Sarebbe a dir poco riduttivo concludere qui il funzionamento dell'intelligenza

---

[11] *Dictionary.cambridge.org/it/*, s.v., "artificial intelligence", disponibile presso https://dictionary.cambridge.org/it/dizionario/inglese/artificial-intelligence (ultimo accesso 25 settembre 2020).

[12] SAS Institute (n.d.), "Intelligenza Artificiale: Che cos'è e come funziona", disponibile presso https://www.sas.com/it_it/insights/analytics/what-is-artificial-intelligence.html (ultimo accesso 25 settembre 2020).

artificiale, considerato che l'IA è una scienza molto vasta che comprende diverse teorie, metodi e tecnologie, ma la definizione poc'anzi posta funge da buon punto di partenza: dalla sua analisi, infatti, possiamo estrapolare gli elementi di maggior interesse, cioè algoritmi intelligenti e *self-learning softwares*.

Lo sviluppo di algoritmi intelligenti, cioè algoritmi sempre più nuovi, numerosi e complessi, consente di emulare quella capacità umana di prendere decisioni sulla base dell'ambiente circostante. Non si tratta di un processo decisionale statico, ma dinamico, spinto dal contesto nel quale ci si trova (un banale esempio di modello decisionale dinamico è la "*fight or flight response*"). Un buon esempio di algoritmo intelligente di questo tipo possono essere le auto a guida autonoma: a seconda degli input ricevuti dai vari sensori, la macchina, in presenza di un pericolo, potrebbe decidere di sterzare o frenare; non si tratta di una decisione predeterminata, appunto statica, ma una decisione presa in conformità alla situazione come in quel momento percepita.

Sebbene l'importanza di questi algoritmi sia innegabile, ciononostante uno dei principali passi avanti nella realizzazione di intelligenze artificiali è stato fatto con il *machine learning*. Si tratta di specifiche forme di algoritmi autodidatti, capaci di apprendere dai propri errori; tramite l'apprendimento automatico, "una macchina è in grado di imparare a svolgere una determinata azione anche se tale azione non è mai stata programmata tra le azioni possibili"[13]. È questa la differenza principale tra *machine learning* e algoritmi intelligenti, cioè che questi ultimi effettuano una decisione, influenzata da *input* esterni, fra un numero di possibili decisioni pre-programmate, mentre il primo compie un'azione che non è mai stata programmata. Il *machine learning* è, comunque, un *genus*, all'interno del quale si sono sviluppate diverse *species*, tra le quali un ruolo di spicco assume il *deep learning* (o apprendimento approfondito).

Secondo una definizione tecnica, il *deep learning* è "apprendimento di dati che non sono forniti dall'uomo, ma sono appresi grazie all'utilizzo di algoritmi di calcolo statistico", il cui scopo è "comprendere il funzionamento del cervello umano e come

---

[13] Portale dedicato all'Intelligenza Artificiale, "Intelligenza Artificiale: Cos'è, Come Funziona E A Cosa Serve?", disponibile presso https://www.intelligenzaartificiale.it/ (ultimo accesso 25 settembre 2020).

riesca ad interpretare le immagini e linguaggio" e che, in definitiva, consente di apprendere "i concetti più alti […] a partire dai livelli più bassi"[14].

Per meglio comprendere questo concetto, si pensi alla circolazione stradale: essa si basa, tra l'altro, su sistemi di segnaletica verticale e orizzontale ed un essere umano associa a quei simboli e parole uno specifico significato e, conseguentemente, compie determinate azioni (così, al segnale di stop, si arresta l'autovettura); il sistema di *deep learning* è in grado, una volta addestrato riconoscere la segnaletica, di associare induttivamente a quel simbolo un comportamento e da ultimo compiere l'azione necessaria.

L'effettiva efficacia dei sistemi di *machine learning* è, tuttavia, ancorata ad un ulteriore sistema, le reti neurali. Si consideri la parola: una medesima parola, pronunciata con inflessioni e toni diversi, può essere interpretata in più modi dal nostro cervello ed assumere significati diversi. Questa capacità del cervello umano non è possibile replicarla con singoli algoritmi ed in questo contesto rileva l'importanza delle reti neurali, simulazione artificiale di quelli che sono dendriti, sinapsi, neuroni, ecc., che compongono un cervello umano. È ovvio che il sistema neurale artificiale è molto semplificato rispetto a quello biologico, ma il funzionamento di base è lo stesso: "i nodi ricevono dati in input, li processano e sono in grado di inviare le informazioni ad altri neuroni. Attraverso cicli più o meno numerosi di input-elaborazione-output, […] diventano in grado di generalizzare e fornire output corretti associati ad input non facenti parte del *training set*"[15].

Il vero fulcro di intelligenza delle IA risiede proprio nelle reti neurali, in quanto "una macchina non sarà mai veramente intelligente se non riuscirà a riprodurre un sistema di ragionamento che sia biologicamente ispirato al cervello dell'uomo"[16].

---

[14] Portale dedicato all'Intelligenza Artificiale, "Deep Learning", disponibile presso https://www.intelligenzaartificiale.it/deep-learning/ (ultimo accesso 25 settembre 2020).

[15] Portale dedicato all'Intelligenza Artificiale, "Reti Neurali", disponibile presso http://www.intelligenzaartificiale.it/reti-neurali/ (ultimo accesso 25 settembre 2020).

[16] *op. cit.* Deep Learning

3. Stato dell'arte.

L'intelligenza artificiale ha già superato le capacità umane in diversi ambiti. Nel settore ludico le IA più volte hanno battuto esseri umani, campioni mondiali di un'ampia gamma di giochi e se ciò può risultare scontato o non particolarmente impressionante, bisogna ricordare come non troppo tempo fa padroneggiare il gioco degli scacchi era considerato fra i più alti risultati della mente umana, tant'è vero che si scriveva che "*if one could devise a successful chess machine, one would seem to have penetrated to the core of human intellectual endeavor*"[17]. Perché allora così poco entusiasmo di fronte a queste IA? Risuonano a gran voce quelle le parole di John McCarty, il quale reclamava che "*As soon as it works, no one calls it AI anymore*".

In realtà una spiegazione di fronte a questa moderata eccitazione è presente, in particolar modo se si considera proprio il gioco degli scacchi, per il quale si riteneva fosse necessario apprendere "*abstract concepts, think cleverly about strategy, compose flexible plans, make a wide range of ingenious logical deductions, and maybe even model one's opponent's thinking*"[18]; ma così non è, dato che linee di codice e algoritmi di media complessità ben possono riprodurre strategie vincenti. La "semplicità" delle operazioni richieste per creare queste IA è la risposta al precedente quesito: ci troviamo di fronte ad eccezionali "giocatori" di scacchi ma a nulla di più.

Quale è quindi lo stato attuale dell'IA? In realtà Intelligenza artificiale è termine generico che ricomprende al suo interno tre categorie: *artificial narrow intelligence* (ANI), anche nota come intelligenza artificiale debole; *artificial general intelligence* (AGI), anche nota come intelligenza artificiale forte; *artificial superintelligence* (ASI).

Le intelligenze artificiali deboli sono programmate per svolgere un unico compito. Si tratta dell'unico tipo di IA realizzato con successo e, per tal motivo, quello che è maggiormente presente nella società; esempi di ANI variano da software di traduzione

---

[17] Allen Newell, Shaw J. C. and Simon H. A., "*Chess-Playing Programs and the Problem of Complexity*" (IBM Journal of Research and Development, vol. 2, no. 4, pp. 320-335, Ott. 1958), doi: 10.1147/rd.24.0320.

[18] Nick Bostrom, "*SUPERINTELLIGENCE - paths, dangers, strategies*" (1st ed.), (Oxford: Oxford University Press 2014).

ad assistenti vocali (Siri, Alexa, Cortana), da software di riconoscimento facciale alle autovetture a guida autonoma. A riguardo John R. Searle, filosofo americano, scrive "*the principal value of the computer in the study of the mind is that it gives us a very powerful tool. For example, it enables us to formulate and test hypotheses in a more rigorous and precise fashion*"[19]. Si tratta, per la maggior parte di macchine che simulano, emulano l'intelligenza umana, incapaci di riprodurla nella sua interezza.

Una AGI, invece, non vuole emulare l'intelligenza umana, ma riprodurla: non è in grado di svolgere un determinato compito, ma è in grado di svolgerne una molteplicità con capacità simili o eguali a quelle di un essere umano. Data la definizione di intelligenza proposta da Linda S. Gottfredson, una AGI dovrebbe essere in grado di "*reason, plan, solve problems, think abstractly, comprehend complex ideas, learn quickly and learn from experience*"[20]. Ancora, secondo Searle, "*according to strong AI, the computer is not merely a tool in the study of the mind; rather, the appropriately programmed computer really is a mind*"[21]. Nonostante gli scienziati non siano ancora in grado di costruire una AGI, è altamente probabile che ciò sarà possibile in un futuro vicino.

Da ultimo, le ASI sono delle intelligenze artificiali puramente teoriche e ipotetiche, macchine divenute auto-coscienti, le cui capacità sorpassano quelle di un essere umano.

Invero, il dibattito sulle IA si concentra su ANI e AGI. Tra i vari sostenitori della tesi per cui le macchine non possono definirsi intelligenti, vi è proprio John Searle, che in "*Minds, brains, and programs*", escogita il famoso "*Chinese Room Test*", generalmente contrapposto al Turing Test, il quale ultimo invece valorizza la tesi delle macchine pensanti. Con questo test, Searle vuole dimostrare che una IA in grado di tradurre, svolge l'azione sulla base di una serie di dati pre-fornitigli e grazie ad un opportuno programma manipola le parole senza comprenderne il significato. In ciò risiede l'intelligenza secondo Searle. Le seguenti elaborazioni della teoria di Searle hanno

---

[19]John. R. Searle, "*Minds, brains, and programs*", (*Behavioral and Brain Sciences 3 (3): 417-457*, 1980)

[20] Linda S. Gottfredson (n.d.). [Editorial]. "*Mainstream Science on Intelligence: An Editorial With 52 Signatories, History, and Bibliography"*.

[21] *op. cit. Minds, brains, and programs.*

condotto a definire una macchina intelligente solo quando in grado di riprodurre il funzionamento del cervello.

Tuttavia è bene considerare come Searle scriveva del "*Chinese Room Test*" quando la tecnologia era ai suoi albori e per tal motivo i sostenitori della AGI ritengono, oggi, che si tratti di una questione di tempo prima che quest'ultima possa trovare vita. Ancora, se si considera quanto precedentemente detto delle reti neurali (sistemi artificiali che, appunto, riproducono il funzionamento del cervello), risulta più agevole sostenere quest'ultima tesi.

4. I soggetti della IA.

Sebbene l'IA sia in grado di agire autonomamente, la sua creazione passa comunque dall'uomo. La catena di produzione delle intelligenze artificiali (sia dell'hardware che del software), non presenta particolari caratteristiche che la differenziano da quella di altri prodotti informatici.

Nell'ambito del presente studio l'attenzione sarà focalizzata, prevalentemente, sulle figure del produttore e del consumatore, avuto riguardo ai risvolti giuridici connessi ad errori di programmazione ovvero ad usi impropri.

4.1. Il produttore.

Le caratteristiche definitorie del concetto di produttore sono sostanzialmente uniformi nel panorama internazionale.

A livello comunitario il produttore è definito come "il fabbricante di un bene di consumo, l'importatore del bene di consumo nel territorio della Comunità europea o qualsiasi altra persona che si presenta come produttore apponendo sul bene di consumo il suo nome, marchio o altro segno distintivo"[22], formula poi ripresa dal Codice del Consumo italiano[23].

---

[22] Cfr. Articolo 1, comma 2, lett. *d*, Direttiva 1999/44/CE del Parlamento europeo e del Consiglio.

[23] Cfr. Articolo 3, lett. d), D. Lgs 206/2005.

Negli Stati Uniti, il medesimo concetto di "fornire un bene di consumo" è presente nello *United States Code*, *Title 15, Chapter 50, Section 2301*, *number (4)* che identifica nel "*supplier*", "*any person engaged in the business of making a consumer product directly or indirectly available to consumers*"[24].

Il *Código de Defesa do Consumidor* Brasiliano offre una soluzione simile, seppur inglobando nella categoria anche i fornitori di servizi; si legge infatti all'articolo 3 "*Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços*"[25].

In sintesi, dunque, il produttore è colui che fabbrica un determinato bene affinché venga reso disponibile ai consumatori.

Nel settore informatico alla realizzazione di un singolo bene può concorrere una pluralità di produttori: accade spesso, infatti, che l'hardware sia assemblato da un'azienda diversa da quella che sviluppa il software.

Si prenda ad esempio il mondo della telefonia, nel quale l'intelligenza artificiale assume il ruolo di "assistente vocale". L'industria telefonica, lato software, è dominata da Android e da iOS (sistemi operativi realizzati, rispettivamente, da Google e Apple) mentre i maggiori produttori di apparecchi cellulari, i dati più recenti[26], sono Huawei, Samsung ed Apple. La cosa che più interessa è come dalle ultime rilevazioni di vendita, Google sia relegata nella categoria "altri", ma comunque sia il primo fornitore di software (consentendo l'utilizzo del proprio software Android ad altre società, tra cui, appunto, Samsung e Huawei). La scissione che viene così a crearsi tra produttore dell'hardware e sviluppatore del software, è il motivo di questa parentesi: da un lato vediamo il "modello Apple" (comunque riscontrabile anche in altre aziende, estranee alla produzione di tecnologia "da ufficio", si pensi a Tesla che produce da sé hardware,

---

[24] Cfr. 15 U.S. Code Chapter 50— Consumer Product Warranties, §2301.

[25] Cfr. Legge N. 8.078 dell'11 Settembre 1990, Código De Defesa Do Consumidor.

[26] Canalys (31 luglio 2020). "*Global smartphone market Q2 2020*", disponibile presso https://www.canalys.com/newsroom/canalys-global-smartphone-market-declines-q2-2020 (ultimo accesso 25 settembre 2020).

in questo caso l'automobile, e software[27]) nel quale vi è unità fra produttore hardware e software, dall'altra il "modello Android", nel quale troviamo una separazione fra le due tipologie di produttori. Tale separazione presenta profili di criticità qualora sorgano inconvenienti e vi sia la necessità di attribuzione di responsabilità (*v. infra* capitolo 4).

4.2. L'intermediario.

Un'ulteriore figura è quella dell'intermediario, soggetto che si frappone, nella vendita del bene, fra produttore e consumatore. Sebbene il ruolo dell'intermediario sia di grande rilevanza sotto il profilo economico, ai fini della ricerca che si sta conducendo assume un ruolo marginale. Ciò si può desumere dalle stesse legislazioni nazionali, che equiparano le due figure: il nostro Codice del Consumo, articolo 3, lett. *d*, parla di produttore come "[…] il fabbricante del bene o il fornitore del servizio, o un suo intermediario"; lo *U.S. Code* parla di *supplier* come chiunque ~~che~~ *directly or indirectly* renda disponibile prodotti per i consumatori, alludendo, con la formula "indirectly", alla categoria degli intermediari; identico discorso può farsi analizzando l'articolo 3 del *Código de Defesa do Consumidor* Brasiliano, che fa esplicito riferimento alla categoria degli intermediari, quando include nella definizione di "*fornecedor"* coloro che svolgono attività di distribuzione (*distribuição*) di prodotti.
Ciò posto la figura dell'intermediario, salvo casi limite (connessi, ad es., alle modalità di conservazione del prodotto ovvero a dolose manomissioni), non è interessata da profili di responsabilità correlati al commercio di IA.

4.3. Il consumatore.

La definizione di consumatore, d'altra parte, risulta non uniforme nei vari ordinamenti internazionali
Il legislatore europeo, ovviamente ripreso da quello italiano nel Codice del Consumo, e sempre nella nella già citata direttiva 1999/44/CE (articolo 1, comma 2, lett. *a*) intende

[27] Tesla (n.d.). "Autopilot AI", disponibile presso https://www.tesla.com/it_IT/autopilotAI (ultimo accesso 25 settembre 2020).

per consumatore "qualsiasi **persona fisica** che, nei contratti soggetti alla presente direttiva, agisce per fini che non rientrano nell'ambito della sua attività commerciale o professionale;" l'esplicito riferimento alla categoria delle persone fisiche, esclude dal novero le persone giuridiche.

Una soluzione intermedia è proposta dallo *United States Code*, *Title 15, Chapter 50, Section 2301, number (3)* che stabilisce che consumatore "*means a buyer (other than for purposes of resale) of any consumer product, any person to whom such product is transferred during the duration of an implied or written warranty (or service contract) applicable to the product, and any other person who is entitled by the terms of such warranty (or service contract) or under applicable State law to enforce against the warrantor (or service contractor) the obligations of the warranty (or service contract).*"

In questo caso si fa riferimento a persone fisiche o giuridiche, ma al semplice acquirente di un "*consumer product*" o al titolare di diritti di garanzia (*implied or written warranty*) sul prodotto, potendosi quindi includere entrambe le tipologie di persone, fisiche e giuridiche, mentre il discrimine è costituito dal fatto che l'acquisto non sia effettuato con l'intento di operare una rivendita.

In maniera non dissimile si pone il *Competition and Consumer Act 2010* Australiano, il quake ricollega il concetto di consumatore ad un particolare comportamento del soggetto agente, piuttosto che alle qualità di quest'ultimo; si legge infatti: "*a person shall be taken to have acquired particular goods as a consumer if, and only if: (i) the price of the goods did not exceed the prescribed amount* (AUD 40,000)*; or (ii) where that price exceeded the prescribed amount—the goods were of a kind ordinarily acquired for personal, domestic or household use or consumption or the goods consisted of a commercial road vehicle; and the person did not acquire the goods […] for the purpose of using them in trade or commerce*"[28]. Il *Competition and Consumer Act 2010*, allo stesso modo dello *U.S. Code*, richiede che il bene sia acquistato per fini diversi da quello di rivendita e parimenti non distingue fra persone fisiche e giuridiche. Tuttavia, si può leggere nella *Australian Consumer Law Review* come in effetti "*many small and medium-sized businesses, as well as consumers, use and rely on protections*

[28] Cfr. Competition and Consumer Act 2010 (Cth) sch 2 ('Australian Consumer Law'), pt I, 4B

in the ACL"[29] è ciò principalmente perché la previsione di una soglia monetaria consente a certe imprese di godere dei diritti previsti dalla *Consumer Law*, fin tanto quanto che questa soglia non venga superata.

In termini più netti si esprime il *Código de Defesa do Consumidor* Brasiliano, articolo 2 che definisce il consumatore come "*toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final*"; in questo caso persone fisiche e giuridiche rientrano nella definizione e nella tutela predisposta dal *Código*.

Da questa comparazione fra i diversi codici e atti approntati per la tutela del consumatore si può notare che a livello europeo società, imprese, enti senza scopo di lucro, ecc. non riescano a godere della tutela specificamente prevista per il consumatore.

[29] Consumer Affairs Australia and New Zealand, *Australian Consumer Law Review*, Marzo 2016, pagina 11

Capitolo Secondo
Status Legale dell'IA

1. Primi approcci normativi.

Le intelligenze artificiali, sul piano commerciale, vengono normalmente classificate tra i prodotti; tuttavia negli ultimi anni si è registrato un crescendo di teorie e prassi che riconoscono i robot, e annesse IA, come titolari di una posizione giuridica propria.

Nel maggio del 2016 il Parlamento europeo ha presentato un progetto di relazione, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica. Nella Introduzione, alla lettera T, si sottolinea come "in ultima analisi, l'autonomia dei robot solleva la questione della loro natura alla luce delle categorie giuridiche esistenti – se devono essere considerati come persone fisiche, persone giuridiche, animali o oggetti – o se deve essere creata una nuova categoria con caratteristiche specifiche proprie e implicazioni per quanto riguarda l'attribuzione di diritti e doveri, compresa la responsabilità per i danni"[30].

Non si è dovuto aspettare molto per vedere le preoccupazioni espresse in questo *draft report* divenire realtà: nell'ottobre del 2017 l'Arabia Saudita ha concesso la cittadinanza ad un robot di nome "Sophia". Poco dopo, nel novembre del 2017, il Giappone ha accordato un permesso di residenza nel quartiere di Shibuya di Tokyo ad un chatbot di nome "Shibuya Mirai" (che può essere tradotto con "il futuro di Shibuya").

Andando oltre il dato simbolico di tali certificazioni, preme soffermarsi su quelle che sono le implicazioni giuridiche che tali riconoscimenti potrebbero avere. È bene, tuttavia, subito rilevare come la concessione della cittadinanza, da una parte, e della residenza dall'altra siano state effettuate senza introdurre modifiche alle specifiche normative, ma con il simbolico intento di aggiudicarsi un primato nella corsa alla regolamentazione di robot e intelligenze artificiale, come a voler dimostrare che avanguardia tecnologica e avanguardia giuridica possano procedere di pari passo; in

[30] Progetto di Relazione del Parlamento europeo del 31 maggio 2016 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)) (PR\1095387IT.doc).

quest'ottica, sono emblematiche le parole pronunciate dalla stessa "Sophia", nel corso di un'intervista sul palco del *Future Investment Initiative* di Riyad: "Sono onorata e fiera per questo riconoscimento unico. È un momento storico perché sono il primo robot al mondo riconosciuto come cittadino"[31].

Prima ancora di provare ad inquadrare le IA in una delle categorie individuate dal Parlamento europeo nel Progetto di Relazione, è necessario considerare come il riconoscimento della residenza e della cittadinanza abbiano delle implicazioni loro proprie, in certo modo scisse dalla personalità giuridica.

Invero, allo status di "*official resident*", in Giappone, seguono alcuni diritti e doveri: ad esempio, è riconosciuto il rispetto dei diritti fondamentali dell'uomo, così come è richiesto il pagamento delle tasse nazionali e locali. Essendo "Mirai" stato equiparato ad un bambino di sette anni, mentre potrebbero porsi interrogativi in relazione al rispetto di alcuni diritti fondamentali: considerato che, tra essi, è presente il diritto alla vita e supponendo che "Mirai" sia titolare di questo diritto, ci si potrebbe opporre ad un suo spegnimento, in quanto equiparabile ad una terminazione della vita.

Il caso di "Sophia" risulta maggiormente problematico sotto due profili: la maggiore estensione di diritti riconosciuti al cittadino rispetto al residente e la minorata condizione delle donne in Arabia Saudita. La costituzione saudita riconosce una pluralità di diritti ai cittadini, tra cui *welfare rights* (art. 27), *health care* (art. 31), *due process* (artt. 43-47), ma, soprattutto, l'articolo 17 del *Municipal Councils Law* stabilisce che "*every citizen (male or female) has the right to vote […]*"[32]; se rigidamente applicata, la cittadinanza consentirebbe, quindi, a "Sophia" la possibilità di votare alle elezioni del *city council* o l'accesso a cure (*rectius* riparazioni) gratuite. V'è poi la questione delle limitazioni ai diritti delle donne, che sono sottoposte alla vigilanza di un tutore, noto come "*mahram*", il quale fornisce autorizzazione per compiere

---

[31] The Jakarta Post. "*Meet Sophia: The first robot declared a citizen by Saudi Arabia*" YouTube video, 3:16. 29 ott 2017, disponibile presso https://www.youtube.com/watch?v=E8Ox6H64yu8 (ultimo accesso 25 settembre 2020).

[32] *Elections in Kingdom of Saudi Arabia* (5 marzo 2020), disponibile presso https://www.my.gov.sa/wps/portal/snp/aboutksa/electionsInTheKingdomOfSaudiArabia/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8zivQIsTAwdDQz9LSw8XQ0CnT0s3JxDfA2AQD84NU-_INtREQAI12hE/ (ultimo accesso 25 settembre 2020).

determinate azioni (quale, ad esempio, accedere a cure mediche particolari o interventi chirurgici); sembra, comunque, che l'attribuzione del sesso femminile a "Sophia" abbia una valenza puramente formale, considerato che "*Sophia s'est montrée seule face au public, sans son tuteur. Chose interdite pour une Saoudienne. De plus, elle ne portait pas l'abaya, pourtant obligatoire*"[33].

2. Le classificazioni indicate dal Parlamento Europeo. Considerazioni.

Cerchiamo ora di inquadrare le IA nell'ambito delle categorie di soggetti proposte nel Progetto di Relazione elaborato dal Parlamento Europeo.
L'idoneità ad essere "soggetti" (cioè centri di imputazione di situazioni giuridiche soggettive), viene definita come "capacità giuridica", che, nella maggior parte degli ordinamenti, compete a persone fisiche ed enti.

2.1. Persone fisiche.

Consideriamo, in primo luogo, le persone fisiche. Una persona fisica acquista la capacità giuridica in quanto essere umano[34], cui sono attribuiti "diritti inviolabili" presenti nelle moderne carte costituzionali e in vari trattati internazionali (es. Dichiarazione Universale Dei Diritti Dell'uomo; Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali; Patto Internazionale Relativo ai Diritti Civili e Politici; Carta dei Diritti Fondamentali dell'Unione Europea). Tali diritti sono garantiti a tutti gli uomini in quanto tali, indipendentemente dalla concessione di cittadinanza o residenza, come specificato dalla Corte di Cassazione italiana: "la tutela di diritti come quelli alla vita, all'incolumità ed alla salute deve essere

---

[33] Mooréa Lahalle, "*L'Arabie saoudite accorde la citoyenneté à un robot... de sexe féminin*" (13 novembre 2017), disponibile presso https://madame.lefigaro.fr/societe/l-arabie-saoudite-accorde-la-citoyennete-a-sophia-robot-de-sexe-feminin-271017-135000 (ultimo accesso 25 settembre 2020).

[34] Cfr. "La capacità giuridica si acquista dal momento della nascita", art. 1, comma 1, cod. civ. it.

assicurata senza alcuna disparità di trattamento a tutte le persone indipendentemente dalla cittadinanza italiana, comunitaria o meno"[35].

L'attribuzione della cittadinanza, poi, amplia ulteriormente il quadro di diritti (es. diritto di voto) e doveri (es. doveri fiscali) della persona fisica.

Categorizzare le intelligenze artificiali come persone fisiche creerebbe inconvenienti giuridici difficilmente superabili: si pensi al caso di un robot che ferisca a morte un essere umano; al robot, in primo luogo, dovrebbe essere garantito un giusto processo; cosa accadrebbe se fosse giudicato "colpevole"? si tratterebbe di un robot difettoso e, in quanto tale, dovrebbe essere "ritirato dal commercio" e smontato, ma, se titolare del diritto alla vita, ciò equivarrebbe ad ucciderlo e a violare il principio di abolizione della pena di morte.

Date queste ultime considerazioni, in aggiunta al fatto che le attuali teorie scientifiche considerano la possibilità di attribuire coscienza ed emotività alle IA come remota e appartenente ad un futuro lontano, è fortemente sconsigliata una rigida equiparazione con le persone fisiche.

2.2. Persone giuridiche.

Inquadrare le intelligenze artificiali tra le persone giuridiche risulta, invece, meno complesso.

Le persone giuridiche godono di diritti e doveri in maniera ridotta rispetto le persone fisiche, che riguardano principalmente la capacità di stipulare contratti e di essere responsabili, in sede civile e penale, delle proprie azioni.

Una ridotta rosa di diritti e doveri sembra calzare meglio le esigenze delle IA, oltretutto se si considerano le parole di Ben Goertzel, uno degli scienziati che ha contribuito alla realizzazione di "Sophia", il quale ha ammesso che "*Sophia […] is not yet capable of*

[35] Cass. civ., sez. III, 14 novembre 2014, n. 23432

understanding the world nearly as well as would ordinarily be required for human citizenship"[36].

Tuttavia, posto che la personalità giuridica costituisce *fictio iuris* necessaria per inquadrare delle entità il cui scopo è principalmente di promuovere e aiutare a perseguire interessi umani e considerato che le IA possono considerarsi come esseri dotati di minima intelligenza, ritengo che anche la classificazione tra le persone giuridiche non sia adeguata.

2.3. Animali.

La visione antropocentrica del mondo, in particolare in ambito giuridico, ridurrebbe le categorie di soggetti in due macro-gruppi, le persone e le cose. Scrive, a tal proposito, Gaio nelle *Institutiones,* "*Omne autem ius, quo utimur, uel ad personas pertinet uel ad res uel ad actiones. sed prius uideamus de personis*"[37], che, parafrasato, sta a significare che due sono le categorie esistenti, le cose o le persone, le cui ultime hanno precedenza. Questo dualismo, tuttavia, già presenta alcune criticità nell'opera di Gaio, in particolare con riferimento agli schiavi che, sebbene siano persone, erano giuridicamente considerate come cose.

Come allora fu per gli schiavi, in tempi più recenti il problema si è posto con gli animali e, attualmente, può estendersi alle IA, la cui natura di esseri senzienti e intelligenti, al pari degli animali, contraddice la loro classificazione nelle *res*, oggetti di proprietà e scambio fra le persone.

Proprio in relazione agli animali non è raro vedere oggi giurisprudenza e legislatori convergere verso una riqualificazione della loro posizione: nell'aprile del 2014 l'assemblea nazionale francese ha adottato un emendamento del codice civile[38],

---

[36] Sophia and SingularityNET: Q&A [Intervista di C. Lawrence], (*Humanity+ Magazine,* 5 Novembre 2017), disponibile presso https://hplusmagazine.com/2017/11/05/sophia-singularitynet-qa/ (ultimo accesso 25 settembre 2020).

[37] Gaio, "*Institutiones*", *Commentarii Qvattvor*, *Commentarivs Primvs*, II "*De iuris diuisione*", 8.

[38] Assemblée Nationale (France), Amendement n°59, 11 aprile 2014, disponibile presso http://www.assemblee-nationale.fr/14/amendements/1808/AN/59.asp (ultimo accesso 25 settembre 2020).

modificando lo status degli animali da cose a "esseri viventi senzienti"[39]; nel maggio del 2015 il parlamento neozelandese ha approvato l'*Animal Welfare Amendment Bill*, nel quale, allo stesso modo, gli animali sono riconosciuti come esseri senzienti, richiedendo, ulteriormente, che "*owners of animals, and persons in charge of animals, to attend properly to the welfare of those animals*"[40]; ancora, nel novembre del 2018, il parlamento belga ha adottato all'unanimità un'ordinanza nella quale si riconoscono gli animali come "*a living being endowed with sensitivity, interests of its own and dignity, that benefits from special protection*"[41]; parimenti e più di recente, in Canada, è stato presentato l'*Animal Welfare And Safety Act*, nel quale si specifica che gli animali "*are sentient beings that have biological needs*"[42]; nel nostro Paese la Corte di Cassazione ha riconosciuto gli animali "quali esseri viventi capaci di percepire con dolore comportamenti non ispirati a simpatia, compassione ed umanità"[43], così equiparando, al pari degli umani, il maltrattamento psicologico a quello fisico.

Importanti sembrano quindi i passi avanti svolti in materia, ma v'è chi sostiene che tali mosse non siano altro che "provvedimenti-bandiera", come sostiene uno dei commentatori del codice civile tedesco, il quale descrive l'esclusione degli animali nella categoria delle cose un "*sentimental pronouncement without any effective legal content*"[44]; peraltro lo stesso emendamento del Code civil francese, specifica che, se non nei casi di norme che li proteggono, "*les animaux sont soumis au régime des biens corporels*"[45].

---

[39] Cfr. "*Les animaux sont des êtres vivants doués de sensibilité*", art. 515-14, C. civ. fr.

[40] Cfr. New Zealand Judicature Amendment Act 1972, pt 1, 3A

[41] Christopher Vincent, "*Brussels parliament adopts crucial animal rights bill*" (23 novembre 2018), disponibile presso https://www.brusselstimes.com/brussels/52089/brussels-parliament-adopts-crucial-animal-rights-bill/ (ultimo accesso 25 settembre 2020).

[42] Cfr. Quebec Animal Welfare and Safety Act (chapter B-3.1)

[43] Cass. Pen., sez. III, n. 46291 del 16/10/2003

[44] Visa A.J. Kurki, "*Legal Personhood: Animals, Artificial Intelligence and the Unborn*" (Vol. 119. Cham :: Springer International Publishing :, 2017).

[45] Cfr. art. 515-14, C. civ. fr

Si è dunque ancora lontani da una equiparazione tra animali ed esseri umani, ma a ben vedere, l'estensione dei diritti (e doveri) garantiti alle persone non può essere riprodotta anche per gli animali: si può leggere infatti in una opinione della corte suprema di New York, *Appellate Division*, proprio in relazione all'applicazione di alcuni diritti fondamentali (diritto alla libertà) umani ad uno scimpanzé di nome Tommy, che "*chimpanzees cannot bear any legal duties, submit to societal responsibilities or be held legally accountable for their actions. In our view, it is this incapability […] that renders it inappropriate to confer upon chimpanzees the legal rights—such as the fundamental right to liberty protected by the writ of habeas corpus—that have been afforded to human beings*"[46].

Per quanto il riconoscimento di alcuni diritti inviolabili dell'uomo sia oggi ritenuto un imperativo anche per gli animali, appare comunque inopportuna una completa equiparazione del loro status, risultando preferibile individuare, fra persone e cose, un *tertium genus*.

Se, come si è appena detto, già la classificazione degli animali come esseri intelligenti e senzienti richiede un apposito quadro giuridico, ritengo sia parimenti inadeguata l'equiparazione agli animali delle intelligenze artificiali, considerate le diversità delle due categorie in termini di intelligenza e senzienza.

L'essere senziente è dotato di "caratteristiche biologiche e prerogative proprie degli esseri umani"[47]; più nello specifico, come afferma il monaco buddista francese di scuola tibetana Matthiue Ricard: "L'essere detto «senziente» è un organismo vivente capace di avvertire la differenza tra benessere e dolore, tra i diversi modi in cui viene trattato, vale a dire tra le condizioni propizie o nocive alla sua sopravvivenza"[48]. In altre parole, un essere senziente è in grado di provare talune emozioni (ad esempio la paura) ed associarle ad un determinato comportamento (così un animale impaurito reagirà scappando). Tali capacità non sono riscontrabili nelle intelligenze artificiali: esse

---

[46] People ex rel. Nonhuman Rights Project, Inc. v Lavery, 124 AD3d 148 (3rd Dep't 2014).

[47] *Treccani.it*, s.v., "senzienza", disponibile presso http://www.treccani.it/vocabolario/senzienza_%28Neologismi%29/ (ultimo accesso 25 settembre 2020).

[48] Matthiue Ricard, "*Sei un animale!*" (Milano: Sperling & Kupfer, 2016).

mancano di emotività e qualunque reazione assimilabile a quelle sopra descritte è il frutto di una accurata programmazione.

D'altra parte l'intelligenza animale è puramente istintiva, racchiude esclusivamente quelle capacità necessarie alla sopravvivenza. L'intelligenza artificiale, invece, è creata a immagine e somiglianza di quella umana; ciò è vero soprattutto se si considera uno degli argomenti principali di coloro che sostengono la non assimilabilità tra intelligenza umana e animale: gli animali non sono in grado di pensare razionalmente e non sono in grado di parlare. Proprio queste ultime due caratteristiche definiscono le intelligenze artificiali.

In conclusione, per le ragioni ora esposte, IA ed animali non possono essere equiparati, tantomeno nell'ambito giuridico. Ritengo, dunque, più opportuno collocare le prime in un ulteriore *quartum genus*.

2.4. Persone elettroniche.

Identificare un nuovo modello di personalità legale per le intelligenze artificiali richiede qualche cautela, in quanto è necessario separare i modelli teorici da applicare ad una utopica realtà da quelli effettivamente necessari per il futuro prossimo.

Sebbene alcuni autori, fondando le loro argomentazioni esclusivamente sull'assenza di principi e dici e di coscienza, considerino prematuro parlare di personalità giuridica per le IA, molti ritengono che, grazie anche al rapido sviluppo della scienza e delle tecnologie, già da adesso debba porsi la questione circa una personalità c.d. "elettronica". Scrive a tal proposito G. A. Gadzhiev, giudice della corte costituzionale russa, che, sebbene "*robot's legal personality recognition still is not actual*", "*after a while the creation of autonomous artificial intelligence will entail a demand for legitimization of robot's legal personality*"[49].

È chiaro quindi come il nodo giuridico sulla personalità vada sciolto prendendo in considerazione lo stato attuale delle tecnologie, separando le intelligenze artificiali più

[49] Gadis A. Gadzhiyev, "*Whether the Robot-Agent is a Person? (Search of Legal Forms for the Regulation of Digital Economy)*" [Abstract] (*Journal of Russian Law, 6*(1), 15-30, 2017), doi:10.12737/art_2018_1_2

semplici (ANI) da quelle più avanzate (AGI), cosi come evidenziato dal Parlamento e dalla Commissione europea, i quali concordano nella necessità di istituire "uno status giuridico specifico per i robot, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche con diritti e obblighi specifici […] nonché il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome in modo intelligente o che interagiscono in modo indipendente con terzi"[50].

Il modello migliore per sviluppare l'argomento, a mio avviso, è contenuto nel progetto di legge proposto da Grishin Robotics, anche noto come *Grishin Law*, che propone emendamenti al codice civile della Federazione Russa, in termini di miglioramento della regolamentazione giuridica delle relazioni nel campo della robotica. Con tale proposta si vuole introdurre una specifica sezione nel codice civile per quelli che vengono definiti come "agenti-robot", cioè "un robot che, per decisione del proprietario e per le sue caratteristiche progettuali, è destinato a partecipare al *civil turnover*[51]". Le peculiari caratteristiche tecniche di questi robot-agenti consentono loro di acquisire uno specifico status all'interno della società, giustificando la previsione di una categoria di soggetti giuridici apposita, appunto le persone elettroniche. La *Grishin Law* specifica che l'agente-robot "ha una proprietà separata ed è responsabile dei propri obblighi, può acquisire ed esercitare diritti civili e assumersi obblighi civili per proprio conto. Nei casi stabiliti dalla legge, un agente robotico può agire come partecipante a procedimenti civili". Un robot qualificato come agente-robot "è dotato di capacità giuridica" ed è in grado di agire "in qualità di soggetto di rapporti giuridici" e di effettuare "transazioni per proprio conto, inclusa la stipula di rapporti contrattuali con altre persone".

Qualora per legge, decisione del produttore o caratteristiche tecniche proprie, una intelligenza artificiale non possa essere classificata come agente-robot, la sua

---

[50] Cfr. Progetto di Relazione 2015/2103(INL), art. 31, lett. *f*

[51] il *civil turnover*, nelle società sovietiche, comprende quell'insieme di fatti giuridicamente rilevanti (atti amministrativi, transazioni, atti che costituiscono diritti) e le relazioni giuridiche che ne scaturiscono, in virtù delle quali la proprietà è trasferita da un soggetto (cittadini e persone giuridiche) ad un altro.
Cfr. *The Great Soviet Encyclopedia, 3rd Edition*. S.v. "Civil Turnover", disponibile pressohttps://encyclopedia2.thefreedictionary.com/Civil+Turnover (ultimo accesso 25 settembre 2020).

qualificazione giuridica rimarrà assorbita nell'ambito delle *res*, considerata un semplice, seppur avanzato, prodotto informatico.

In definitiva, le persone elettroniche presentano un qualcosa in più di una persona giuridica, trattandosi di esseri intelligenti che non necessariamente costituiscono il mezzo per il perseguimento di determinati interessi umani (come invece accade per associazioni, società, ecc.), e un qualcosa in meno di una persona fisica, considerata l'impossibilità di equiparare l'ampio spettro di diritti e doveri di cui è titolare l'essere umano a quelli di una macchina.

3. Diritti e doveri delle IA: alcuni esempi.

Le persone elettroniche possono beneficiare di diritti ed essere destinatarie di obblighi giuridici?

La risposta potrebbe essere mutuata riprendendo il discorso già fatto per le persone giuridiche, ossia garantendo alle IA i diritti necessari per l'esercizio della capacità contrattuale e i doveri relativi alla responsabilità, quanto meno in sede civile, delle proprie azioni. Tuttavia gli enti diventano soggetti di diritto sulla base di un fondamentale presupposto: l'autonomia patrimoniale; si può parlare di personalità giuridica soltanto per quegli enti che non solo hanno un loro patrimonio ma, con quello stesso patrimonio, rispondono delle loro obbligazioni. È necessario quindi stabilire come attribuire autonomia patrimoniale alle IA ed un buon punto di partenza potrebbe essere la produzione di un reddito.

La produzione di reddito è ricollegata allo svolgimento di un qualche tipo di attività lavorativa e allora l'analisi può partire proprio dall'individuare quei settori nei quali si possono già trovare sistemi "lavoratori". Negli ultimi anni diverse tecnologie sono state implementate nell'ambito delle delivery, sostituendo i classici fattorini: si pensi a Starship[52], una compagnia creata nel 2014 che produce *food-delivery* robot completamente a guida autonoma, o ad Amazon, che nel 2016 ha effettuato la sua prima

---

[52] *The self-driving delivery robot*, Starship, disponibile presso https://www.starship.xyz/business/ (ultimo accesso 25 settembre 2020).

consegna con Prime Air, grazie ad un drone completamente autonomo e senza pilota umano[53]. Ancora, nel mondo dei social influencer, si consideri, per fama e non per unicità, l'impatto avuto da *Lil Miquela*, virtual influencer creato grazie alla computer grafica (CGI) a scopi pubblicitari[54] ed apparso su Instagram nel 2016 e che oggi conta più di due milioni e mezzo di *followers*. Non si può parlare propriamente di macchine pensanti, di intelligenza artificiale, ma è bene osservare come si tratti di realtà non futuribili, ma attuali. Se, però, la tecnologia ci consente, ad oggi, di creare robot con caratteristiche antropomorfiche[55] (anche se non si tratta di un requisito essenziale nella loro creazione), IA in grado di apprendere dal mondo che le circonda (vedi Sophia), allora non risulta più cosi implausibile pensare a tali macchine come soggetti attivi, appunto agenti, della società civile, anche in ambito lavorativo. Dunque, ci si può fondatamente prefigurare un prossimo futuro nel quale, anche grazie all'abbassamento dei prezzi di tali tecnologie, un negoziante utilizzerà una intelligenza artificiale per gestire parte dei rapporti economici del proprio negozio. Sorge quindi la domanda se questi robot-agenti possano avere diritto ad una qualche forma di reddito e, da ultimo, avere un patrimonio proprio di cui disporre. Sulla base di questa autonomia patrimoniale, infatti, si potrebbe riconoscere una limitata capacità negoziale, consentendo alle persone elettroniche, per riprendere l'esempio di cui sopra, di stipulare contratti di compravendita ed esercitare la professione all'interno di un negozio.

Ancora, si è posto in tempi recenti un problema di attribuzione di diritti d'autore alle intelligenze artificiali. In via del tutto generale, vengono tutelate dal diritto d'autore le opere letterarie ed artistiche, qualunque ne sia il modo o la forma di espressione[56]. Più nello specifico, vengono tutelate quelle opere c.d. di ingegno che presentino un

---

[53] Amazon Prime Air, Amazon, disponibile presso https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011 (ultimo accesso 25 settembre 2020).

[54] Kaitlyn Tiffany, "*Lil Miquela and the virtual influencer hype, explained*" (Vox, 03 giugno 2019), disponibile presso https://www.vox.com/the-goods/2019/6/3/18647626/instagram-virtual-influencers-lil-miquela-ai-startups (ultimo accesso 25 settembre 2020).

[55] Boston Dynamics. "Parkour Atlas" YouTube video, 0:29. 11 ottobre 2018. https://www.youtube.com/watch?v=LikxFZZO2sk (ultimo accesso 25 settembre 2020).

[56] Cfr. Convenzione di Berna per la protezione delle opere letterarie e artistiche, art. 2, 1)

"carattere creativo"[57], che siano "*original works of authorship*"[58]: il diritto d'autore viene riconosciuto sulla base della condizione fondamentale che l'opera presenti un minimo di originalità oggettiva rispetto a similari opere. Se il requisito di originalità venisse applicato in maniera rigida potrebbe comportare che alcune *narrow AI* (*v. supra* capitolo 1) vedano attribuirsi la titolarità delle loro "opere": si può prendere ad esempio l'IA[59] in grado di creare volti completamente nuovi dal nulla, dove l'intervento umano è ridotto alla compilazione dell'algoritmo e alla immissione di dati, in questo caso milioni di immagini di volti di persone vere. Si tratta, però, di un risultato illogico, tanto è vero che la comunità giuridica conviene nell'individuare l'elemento di originalità e creatività nello sviluppare il software, di modo che l'opera creata dalla IA altro non sarà che un'opera derivata, "un'opera dell'ingegno riconducibile all'intelletto umano dell'autore-programmatore"[60]. Di nuovo il problema si pone se si considera la possibilità di unire le tecnologie ad oggi esistenti: una intelligenza artificiale in grado di scattare foto professionali e in grado di apprendere da ciò che la circonda (ossia capace di apprendere dalle opere di fotografi umani e non), vedrebbe la sua dipendenza dall'uomo notevolmente ridotta; l'uomo ha creato l'intelligenza artificiale dandole capacità di scattare foto con modalità semi professionali, ma è l'IA che ha imparato e migliorato la sua tecnica. A questo punto non sarebbe corretto parlare di opera derivata: diremmo mai che le opere di Giotto debbano essere attribute a Cimabue, considerato quest'ultimo come maestro del primo? Potremmo definire autore di un'opera il rivenditore di pennelli e colori, strumenti senza i quali il pittore non potrebbe creare?

Risulta, invece, più agevole considerare la portata dei doveri. Qualora, infatti, al sistema intelligente fosse garantito un patrimonio, alla disponibilità economica potrebbero essere ricollegati doveri quali l'adempimento alle obbligazioni contratte ovvero doveri

---

[57] Cfr. Art. 2575, comma 1, cod. civ. it.

[58] Cfr. 17 U.S. Code § 102. Subject matter of copyright: In general

[59] StyleGAN2 (Dec 2019) - Karras et al. and Nvidia, in https://thispersondoesnotexist.com

[60] Giovanni Bonomo "Opere dell'ingegno e Intelligenza Artificiale" (ilsole24ore, 17 settembre 2019), disponibile presso https://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2019-09-17/opere-ingegno-e-intelligenza-artificiale-095708.php (ultimo accesso 25 settembre 2020).

di natura fiscale: se le intelligenze artificiali entrassero a far parte della società civile, ed essendo in qualche modo "retribuite", ben potrebbero essere qualificate come soggetti debitori dei tributi.

Alla luce di quanto esposto nelle precedenti pagine, non appare eccessivamente fantascientifico che un robot possa essere dotato di un portfolio, le cui entrate sono determinate dalle attività da esso svolte e le uscite dai doveri poc'anzi esposti. Tuttavia, attribuzioni così simili a quelle umane, richiederebbero un massiccio intervento sia dei legislatori, che si troverebbero a dover rinnovare interi settori del diritto, sia dei governatori, chiamati a revisionare l'assetto socio-economico delle proprie nazioni. L'attribuzione di diritti e doveri dovrebbe quindi essere intesa in solo senso funzionale: anche in assenza di una autonomia patrimoniale, le intelligenze artificiali dovrebbero essere dotate di capacità negoziale, in modo tale che esse possano effettivamente agire all'interno della società civile. Quella che prima si è definita come "attribuzione di reddito" potrebbe essere letta in chiave assicurativa: coloro che intendano avvalersi dell'attività di robot-agenti, saranno chiamati a contribuire a specifici fondi di garanzia o assicurazioni per danni e/o inadempienze dei robot-agenti (*v. infra* capitolo 5). Dal canto loro, le IA sarebbero capaci di rispondere dei doveri e oneri che scaturiscono dalle obbligazioni contratte proprio grazie a quei sistemi assicurativi.

Capitolo Terzo
Principi Regolatori

1. Legislazioni vigenti.

Il settore dell'intelligenza artificiale risulta ancora sprovvisto di un quadro normativo di ampio respiro. A livello nazionale pochi progressi sono stati fatti e, qualora presenti, gli interventi legislativi risultano di marginale importanza. Inoltre, i vari Stati affrontano il problema in maniera fortemente disomogenea: molte nazioni, quali, ad esempio, il Canada, sembrano focalizzate più sul finanziare ricerca e sviluppo delle intelligenze artificiali, che sul predisporre specifici quadri normativi ovvero appositi regolamenti, rimandando a preesistenti corpi normativi (continuando con l'esempio canadese, si fa riferimento alla *Charter of Rights and Freedoms*, *Personal Information Protection and Electronic Documents Act*, o più in generale all'"*existing marketplace framework*"); tali strumenti, tuttavia, già si ritengono poco affidabili nel combattere i grandi colossi della tecnologia, risultando "*largely unsuccessful in holding these companies accountable*"[61]. Per tali ragioni appare opportuno che i vari Stati si muovano verso la predisposizione di corpi normativi che affrontino direttamente il problema; ciò è quanto ha sostenuto Microsoft, proprio uno di quei colossi che operano nel settore, spiegando come "*next-generation policies and laws are needed for next-generation technologies*", in quanto sia i produttori "*are looking for guidelines that will help anticipate potential issues and ensure responsible innovation*" sia i governi "*are eager to remove technology hurdles and encourage the adoption of AI technologies that will promote worker safety, create more jobs, and help national competitiveness*"[62].

---

[61] Jesse Hirsh, "*The Policy Deficit Behind Canadian Artificial Intelligence*", (*Centre for International Governance Innovation*, 13 febbraio 2018), https://www.cigionline.org/articles/policy-deficit-behind-canadian-artificial-intelligence (ultimo accesso 25 settembre 2020).

[62] Greg Shaw, *The Future Computed Ai & Manufacturing* (Microsoft Corporation Redmond, Washington U.S.A. 2019), exec. summary, pagina 15, disponibile online presso https://3er1viui9wo30pkxh1v2nh4w-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/393/2019/06/Microsoft_TheFutureComputed_AI_MFG_Final_Online.pdf (ultimo accesso 25 settembre 2020).

Altri Paesi, quali il Giappone e l'Arabia Saudita (*supra*), hanno accelerato troppo rapidamente l'evoluzione normativa dell'intelligenza artificiale, configurando quest'ultima come titolare di posizioni giuridiche che mal le si adattano, senza aver preliminarmente affrontato fondamentali profili di *governance*.

Altre nazioni stanno studiando il problema con maggiore attenzione, mediante la predisposizione di embrionali strutture legislative oppure l'istituzione di commissioni di lavoro: è il caso della "Grishin Law" (*supra*), proposta di legge presentata nel 2016 al parlamento russo, che fornisce un approccio fortemente innovativo, sia sotto profili di nuove definizioni di "robot" e IA, sia per profili relativi alla responsabilità di queste nuove tecnologie; è il caso, poi, del Regno Unito, dove, nel 2017, è stata istituito una Commissione sull'IA (*AI Commission*) all'interno della *House of Lords*, il cui scopo, ben illustrato da Lord Clement-Jones, *Chairman* del Committee, "*is to understand what opportunities exist for society in the development and use of artificial intelligence, as well as what risks there might be*".

Negli Stati Uniti, i vari legislatori, dei singoli Stati e federale, hanno focalizzato l'attenzione principalmente nel settore dei veicoli a guida autonoma.

Sul piano federale, come si evince dal "*Future of Artificial Intelligence Act of 2017*", particolare attenzione è posta nella istituzione di un "*Federal advisory committee to advise the Secretary on matters relating to the development of artificial intelligence*"[63] e nel ricercare nuove definizioni generali. In realtà, nel Giugno 2016, l'*Office of Science and Technology Policy (OSTP)* della Casa Bianca ha annunciato una *Request for Information* (*RFI*) sull'intelligenza artificiale, alla quale hanno contribuito 161 partecipanti, tra cui accademici e ricercatori, organizzazioni senza scopo di lucro e industrie; in questa sede è emersa una convergenza unanime nel ritener che una regolamentazione ad ampio spettro sarebbe al momento sconsigliabile: "*commenters said that the goals and structure of existing regulations were sufficient, and commenters called for existing regulation to be adapted as necessary to account for the effects of AI.*

---

[63] U.S. Congress, Senate, "*Future of Artificial Intelligence Act of 2017*", S 2217, 115th Cong., 1st sess., introduced in Senate December 12, 2017, disponibile presso https://www.congress.gov/bill/115th-congress/senate-bill/2217/text (ultimo accesso 25 settembre 2020).

For example, commenters suggested that motor vehicle regulation should evolve to account for the anticipated arrival of autonomous vehicles, and that the necessary evolution could be carried out within the current structure of vehicle safety regulation"[64], si legge proprio in un rapporto dell'OSTP.

Guardando invece alla legislazione dei singoli Stati, si può osservare una recente ma rapida crescita di norme e ordini esecutivi: il punto di partenza è da ritrovare nel 2011, quando, per la prima volta, lo Stato del Nevada ha autorizzato "*a fully autonomous vehicle to be tested or operated on a highway within Nevada if certain requirements related to safety are met*"[65]. Da questo momento l'idea di legiferare in materia di veicoli a guida autonoma si è rapidamente diffusa in altri Stati, la maggior parte dei quali si è attivata direttamente con nuove legislazioni (è questo il caso, a livello esemplificativo, della California, con il Senate Bill No. 1298, Chapter 570 del 2012, o della Florida, che, sempre nel 2012, ha autorizzato "*the testing of autonomous vehicles*"[66]); alcuni Stati, invece, hanno operato mediante ordini esecutivi (in particolare i *Governors* in Arizona, Delaware, Hawaii, Idaho, Illinois, Maine, Massachusetts, Minnesota, Ohio, Washington e Wisconsin[67]).

Da ultimo, anche in Germania, con il *German Traffic Act* si è prestata, come nel caso americano, specifica attenzione alle intelligenze artificiali presenti nelle auto a giuda autonoma; tuttavia, l'innovazione tedesca non è stata nel senso di autorizzare la

---

[64] U.S. Executive Office of the President - National Science and Technology Council - Committee on Technology: "*Preparing for the Future of Artificial Intelligence*" (Office of Science and Technology Policy, Ottobre 2016), disponibile online presso https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (ultimo accesso 25 settembre 2020).

[65] Jann Stinnesbeck, Research Division Legislative Counsel Bureau, "*Research Brief On Autonomous Vehicles*" (Novembre 2017), disponibile online presso https://www.leg.state.nv.us/Division/Research/Publications/ResearchBriefs/AutonomousVehicles.pdf (ultimo accesso 25 settembre 2020).

[66] Julie L. Jones, "*Autonomous Vehicle Report*" (pp. 1-7, Rep. No. #13-008, 2014), disponibile presso https://www.flhsmv.gov/html/HSMVAutonomousVehicleReport2014.pdf (ultimo accesso 25 settembre 2020).

[67] Dati Forniti dalla *National Conference on State Legislatures*, disponibile presso https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx (ultimo accesso 25 settembre 2020).

circolazione in *testing* di tali veicoli, bensì di introdurre specifiche modifiche al *corpus* di norme che regolano la responsabilità per incidenti stradali.

Da questa analisi si può dedurre che le preoccupazioni delle varie nazioni si siano concentrate o sul finanziare lo sviluppo della tecnologia o, tuttalpiù, a regolare quegli aspetti giuridici maggiormente colpiti dall'innovazione tecnologica. In questo contesto sembra invece, che l'Unione Europea stia tendando un approccio differente, prestando maggiore attenzione ai profili di *governance* dell'IA. In quest'ottica si pone la risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, norma di vasta portata, che investe una molteplicità di aspetti, quali questioni di responsabilità, problemi etici, regole di condotta per sviluppatori, produttori ed operatori nel campo della robotica. Proprio nella sezione "Principi etici", si pone l'accento su come "l'attuale quadro giuridico dell'Unione debba essere aggiornato e integrato", ritenendosi altresì necessario "un quadro etico di orientamento chiaro, rigoroso ed efficiente per lo sviluppo, la progettazione, la produzione, l'uso e la modifica dei robot"[68].

Deve quindi essere l'Europa il vero punto di partenza nella ricerca di quelli che sono possibili principi regolatori di questa scienza e questo perché "*Europe recognizes that governance innovation has to keep up with technology innovation. It seems like common sense: as the economy is transformed by AI, the regulatory environment must keep up*"[69]. Le varie organizzazioni internazionali operanti sul territorio europeo (in particolare il Consiglio d'Europa), l'Unione Europea stessa, e, per certi aspetti, i singoli Stati con i loro esperti, hanno infatti concentrato la loro attenzione sulla ricerca di alcuni punti chiave, necessari per un responsabile sviluppo delle intelligenze artificiali.

Tra le molteplici carte e rapporti governativi, ritengo che la migliore classificazione, per esaustività e autorevolezza, sia quella proposta dalla *European Commission For The Efficiency Of Justice* (in seguito, CEPEJ); tale classificazione, infatti, si caratterizza, da una parte, per utilizzare espressioni e concetti tecnico-giuridiche e, dall'altra, per la

---

[68] Cfr. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (doc. P8_TA(2017)0051)

[69] *op. cit.* Jesse Hirsh, "*The Policy Deficit Behind Canadian Artificial Intelligence*".

brevità, poiché racchiude in cinque soli principi le linee guida necessarie per regolamentare le IA.

Nel dicembre del 2018, la CEPEJ ha redatto la "Carta Etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi" (d'ora in avanti "Carta Etica") che, sebbene realizzata tenendo a mente principalmente l'impatto delle IA nei sistemi giudiziari, individua cinque principi cardine che possono essere estesi a tutti gli ambiti di applicazione di tale tecnologia: principio del rispetto dei diritti fondamentali; principio di non-discriminazione; principio di qualità e sicurezza; principio di trasparenza, imparzialità ed equità; principio del "under user control".

Nell'analizzare questi principi farò comunque riferimento ad ulteriori documenti, in modo tale da meglio integrare quanto proposto dalla CEPEJ; in particolare saranno presi in considerazione i seguenti documenti:

- Principi di Asilomar, sviluppati dal *Future of Life Institute* durante la conferenza di Asilomar del 2017 (d'ora in avanti "Asilomar");
- *Montreal Declaration for Responsible AI* del 2017 (d'ora in avanti "Montreal");
- *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, pubblicato dallo *European Group on Ethics in Science and New Technologies* nel 2018 (d'ora in avanti "EGE");
- "*Five overarching principles for an AI code*", presenti nel paragrafo 417 dello nel report sull'intelligenza artificiale della House of Lords, *AI in the UK: ready, willing and able?*, pubblicato nel 2018 (d'ora in avanti "AIUK");
- Orientamenti Etici per un'IA affidabile, sviluppati dal Gruppo di Esperti ad alto livello sull'intelligenza artificiale e pubblicati nel 2019 (d'ora in avanti "Gruppo di Esperti");
- Statuto Etico e Giuridico dell'IA, elaborato dalla Fondazione Leonardo nel 2019 (d'ora in avanti "Statuto");
- *For a Meaningful Artificial Intelligence*, del matematico e membro del parlamento francese Cédric Villani, pubblicato nel 2018 (d'ora in avanti "Villani").

Tuttavia, prima ancora di esaminare i suddetti cinque principi, risulta d'obbligo soffermarsi sulle prime, vere "fonti normative" governatrici della robotica, sviluppate da Isaac Asimov.

2. Le leggi di Asimov.

Quando ancora il tema dei robot e dell'intelligenza artificiale era pura fantascienza, già si avvertiva la necessità di delineare talune regole di base per una buona "convivenza" fra macchine e umanità. Era il 1942 quando Isaac Asimov, scrittore americano e professore di biochimica all'università di Boston, pubblico sulla rivista di fantascienza "*Analog Science Fiction and Fact*" il racconto "*Runaround*". Senza soffermarsi in maniera approfondita sull'aspetto narrativo del racconto, preme qui evidenziare come si tratti del primo lavoro nel quale vengono enunciate le tre, originali, leggi della robotica: "*One, a robot may not injure a human being, or, through inaction, allow a human being to come to harm*"; "*Two* […] *a robot must obey the orders given it by human beings except where such orders would conflict with the First Law*"; "*three, a robot must protect its own existence as long as such protection does not conflict with the First or Second Laws*"[70]. A queste tre, Asimov stesso ne accosta una quarta, "*the zeroth law*"[71], secondo cui "*the prevention of harm to human beings in groups and to humanity as a whole comes before the prevention of harm to any specific individual*"[72].

Sebbene siano inserito in un contesto romanzesco, le quattro leggi hanno raggiunto nel tempo una fama e un'importanza tali da formare le basi per un'etica della robotica e della intelligenza artificiale; diversi sono i rimandi a tali principi, soprattutto in documenti ufficiali, tanto in forma esplicita, che implicita.

Un esplicito rimando ad Asimov si può trovare nella già citata Risoluzione del Parlamento europeo, dove le quattro leggi vengono in considerazione come vere e proprie norme, in particolare modo "rivolte ai progettisti, ai fabbricanti e agli utilizzatori di robot, compresi i robot con capacità di autonomia e di autoapprendimento integrate, dal momento che tali leggi non possono essere convertite in codice

---

[70] Isaac Asimov, "*Runaround*", in *I, Robot* (pp. 20-34), (NY, NY: The New American Library., 1956).

[71] L'utilizzo di tale nomenclatura vuole evidenziare come le leggi recanti un numero minore superino, per importanza, quelle con numero maggiore.

[72] Isaac Asimov, "*The Zeroth Law*", in *Robots and empire*. (Garden City, NY: Doubleday, 1985).

macchina”[73]. La stessa risoluzione appare, in alcuni tratti, estrapolare i concetti contenuti nelle leggi di Asimov, e riorganizzarli al fine di ricostruire principi generali: nella sezione “Principi generali riguardanti lo sviluppo della robotica e dell'intelligenza artificiale per uso civile”, numero 3, il nucleo essenziale del periodo "ritiene che sia fondamentale, nello sviluppo della robotica e dell'intelligenza artificiale, garantire che gli uomini mantengano in qualsiasi momento il controllo sulle macchine intelligenti”[74] ricalca proprio la seconda legge della robotica; ancora, nella sezione “Principi etici”, numero 13, laddove nel sottolineare “che il quadro etico di orientamento dovrebbe essere basato sui principi di beneficenza, non maleficenza”[75], la risoluzione sembra ispirarsi alla prima legge.

Gli stessi principi presenti nella “Carta Etica”, possono essere interpretati in chiave delle leggi di Asimov. Estendendo il significato letterale di queste ultime, infatti, si possono trovare delle similarità: se il concetto di “*harm*”, presente nella prima legge, viene inteso non solo come danno fisico, ma anche come danno morale, allora si può affermare che le intelligenze artificiali non debbano violare i diritti fondamentali dell’uomo; dando la stessa accezione di danno morale a “*the prevention of harm to human beings in groups*”, presente nella *zeroth law*, si mette in evidenza il principio di non discriminazione fra gruppi diversi di esseri umani; da ultimo, richiedere che l’essere umano mantenga sempre un “*user control*” sull’IA, può essere ricondotto al requisito che “*a robot must obey the orders given it by human beings*” espresso nella prima legge.

3. Principio del rispetto dei diritti fondamentali.

La “Carta Etica” redatta dalla CEPEJ, richiede, innanzitutto, che venga assicurata “l’elaborazione e l’attuazione di strumenti e servizi di intelligenza artificiale”, compatibilmente con “i diritti fondamentali”; per evitare che un utente finale possa

---

[73] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)) (doc. P8_TA(2017)0051)

[74] *ibid.*

[75] *ibid.*

deviare il funzionamento di una IA, facendola agire contrariamente ai diritti fondamentali, si precisa come debba essere accordata preferenza ad un approccio "*etichal-by-design*"[76].

L'ampia gamma di diritti riconosciuti come fondamentali ed inviolabili dal diritto internazionale ed europeo mal si presta ad un'analisi dettagliata, ma vi è una generale concordanza su alcune "famiglie di diritti fondamentali […] particolarmente pertinenti per quanto riguarda i sistemi di IA"[77]; tali famiglie sono ben riassunte nel principio numero 11 di "Asilomar": "*Human Values: AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity*".

3.1. Dignità umana.

Con "dignità umana" si fa riferimento a quel concetto per cui ogni essere umano ha un suo "valore intrinseco" che non deve essere influenzato da altri; la dignità umana funge da limite per l'autodeterminazione e le azioni di altri uomini. Tale valore intrinseco può essere danneggiato anche dalle IA, per le quali, precisa il "Gruppo di Esperti", "il rispetto per la dignità umana implica che tutte le persone siano trattate con il rispetto loro dovuto in quanto *soggetti* morali, piuttosto che come semplici *oggetti* da vagliare, catalogare, valutare per punteggio, aggregare, condizionare o manipolare". L'EGE riconosce anche come sia necessario predisporre "*(legal) limits to the ways in which people can be led to believe that they are dealing with human beings while in fact they are dealing with algorithms and smart machines*". Da ultimo e secondo lo Statuto Etico, si pongono in contrasto con la dignità umana quelle tecnologie che "manipolano l'utente - anche a fine di bene - o a cui sono delegate decisioni di grande importanza sociale o esistenziale senza che sia possibile comprenderne le dinamiche", risultando

---

[76] La scelta etica non viene lasciata alla libera determinazione dell'utente, ma viene implementata direttamente dal programmatore ed utilizzata durante la fase di primo apprendimento della IA.

[77] Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, "*Orientamenti Etici per un'IA Affidabile*", istituito dalla Commissione europea nel giugno 2018.

imperativo che non vengano diffuse “tecnologie che non colgono il valore intrinseco di ogni individuo dissolvendo la sua particolarità nella generalità di modelli statistici”.

3.2. Libertà individuale.

L’uomo deve essere posto nella condizione di poter autonomamente prendere tutte o la maggior parte delle decisioni importanti che lo riguardano. La forte pervasività che le IA hanno ed avranno sulla società impone qualche cautela: il “Gruppo di Esperti” avverte che “per salvaguardare la libertà individuale occorre ridurre al minimo la coercizione illegittima diretta o indiretta, le minacce all'autonomia mentale e alla salute psichica, la sorveglianza ingiustificata, l'inganno e la manipolazione iniqua”; similmente, in “Montreal”, si specifica che sistemi di IA “*must not be developed or used to impose a particular lifestyle on individuals, whether directly or indirectly, by implementing oppressive surveillance and evaluation or incentive mechanisms*”. In altre parole e come specificato in “EGE”, “*all ‘autonomous’ technologies must, hence, honour the human ability to choose whether, when and how to delegate decisions and actions to them*”.

3.2.1. Privacy.

All’interno dell’ampio concetto di libertà individuale assume particolare importanza la privacy. Per un corretto funzionamento delle intelligenze artificiali i “dati” sono di fondamentale importanza: la macchina ne necessita in fase di progettazione (durante il primo apprendimento) e la sua capacità di apprendimento automatico si basa su ulteriori dati, specificamente quelli percepiti dall’IA. Come conciliare l’esigenza di protezione del *data privacy* con lo sviluppo di questa tecnologia? I principi numero 12 e 13 di “Asilomar” forniscono una prima risposta: da una parte “*people should have the right to access, manage and control the data they generate, given AI systems’ power to analyze and utilize that data*”, dall’altra “*the application of AI to personal data must not unreasonably curtail people’s real or perceived liberty*”. In maniera non dissimile da

quanto avviene oggi, l'essere umano deve essere posto nella condizioni di poter sempre sapere quali e quanti dei suoi dati personali vengono raccolti, per quali fini verranno usati e, se non strettamente necessari, dovrà poter richiedere l'eliminazione di questi dati; qualora ciò non sia possibile, dovranno essere integrati nelle IA sistemi di *encrpytion*.

La *privacy protection* non si esaurisce nel controllo e nella gestione dei dati raccolti, ma assume rilievo anche nella veste di "spazio personale": l'intimità della persona è già oggi minata da sistemi sempre più diffusi e sofisticati di sorveglianza ed un uso improprio delle IA potrebbe solo esasperare preesistenti preoccupazioni. "Montreal" pone l'accento proprio su questo aspetto, evidenziando come "*personal spaces in which people are not subjected to surveillance or digital evaluation must be protected from the intrusion of AIS"* e come, in ultima istanza, "*people must always have the right to digital disconnection in their private lives, and AIS should explicitly offer the option to disconnect at regular intervals, without encouraging people to stay connected*".

3.3. Democrazia e Stato di diritto.

L'impatto che le IA avranno sui processi democratici sicuramente avrà dei risvolti positivi: basti pensare a come persone o intere zone geografiche svantaggiate verranno facilitate alla partecipazione civile. Tuttavia l'ingresso di questi sistemi nei processi democratici, quali i sistemi di voto, fa suonare qualche campanello di allarme: chiarisce, infatti, il "Gruppo di Esperti" che "i sistemi di IA possono sostanzialmente migliorare la portata e l'efficienza della fornitura di beni e servizi pubblici alla società da parte dei governi ma, allo stesso tempo, le applicazioni di IA potrebbero avere effetti negativi sui diritti dei cittadini che dovrebbero essere salvaguardati"; risulta quindi obbligatorio garantire che le intelligenze artificiali non operino "con modalità che compromettano gli impegni di base su cui si fonda lo Stato di diritto".

Peraltro il sistema democratico viene a rilevare anche a priori, cioè prima che una intelligenza artificiale venga introdotta nella società: una tale immissione non può essere incontrollata e non può avvenire senza preliminari verifiche; chiarisce infatti

"Montreal" che "*AIS must meet intelligibility, justifiability, and accessibility criteria, and must be subjected to democratic scrutiny, debate and control*".

3.4. *Human well-being*.

Una intelligenza artificiale deve essere in grado non solo di rispettare i diritti fondamentali dell'uomo, ma anche di promuoverli. La promozione del benessere dell'uomo, del suo *well-being*, è punto chiave della maggior parte dei documenti relativi ai principi-guida per lo sviluppo delle IA. Tanto si evince, ad esempio, in "AIUK" secondo cui le IA "*should be developed for the common good and benefit of humanity*"; in "Montreal", invece, si va oltre il classico antropocentrismo, specificando che "*the development and use of artificial intelligence systems (AIS) must permit the growth of the well-being of all sentient beings*"; ancora, con specifico riferimento alle libertà fondamentali, il "Gruppo di Esperti" auspica che le IA consentano all'uomo di "esercitare un controllo addirittura maggiore sulla propria vita".

L'apprensione per il benessere umano si esprime, in altri autori, nella necessita che le IA siano sostenibili. Nello "Statuto", se da una parte si elogiano i "continui progressi nel campo dell'informatica ed in particolare del *machine learning* e della robotica", grazie ai quali si favorirà "il raggiungimento dei 17 obiettivi di sviluppo sostenibile (SDG) nei prossimi anni", dall'altra si avverte una preoccupazione per quelli che potrebbero essere i costi di realizzazione e di utilizzo di tali tecnologie e, inoltre, di come l'IA possa essere utilizzata ed implementata nei Paesi in Via di Sviluppo. A tal proposito, "Villani" ammonisce che sostenibilità "*does not just mean considering the application of AI in our ecological transition, but rather designing natively ecological AI and using it to tackle the impact of human action on the environment*" e in "EGE" si ribadisce che questa tecnologia "*must be in line with the human responsibility to ensure the basic preconditions for life on our planet, continued prospering for mankind and preservation of a good environment for future generations*".

4. Principio di non-discriminazione.

La “Carta Etica” e “Montreal” concordano nell’individuare il nucleo del principio di non-discriminazione nel “prevenire specificamente lo sviluppo o l'intensificazione di qualsiasi discriminazione tra persone o gruppi di persone”. Tale apprensione diventa particolarmente forte quando l’intelligenza artificiale deve elaborare i c.d. “dati sensibili”, ossia dati che possono riguardare l’origine razziale o etnica, la fede religiosa, le condizioni socio-economiche, le opinioni politiche, l’appartenenza a un sindacato, dati genetici, biometrici e/o sanitari, dati relativi alla vita o all’orientamento sessuale. La vera preoccupazione è che una IA possa, nel suo agire, seguire taluni dei pregiudizi umani; secondo lo “Statuto”, infatti, “i dati rilevati ed utilizzati nei sistemi di *machine learning* dipingono i tessuti sociali incorporandone i relativi pregiudizi. In assenza di specifiche cautele e previsioni, i modelli statistici prodotti cristallizzano e possono amplificare tali *bias*”.

La problematica dei *bias* è stata compiutamente analizzata da Kristian Hammond[78], professore di *Computer Science* e *Journalism* alla Northwestern University, il quale individua cinque possibili fonti di *bias*: *data-driven bias*, *bias through interaction*, *emergent bias*, *similarity bias*, *conflicting goals bias*.

Nel primo caso il pregiudizio deriva dai dati sui quali opera l’IA, in particolare dati incompleti, distorti o errati; un’esempio di questo tipo di errore sono alcuni software sperimentali utilizzati per calcolare la possibilità di recidiva di alcuni condannati: tali IA, basandosi esclusivamente su dati socio-economici e culturali, calcolavano una più alta possibilità di recidiva nelle persone di colore rispetto ai caucasici (*v. infra* capitolo 5).

Nei *bias* di interazione, invece, l’errore/pregiudizio sorge nel momento in cui il software entra in contatto con utenti umani esterni, apprendendo i loro pregiudizi: è questo il caso di “Tay”, chatbot della Microsoft, la quale aveva come obiettivo quello di

---

[78] Krisitian Hammond, "*5 unexpected sources of bias in artificial intelligence*" (10 dicembre 2016), disponibile presso https://techcrunch.com/2016/12/10/5-unexpected-sources-of-bias-in-artificial-intelligence/?guccounter=1 (ultimo accesso 25 settembre 2020).

sostenere conversazioni con giovani americani; tuttavia la rete ha approfittato "delle sue modalità di apprendimento e ingenuità e le ha insegnato messaggi razzisti e xenofobi"[79].
Nel terzo caso, più che di sviluppo di pregiudizi, si può parlare di conservazione di preesistenti convinzioni: il classico esempio è il *news feed* di Facebook, dove le IA raccolgono gli interessi degli utenti, creando raccomandazioni personalizzate per ciascuno di essi; ciò comporta che l'utente non è mai esposto a contenuti diversi, rimanendo chiuso nella sua "bolla" di convinzioni.
Il *similarity bias* ha, allo stesso modo, l'effetto di chiudere l'utente in un "bolla"; a differenza del precedente *bias*, tale effetto non si realizza mediante la raccolta di dati su interessi e raccomandazioni personalizzate: un esempio chiarificatore può essere Google News, nel quale l'algoritmo associa una serie di risultati, notizie, similari alla ricerca effettuata; punti di vista differenti ampliano le capacità di ragionamento, ma se ci si approccia solo a "risultati simili" si rischia di creare un'ulteriore bolla.
Infine, per quanto riguarda l'ultima categoria, si fa riferimento a sistemi disegnati per assolvere a specifiche funzioni che, però, offrono risultati *prejudice-driven*: si pensi ad una IA programmata per suggerire agli utenti eventuali posizioni di lavoro disponibili; qualora un utente donna effettui una ricerca, il sistema prediligerà quei posti vacanti etichettati come "infermiere", piuttosto che come "operatore sanitario" e questo perché si fa leva sull'associazione stereotipata donna-infermiere. L'IA ha apparentemente svolto il suo compito, ma in ultima istanza non fa altro che rafforzare preesistenti pregiudizi.
Al fine di prevenire la creazione di IA discriminatorie, la "Carta Etica" incoraggia "l'utilizzo dell'apprendimento automatico e delle analisi scientifiche multidisciplinari". Il "Gruppo di Esperti" sostiene poi che per una promozione dell'uguaglianza in termini di IA, essa debba "essere il più inclusiva possibile e rappresentare gruppi di popolazione diversi"; l'inclusività della tecnologia deve peró essere rispettata anche dai produttori, i quali dovrebbero essere obbligati a formare team il più rappresentativi possibile, quanto

---

[79] Luisanna Benfatto, "Microsoft blocca il software Tay: Era diventato razzista e xenofobo" (ilsole24ore, 25 marzo 2016), disponibile presso https://st.ilsole24ore.com/art/tecnologie/2016-03-25/microsoft-blocca-software-tay-era-diventato-razzista-e-xenofobo--095134.shtml?refresh_ce=1 (ultimo accesso 25 settembre 2020).

meno per evitare risultati simili a quelli raggiunti con i dispenser di sapone c.d. "razzisti": si tratta, cioè, di dispenser che non riconoscono il palmo della mano di persone di colore, ma solo quello di persone caucasiche[80]. Si argomenta, a tal proposito, che non si sarebbe manifestato questo problema "*if the dispenser's design team had tested the product with black users, or if the design team consisted of racially diverse employees*"[81].

Le soluzioni proposte in "AIUK", paragrafi 114-115-116, sembrano racchiudere quanto detto finora: per contrastare la possibile discriminatorietà delle IA è necessario creare "*more diverse datasets, which fairly reflect the societies and communities which AI systems are increasingly affecting*"; è obbligatorio che lo sviluppo di IA sia promosso da "*diverse workforces*" e con un "*interdisciplinary approach*"; infine è imperativo effettuare "*auditing after the fact, auditing during data processing*" o comunque implementare "*processes that could detect biases*" e creare una apposita certificazione di conformità.

5. Principio di qualità e sicurezza.

Per ogni sistema in grado di apprendere, l'*output*, cioè il risultato, è necessariamente condizionato dai dati che sono stati inseriti come *input*. Qualità e sicurezza debbono riguardare la tipologia dei dati immessi; a tal proposito, la "Carta Etica" sviluppa tale principio nel senso di "utilizzare fonti certificate e dati tangibili con modelli elaborati multidisciplinarmente, in un ambiente tecnologico sicuro". Si è visto nel paragrafo precedente le conseguenze a cui possono portare dei dati "instabili" ed è quindi obbligatorio che essi provengano "da fonti certificate e non dovrebbero essere modificati fino a quando non sono stati effettivamente utilizzati dal meccanismo di apprendimento"; quando si parla di ambiente sicuro, si richiede che l'intero processo di

---

[80] Futureism. "*This 'Racist soap dispenser' at Facebook office does not work for black people*" YouTube video, 1:01. 18 ago. 2017. https://www.youtube.com/watch?v=YJjv_OeiHmo (ultimo accesso 25 settembre 2020).

[81] Victoria Sgarro, "*What Exactly Does It Mean to Call for "Ethics in Design"?*" (13 agosto 2018), disponibile presso https://slate.com/technology/2018/08/ethics-in-design-what-exactly-does-that-mean.html (ultimo accesso 25 settembre 2020).

elaborazione dei dati e primo apprendimento dell'IA debba essere tracciabile, "al fine di garantire che non abbia avuto luogo alcuna modifica in grado di alterare il contenuto o il significato della decisione trattata" (ad esempio per evitare tentativi di *hacking*).

D'altro canto il significato di "sicurezza" può assumere l'ulteriore significato di "IA sicure per l'uomo". Si tratta della c.d. dottrina del "*primum, non nocere*", sulla scorta della quale si ritiene che le emergenti tecnologie autonome non debbano causare danno all'uomo. Grande è, infatti, la preoccupazione internazionale per la creazione di sistemi armati autonomi (LAWS, *lethal autonomous weapons system*), preoccupazione che non differisce molto da quella provata durante la Guerra Fredda per la corsa agli armamenti nucleari. A riprova di ciò, in "EGE" si afferma che "*special attention should also be paid to potential [...] weaponisation of AI*", mentre in "Asilomar" si esplicitamente sostiene che "*an arms race in lethal autonomous weapons should be avoided*".

Sebbene i LAWS al momento risultino ancora una possibilità, piuttosto che una realtà, sembra comunque che gli Stati siano più interessati ad una loro regolamentazione; per quanto argomenti di etica possano essere promossi (un esercito di robot comporterebbe sicuramente una riduzione delle vittime di guerra, quantomeno fra i militari) è ovvio che più appetitoso risulta l'aspetto economico: un esercito robot, per quanto costoso, comporterebbe una spesa minore rispetto ad un esercito umano (considerando che un esercito robot non avrebbe bisogno di pubblicità di recluta, di campi d'addestramento, di provviste, rifornimenti, accampamenti sul terreno di guerra, ecc.).

Purtroppo i vantaggi di un'automazione militare risultano puramente apparenti: svincolate dal peso economico e dalla spesa etica (cioè le vite dei soldati), le diverse Nazioni potrebbero ricorrere a conflitti armati per una qualunque inezia, rendendo tali scontri all'ordine del giorno. È necessario pertanto ascoltare gli esperti del settore[82] ed accedere alla tesi per cui i sistemi di IA debbano essere ispirati a presupposti pacifici e, di conseguenza , impedire lo sviluppo di LAWS.

---

[82] Nel luglio del 2015, durante l'IJCAI-15, la Conferenza Internazionale sull'Intelligenza Artificiale di Buenos Aires, oltre 2000 intellettuali e scienziati, tra cui Stephen Hawking, Elon Musk, Steve Wozniak, Noam Chomsky, il co-fondatore di Skype Jaan Tallinn e il CEO di DeepMind, Google Demis Hassabis, hanno firmato una lettera aperta nella quale ammonivano dei rischi che comporta lo sviluppo di LAWS.

6. Principio di trasparenza, imparzialità ed equità.

Obiettivo di questo principio è "rendere le metodologie di trattamento dei dati accessibili e comprensibili, autorizzare verifiche esterne", cercando un equilibrio fra "l'esigenza di trasparenza, imparzialità ed equità". Così spiega questo principio la "Carta Etica" e, ad eccezion fatta per la "trasparenza", esso presenta notevoli similarità con il principio di non discriminazione. In realtà il precedente principio può essere letto in chiave negativa (come una IA non dovrebbe essere realizzata) mentre imparzialità ed equità possono essere letti in chiave positiva (come realizzare una IA). Infatti, in linea con la finalità di "beneficenza", "Montreal" richiede che "*the development and use of AIS must contribute to the creation of a just and equitable society*" e questo, come si può leggere nello "Statuto", perché "l'IA può diventare una forza attiva per la riduzione delle diseguaglianze, incorporando un concetto di giustizia distributiva che guardi alle categorie marginali come soggetti di intervento prioritari"; ancora in "EGE" viene rimarcato come "*AI should contribute to global justice and equal access to the benefits and advantages that AI, robotics and 'autonomous' systems can bring*". In altre parole l'IA deve essere implementata nella società nella maniera più omogenea possibile, favorendo l'accesso alla tecnologia *in primis* alle categorie più bisognose di essa e avendo come obbiettivo di estendere questo stesso accesso ad ogni singolo o categoria di soggetti.

Veniamo ora al principio di trasparenza, il quale può assumere la duplice veste di trasparenza tecnica e trasparenza decisionale.

Per trasparenza tecnica si accenna alla possibilità che le modalità di realizzazione della IA siano rese pubbliche o comunque facilmente conoscibili, mediante, ad esempio, codici o documentazioni *open source*. Purtroppo, per quanto auspicabile, questa soluzione risulta piuttosto problematica, considerato l'interesse economico che le aziende hanno nel proteggere i propri segreti aziendali. Un diverso approccio potrebbe essere quello di istituire agenzie d'ispezione e predisporre certificazioni *ad hoc,* effettuando un primo *screening* delle IA che vengono immesse nella società; ulteriormente si potrebbe prevedere una data di scadenza della certificazione, di modo

che le IA possano essere sottoposte nuovamente a controllo e, in caso di esito positivo, ottenere una rinnovo della certificazione o, in caso di esito negativo, essere rimosse. Un simile approccio è enfatizzato in "Montreal", dove viene richiesto che "*the code for algorithms, whether public or private, must always be accessible to the relevant public authorities and stakeholders for verification and control purposes*".

Più delicata si presenta la trasparenza decisionale, cioè una totale chiarezza nel processo decisionale operato dalla macchina. Si è, infatti, spesso dimostrato problematico spiegare le modalità decisionali di una IA in maniera comprensibile ad un essere umano. Tale problematica è nota come "*black-box problem*", il quale si sviluppa nel seguente modo: è possibile verificare i dati di *input* ed è possibile osservare il risultato di *output*, ma le operazioni effettuate per arrivare dall'*input* all'*output* risultano parzialmente ignote. Il *black-box problem* si è in realtà affermato in tempi recenti, in particolare con l'introduzione del *Deep Learning*. I tradizionali sistemi intelligenti deduttivi venivano forniti di alcune "regole" predeterminate dal programmatore e che erano alla base del processo di *decision-making*; di conseguenza era sufficiente guardare alla tipologia di regola utilizzata per comprendere come il sistema giungeva ad un determinato *output*. Con l'introduzione del *Deep Learning* le regole non sono più individuate dal programmatore: si è detto infatti nel primo capitolo che il *deep learning* è "apprendimento di dati che non sono forniti dall'uomo, ma sono appresi grazie all'utilizzo di algoritmi di calcolo statistico" (*v. supra* capitolo 1). Per meglio comprendere il problema potrebbe essere utile riprendere l'esempio fornito in "Villani": si consideri un sistema di riconoscimento di immagini; il sistema utilizza come primo *input* immagini fornite dal programmatore e formate da migliaia di pixel; successivamente esso memorizza autonomamente milioni di parametri, per classificare le immagini ricevute. Diventa quindi impossibile seguire il percorso dell'algoritmo di classificazione, che passa attraverso quei milioni di parametri, fino alla sua decisione finale. Sebbene comprendere il funzionamento interno di un sistema di *image recognition* possa risultare futile, bisogna estendere questa problematica: simili sistemi vengono utilizzati dalle banche per concedere prestiti ed in un futuro non lontano potrebbero essere utilizzati in sistemi di giustizia predittiva. Di conseguenza e

prendendo nuovamente in prestito le parole di "Villani", "*in the long term, the accountability of this technology is one of the conditions of its social acceptability: […] as a society, we cannot allow certain important decisions to be taken without explanation*".

7. Principio del "*under user control*".

Il principio della sorveglianza umana è quello che raccoglie il maggior consenso nei vari autori ed esperti, dai quali si evince che l'autonomia delle macchine non deve essere mai assoluta e deve essere sempre presente un certo livello di controllo umano.
In "Asilomar" si propone di lasciare nelle mani umani la scelta di "*how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives*"; più incisivamente, in "AIUK", si legge come "*the autonomous power to hurt, destroy or deceive human beings should never be vested in artificial intelligence*". Ancora, con formula onnicomprensiva, l'Assemblea Parlamentare del Consiglio d'Europa pone l'accento sul bisogno "*for any machine, any robot or any artificial intelligence artefact to remain under human control*"[83].
Altri autori guardano al problema considerando le LAWS, che, come si è accennato prima, sono i sistemi automatici che maggiormente suscitano timore. In "EGE", infatti, si sottolinea come il principio del "*Meaningful Human Control* (MHC)" fu per la prima volta elaborato "*for constraining the development and utilisation of future weapon systems*". In questo ambito, come riportato nello "Statuto", bisogna "preservare l'autonomia e la determinazione umana al fine di garantire sempre il controllo dei meccanismi decisionali autonomi" e che predisporre un simile divieto di produzione ed utilizzo di LAWS, "rispetta gli standard prevalenti di *human-on-the-loop* (HOTL) e *human-in-the-loop* (HITL), secondo cui l'applicazione di sistemi autonomi in ambiti safety-critical deve avvenire sempre sotto la supervisione ed il controllo di un operatore umano".

---

[83] Cfr. Assemblea Parlamentare del Consiglio d'Europa, "T*echnological convergence, artificial intelligence and human rights*", Raccomandazione 2102/2017.

Peraltro, è proprio l'autonomia delle IA il risultato più atteso dalla scienza, risultato che, d'altra parte, si pone in contrasto con un pieno controllo da parte dell'essere umano. Come, quindi, può svilupparsi il rapporto fra macchina e uomo? La teoria del *Meaningful Human Control* (o MHC) ha elaborato diverse modalità di sorveglianza umana, tra le quali vengono in particolare modo a rilevare i già citati *human-in-the-loop* (o HITL) e *human-on-the-loop* (o HOTL), il *human-out-of-the-loop* (o HOOTL) e il *human-in-command* (o HIC).

Iniziamo con l'analisi dell'approccio HOOTL, in quanto si tratta del modello che non prevede alcun rapporto fra uomo e macchina: il sistema è in grado di compiere qualunque decisione in modo autonomo e l'essere umano non è in grado di intervenire. Una configurazione simile al HOOTL era quella presente nella nave da crociera Viking Sky, che si trovava nei mari norvegesi nel marzo del 2019 e, a seguito di alcuni problemi al motore, ha dovuto effettuare una evacuazione d'emergenza. Secondo un'analisi degli ufficiali marittimi norvegesi, il problema è stato causato da una bassa pressione dell'olio: i sensori hanno rilevato bassi livelli di olio e hanno forzato un arresto del motore, arresto apparentemente operato senza alcun intervento umano. Secondo un'interpretazione dell'accaduto da parte del Dr. Lance Eliot, esperto mondiale di IA e *machine learning*, è possibile che il mare fortemente mosso abbia creato degli squilibri nelle taniche dell'olio, facendo scattare i sensori ed è quindi possibile che i livelli dell'olio fossero sufficienti e i motori non dovessero essere forzatamente spenti; se ciò fosse vero, la nave avrebbe potuto proseguire il suo corso, quanto meno fino al porto più vicino, ma la completa autonomia del sistema ha ridotto praticamente a zero la possibilità per il capitano di compiere diverse manovre. Seguendo questa ricostruzione è possibile osservare le drastiche conseguenze a cui un modello HOOTL potrebbe portare, risultando quindi sconsigliabile la produzione di IA con integrato un simile sistema.

In maniera opposta si pone lo *human-in-command*. Secondo questa impostazione, infatti, ogni aspetto del funzionamento delle IA e del loro utilizzo è sottoposto a controllo umano. Sebbene si tratti di un modello più sicuro dell'HOOTL, risulta parimenti inadeguato: l'automazione è proprio l'aspetto più atteso di questa tecnologia,

la componente essenziale per il prossimo step evolutivo dell'uomo; è proprio la sinergia che si andrà a creare fra essere umano e macchina che consentirà questa evoluzione, la quale ultima non ammette che si possa avere il controllo dell'uno sull'altra e viceversa. È, dunque, opportuno abbandonare questi modelli estremi e ricercare la soluzione nel mezzo.

L'approccio HITL, secondo il "Gruppo di Esperti", "prevede la possibilità di intervento umano in ogni ciclo decisionale del sistema". In ambito militare, un esempio di HITL è fornito da "AIUK": si tratta del sistema missilistico US Patriot, il quale presenta un c.d. "periodo di veto", grazie al quale un uomo può eseguire un *override* della decisione (in questo caso il bersaglio da colpire) presa autonomamente. Il sistema HITL prevede quindi una certa autonomia delle IA, che sono in grado di prendere decisioni individualmente, ma che richiedono una autorizzazione per eseguirle. L'essere umano può in questo modo fornire un proprio contributo al processo decisionale, inserendo componenti di intelligenza emotiva, di coscienza e compassione o di guida nel non compiere decisioni seguendo esclusivamente logica e statistica. Il Dr. Eliot, peraltro, evidenzia come questi lati positivi presentino altrettanti lati negativi: gli esseri umani possono compiere scelte sbagliate proprio a causa delle loro emozioni o possono non essere in grado di compiere decisioni con la giusta e necessaria velocità. Ancora, Eliot sottolinea come questi sistemi possano creare delle difficoltà per gli esseri umani stessi, in particolare quando la presenza del modello HITL non sia sufficientemente enfatizzata: negli autoveicoli a guida autonoma si da sempre per scontato che l'uomo debba essere in allerta; tuttavia il grado di attenzione si affievolirà sempre di più man mano che l'intervento umano risulterà meno necessario (in particolare quando si creerà quella convinzione che la macchina sia in grado di rispondere a qualunque difficoltà). A dimostrazione di ciò si può richiamare lo sfortunato incidente avvenuto a Tempe, Arizona, dove un veicolo a guida autonoma di proprietà di Uber stava effettuando un corsa di prova su strada ed ha investito un pedone; il conducente, probabilmente rassicurato dalle capacità del veicolo, non ha prestato la giusta attenzione all'ambiente circostante, tant'è vero che, come si può leggere dal rapporto sull'incidente, ha iniziato

la frenata dopo l'impatto con il pedone[84]. Simili incidenti potrebbero verificarsi quando questa tecnologia sarà alla portata di tutti e, riprendendo le parole di Eliot, "*the automation that is getting better will ironically tease humans into become less attentive to the driving task, in spite of the aspect that the human driver is considered always on-the-hook and responsible for the driving of the car*"[85].

Consideriamo ora l'approccio HOTL, nel quale il ruolo dell'essere umano è quello di un sovrintendente; in particolare, secondo il "Gruppo di Esperti", l'intervento umano è limitato al monitoraggio del sistema stesso. A mio avviso, questo modello non differisce particolarmente dall'approccio proposto dal Dr. Eliot, il c.d. *human-governing-the-loop* o HGTL. I presupposti fra questi due sistemi sono analoghi: si tratta sempre di essere umano che sorveglia una IA. Si pone, però, una domanda: in cosa si differenziano questi ultimi modelli dallo HITL, che sempre prevede una ingerenza umana nell'operato della macchina? Ancora una volta soccorre un utile esempio fornito dal Dr. Eliot: supponiamo vi sia una fabbrica i cui operai sono dei robot che svolgono le loro funzioni autonomamente e che a capo di questa stessa fabbrica vi sia un essere umano; supponiamo, poi, che l'essere umano, il sovrintendente, abbia accesso ad un comando da remoto il quale, una volta attivato, è in grado di disattivare tutti i robot. In questo esempio il sovrintendente non è attivamente coinvolto nel lavoro svolto dai robot, non autorizza ogni loro singola operazione, ma è in grado di disattivare ciascuno di essi qualora sia necessario. In ciò risiede la differenza, nel grado di interferenza che l'uomo ha sulla macchina: nello HITL l'interferenza è massima, la macchina non può mai agire in assenza di uno specifico ordine dell'uomo; nello HGTL la macchina ha una ampia autonomia nel compiere le sue attività, ma non possiede una autonomia assoluta, in quanto vi è sempre la possibilità di un intervento umano. Parlare di *human-in-the-loop*

---

[84] Preliminary Report Highway HWY18MH010, National Transportation Safety Board, disponibile presso https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf (ultimo accesso 25 settembre 2020).

[85] Lance Eliot, "*Human In-The-Loop Vs. Out-of-The-Loop in AI Systems: The Case of AI Self-Driving Cars*" (08 aprile 2019), disponibile presso https://www.aitrends.com/ai-insider/human-in-the-loop-vs-out-of-the-loop-in-ai-systems-the-case-of-ai-self-driving-cars/ (ultimo accesso 25 settembre 2020).

per il manager della fabbrica, sempre secondo Eliot, "*is somewhat misleading due to the omnipresent role that this human has*"[86].

Conclusa l'analisi delle varie modalità di sorveglianza umana, ritengo che l'opzione preferibile sia quella proposta da Eliot: come precedentemente anticipato, un eccessivo controllo umano sull'operato delle macchine rallenterebbe irragionevolmente lo sviluppo di questa tecnologia, mentre lasciare le intelligenze artificiali completamente libere condurrebbe a potenziali scenari distopici. Per citare Cicerone, "*in omnibus fere rebus mediocritatem esse optumam*": la via di mezzo, in questo caso, è garantire una più o meno ampia autonomia alle IA, ma fare in modo che l'essere umano abbia sempre una posizione di supremazia, capace in qualunque momento di disattivare la macchina. Tale posizione di supremazia potrebbe essere garantita o ad agenzie governative o ad enti indipendenti appositamente istituiti per controllare, certificare e monitorare le IA che vengono di volta in volta introdotte.

[86] *ibid.*

Capitolo Quarto
Prospettive di Attribuzione di Responsabilità

1. Robot-oggetti o robot-agenti?

Un chatbot esterna dichiarazioni che possono risultare denigratorie e lesive della reputazione di una persona; un LAWS (*v. supra* cap. 3, par. 5, pag. 40) ferisce civili innocenti; un'auto a guida autonoma urta un altro veicolo provocando un incidente. Questi accadimenti sono frutto dell'agire di intelligenze artificiali; si tratta di "azioni" che, se commesse da un essere umano, assumerebbero rilevanza nell'ordinamento giuridico sia nel diritto civile sia nel diritto penale. Sussiste e, se sì, quale è la differenza fra un evento causato da una IA ed uno causato da un uomo?

Per poter rispondere a questo quesito è opportuno comprendere le diverse modalità di interazione che tale tecnologia ha e può potenzialmente avere con l'ambiente esterno e con l'uomo.

Possiamo parlare di interazione "forte" quando l'intelligenza artificiale è fisicamente presente nella realtà quotidiana ed opera a stretto contatto con l'uomo ovvero con IA incorporate in hardware, quali possono essere i veicoli a guida autonoma o, ancora di più, i robot. Laddove l'interazione sia meramente digitale ("interazione debole"), difficilmente potremmo parlare di "azioni elettroniche". Una "interazione debole" si realizza principalmente con IA software (es. gli odierni assistenti vocali)

Nei precedenti capitoli il concetto di intelligenza artificiale è stato più volte assimilato a quello di robot. Tuttavia, una effettiva equiparazione è possibile solo per particolari categorie di robot. È utile, quindi, prendere le mosse da una classificazione di questi robot, in particolare rifacendosi al Glossario Tecnico redatto dagli esperti della *Strategic*

Research Agenda (SRA) for Robotics in Europe[87]. Secondo tale glossario è possibile racchiudere i vari robot in tre macro-categorie:

- Robot tele-operati: sono composti da un set di parti mosse da motori controllati da persone fisiche tramite specifiche interfacce, come un *joy-stick* o anche uno *smartphone*. Essi possono essere definiti come meri strumenti nelle mani di un operatore, poiché le loro azioni sono completamente controllate dall'uomo.
- Robot autonomi: l'autonomia si estrinseca nella capacità di svolgere un compito senza nessun intervento umano durante il processo. L'autonomia, secondo il Glossario Tecnico SRA, comprende anche la capacità di valutare una possibile auto-attivazione e di decidere come comportarsi di conseguenza. Il livello di autonomia dipende dal livello di intervento umano necessario per il compimento dell'azione.
- Robot cognitivi: sono dotati di sistemi che garantiscono loro abilità quali il ragionamento, la percezione. la pianificazione e l'apprendimento basato su una rappresentazione interna del mondo esterno, in maniera non dissimile dai processi mentali umani e animali. Tali capacità cognitive consento al robot di adattarsi anche a un ambiente parzialmente sconosciuto e mutevole.

A ben vedere, le differenze fra robot autonomi e robot cognitivi sono piuttosto sfumate, tant'è vero che generalmente un robot con elevati livelli di autonomia è anche cognitivo; nonostante questo, le due categorie possono essere tenute distinte perché è comunque possibile che esista un robot autonomo non cognitivo: sempre secondo l'esempio fornito nel Glossario Tecnico, ciò può accadere per robot che sono in grado di percepire l'ambiente circostante, senza essere capaci di adattarsi ad esso

Maggiore rilevanza potrebbe avere la distinzione fra robot "automatico" e robot "autonomo": con il primo si fa riferimento ad un automa con capacità di reagire sulla scorta di dati forniti da determinati sensori, mentre con il secondo si indica la capacità

---

[87] Il Glossario tecnico è reperibile presso https://www.eu-robotics.net/cms/front_content.php (ultimo accesso 25 settembre 2020). Cfr. anche Laura Coppini, "*Robotica e intelligenza artificiale: questioni di responsabilità civile*", in Politica del diritto, Rivista trimestrale di cultura giuridica fondata e diretta da Stefano Rodota' 4/2018, pp. 713-740; Amedeo Santosuosso, Chiara Boscarato, Franco Caroleo, "*Robot e diritto: una prima ricognizione*", in NGCC, luglio-agosto 2012, pp. 1-24.

supplementare di elaborare da sé l'ambiente esterno; nel primo caso vi è semplice reazione, nel secondo è presente il ragionamento.

Sulla scorta di quanto appena detto, consideriamo ora quando intelligenza artificiale e robot possono essere considerati un *unicum*: ciò si verifica, in particolare, per i robot autonomi e cognitivi, mentre nei robot tele-operati l'intelligenza artificiale è perlopiù assente.

Il particolare interesse mostrato dalle varie istituzioni per gli sviluppi di questa tecnologia, fa riflettere sulla concreta possibilità di trovarsi di fronte a nuove applicazioni di queste tecnologie: come sottolinea la professoressa Lilian Edwards, esperta di diritto e di proprietà intellettuale, "*robots are something different from ordinary "machines" or tools or software. First, they have a degree of mobility and/or autonomy. This implies a degree of sometimes threatening out of control-ness. Second, they mostly have capacity to learn and adapt. This has really interesting consequences for legal liability*"[88].

Se quindi tradizionalmente i robot e le IA sono considerati come "oggetti" (prodotti), ad oggi questa categorizzazione vacilla: ad uno stadio più evoluto i robot, in particolare quelli autonomi e cognitivi, considerata la loro capacità di agire nell'ambiente in cui sono immersi, possono e debbono essere classificati come "agenti"con inevitabili implicazioni giuridiche correlate alla responsabilità per le loro azioni.

2. Il robot "agente".

Riprendiamo l'esempio proposto nel precedente capitolo di un negoziante che decida di "assumere" una intelligenza artificiale per gestire i rapporti commerciali del proprio negozio; consideriamo, poi, che il ruolo dell'entità digitale sia quello di "commesso". In questo nostro esempio l'IA (che presumibilmente si manifesta come robot, se si parla di assistente fisico, o come bot, se si parla di assistente digitale) assumerebbe una particolare posizione giuridica, quella di c.d. "commesso di negozio", collaboratore

---

[88] Lillian Edwards, "*Edwards' Three Laws for Roboticists*" [Web log post, 01 ottobre 2010]. Disponibile presso http://blogscript.blogspot.com/2010/10/edwards-three-laws-for-roboticists.html (ultimo accesso 25 settembre 2020).

dell'imprenditore a cui sono affidate determinate mansioni che lo pongono in contatto con terzi.

Nell'ordinamento italiano, la figura del commesso è ricompresa nella disciplina della c.d. "rappresentanza commerciale": si tratta di un *corpus* di norme che disciplina gli atti posti in essere da specifici ausiliari interni dell'imprenditore (institore, procuratore e commesso). Il commesso può compiere tutti gli atti che ordinariamente comporta la specie di operazioni di cui è incaricato[89], tra i quali rientrano quelli di compravendita. Il commesso, infatti, gode della capacità di stipulare contratti in nome e per conto dell'imprenditore. La sua attività, però, ricomprende solo mansioni di carattere esecutivo, essendogli preclusa ogni partecipazione alla determinazione del contratto (egli non può, ad esempio, introdurre clausole che determinino deviazione dalla disciplina del tipo contrattuale[90]).

Negli ordinamenti di *common law*, sebbene manchino "norme sulla rappresentanza commerciale, cioè norme simili agli artt. 2204 e 2210"[91], la figura del commesso rientra nella disciplina generale della *agency law*, è una specifica tipologia di *agent* (il c.d. *servant* o, con terminologia di più comune uso, un *employee*), il quale, al pari di quanto avviene in Italia, agisce in nome e per conto del "rappresentato"[92]. In common law, infatti, un *agent* è una persona "*who acts in the name of and on behalf of another, having been given and assumed some degree of authority to do so*"[93].

Se le mansioni di cui si è appena detto fossero svolte da una intelligenza artificiale, allora verrebbe nuovamente a rilevare il termine "robot-agente", ma vestito di un

---

89 Cfr. Art. 2210, comma 1, cod. civ. it.

90 In tal senso, cfr. Cass. civ., Sez. III, 20 gennaio 1999, n. 484

91 Eliana Morandi, "La rappresentanza di società inglesi", in *L'attività negoziale dello straniero comunitario: casi e materiali*, Atti del Seminario di studio Formanote tenutosi a Verona, 26 settembre 2009, disponibile presso https://elibrary.fondazionenotariato.it/articolo.asp?art=24/2405&mn=3 (ultimo accesso 25 settembre 2020).

92 Cfr. Uniform Commercial Code, Section 3-402(a), "*If a person acting, or purporting to act, as a representative signs an instrument by signing either the name of the represented person or the name of the signer, the represented person is bound by the signature to the same extent the represented person would be bound if the signature were on a simple contract*".

93 Don Mayer, Daniel Warner, George Siedel, Jethro K. Lieberman. "*Business Law and the Legal Environment: Master of Accountancy Edition*" (Flatworld, 2012).

diverso significato: se prima "agente" voleva rappresentare l'agire nella società delle IA (si pensi alle auto a guida autonoma o a droni civili e/o militari), in questo contesto "agente" rappresenta una italianizzazione del termine inglese "*agent*". Un robot-agente costituisce quindi quella manifestazione fisica dell'intelligenza artificiale capace di produrre "*through their own intentional acts, rights and obligations on behalf of humans*"[94].

Quanto appena affermato impone di affrontare la questione di una possibile responsabilità "digitale". In altre parole, e per riprendere la medesima domanda posta da Ugo Pagallo, ex-avvocato e attuale professore di diritto all'università di Torino, "chi paga?"

Nel diritto penale l'individuo autore di un reato, paga il suo debito con la società mediante l'irrogazione di pene detentive o pecuniarie; ; nel diritto civile dei contratti, comportamenti illegittimi sono sanzionati attraverso gli istituti della nullità, l'annullamento, la rescissione o la risoluzione del contratto; infine, nel caso di illecito civile, colui che ha provocato un ingiusto danno è tenuto a risarcirlo. Se in questo contesto si inserisce la voce "IA" emerge la questione del "chi paga" precedentemente posta. Di conseguenza, è necessario affrontare separatamente le sfide legali poste dai robot, considerando il loro diverso impatto nei vari rami del diritto.

3. La fase di realizzazione delle IA: la normativa europea vigente.

Per compiere azioni aventi rilevanza giuridica, un robot deve necessariamente interagire nella vita sociale degli uomini, deve, cioè, operare in quello stesso spazio in cui agiscono gli esseri umani.

L'immissione nella società di queste tecnologie passa, d'altra parte, attraverso una loro messa in commercio; risulta quindi utile rilevare se il mercato dei robot sia già provvisto di un *corpus* giuridico adeguato ed in tal senso possono essere prese in considerazione alcune fonti europee: la Direttiva macchine del 2006, la Direttiva sulla

---

[94] Ugo Pagallo, "*The Laws of Robots Crimes, Contracts, and Torts*" 1st ed. 2013 (Dordrecht: Springer Netherlands, 2013), p. 79.

sicurezza dei prodotti del 2001, la Decisione ed il Regolamento sulla commercializzazione dei prodotti, entrambe del 2008, nonché la Direttiva sulla vendita e garanzia di beni di consumo del 1999 (di cui si tratterà in seguito).

Sebbene si tratti di norme non direttamente riguardanti i robot, la cui applicazione estensiva o analogica va comunque verificata, esse possono essere considerate un primo punto di partenza per la ricerca di un quadro normativo disciplinante queste tecnologie. In altre parole e come sostenuto da Amedeo Santosuosso, presidente del Centro di Ricerca Interdipartimentale *European Centre for Law, Science and New Technologies* (ECLT) dell'Università di Pavia, "occorre valutare se le fonti europee vigenti offrano una disciplina adeguata per la produzione e la commercializzazione dei robot nel rispetto delle garanzie di sicurezza pubblica e tutela dei consumatori"[95].

3.1. La Direttiva n. 2006/42/CE.

Lo scopo di tale direttiva è di armonizzare a livello comunitario i requisiti essenziali per la sicurezza e la tutela della salute da rispettare nelle fasi di progettazione e fabbricazione di macchine (qui inteso in senso lato, con riferimento alle categorie di prodotto di cui all'art. 1, par. 1, lett. a) a f)[96]) al fine di migliorarne il livello di sicurezza per l'immissione nel mercato.

Tale direttiva non considera esplicitamente i robot nel suo campo di applicazione, ma ad essi potrebbe applicarsi in via analogica: sulla scorta degli artt. 1 e 2, ricaviamo che la presente direttiva si applica alle "macchine"[97] e che con tale termine si identificano quei prodotti con parti o componenti connessi in un insieme, provvisti di elementi mobili,

---

[95] *op. cit.* Amedeo Santosuosso, Chiara Boscarato, Franco Caroleo, *Robot e diritto: una prima ricognizione*, p. 7.

[96] Ian Fraser, *"Guida all'applicazione della direttiva "macchine" 2006/42/CE*" (2ª ed., giugno 2010), Commissione Europea Impresa e Industria, disponibile presso https://ec.europa.eu/docsroom/documents/9202/attachments/1/translations/it/renditions/native (ultimo accesso 25 settembre 2020).

[97] Cfr. Dir. 2006/42/CE art. 1: "La presente direttiva si applica ai seguenti prodotti: a) macchine; b) attrezzature intercambiabili; c) componenti di sicurezza; d) accessori di sollevamento; e) catene, funi e cinghie; f) dispositivi amovibili di trasmissione meccanica; g) quasi-macchine".

alimentati da una qualunque fonte di energia diversa da quella animale o umana ed utilizzati per una applicazione ben determinata[98].

Se un prodotto ricade nella sfera della direttiva "macchine", prima di poterlo immettere nel mercato, sorgono alcuni obblighi in campo ai produttori o loro rappresentanti autorizzati: sulla scorta di quanto disposto dall'art. 5, il fabbricante deve innanzitutto verificare che il prodotto soddisfi i requisiti di sicurezza illustrati nell'allegato I alla direttiva (a livello esemplificativo: sicurezza e affidabilità dei sistemi di comando, attivazione ed arresto; utilizzo di materiali per la realizzazione privi di rischi; assenza di rischi nell'utilizzo della macchina, sia in caso di uso corretto che di prevedibile uso scorretto); deve, poi, espletare le procedura di valutazione della conformità delle macchine, con cui assicura e dichiara che la macchina soddisfa i requisiti della direttiva, ed elaborare un fascicolo tecnico che dimostri la conformità della macchina ai requisiti della direttiva, che dovrà essere messo a disposizione delle autorità competenti degli Stati membri per almeno 10 anni; redigere, infine, la dichiarazione CE di conformità (che contiene informazioni generali sul fabbricante, il soggetto adibito alla elaborazione del fascicolo e degli altri organismi che effettuano le verifiche di conformità ed informazioni generali sulla macchina).

Da ultimo il fabbricante è abilitato ad apporre il marchio CE ai sensi dell'art. 16. L'apposizione del marchio è di fondamentale importanza, poiché è solo da questo momento che il fabbricante "accetta di assumersi la responsabilità della conformità del prodotto"[99].

---

[98] Cfr. Dir. 2006/42/CE art. 2: "macchina»: — insieme equipaggiato o destinato ad essere equipaggiato di un sistema di azionamento diverso dalla forza umana o animale diretta, composto di parti o di componenti, di cui almeno uno mobile, collegati tra loro solidamente per un'applicazione ben determinata; — insieme di cui al primo trattino, al quale mancano solamente elementi di collegamento al sito di impiego o di allacciamento alle fonti di energia e di movimento; — insieme di cui al primo e al secondo trattino, pronto per essere installato e che può funzionare solo dopo essere stato montato su un mezzo di trasporto o installato in un edificio o in una costruzione; — insiemi di macchine, di cui al primo, al secondo e al terzo trattino, o di quasi-macchine, di cui alla lettera g), che per raggiungere uno stesso risultato sono disposti e comandati in modo da avere un funzionamento solidale; — insieme di parti o di componenti, di cui almeno uno mobile, collegati tra loro solidalmente e destinati al sollevamento di pesi e la cui unica fonte di energia è la forza umana diretta".
E cfr. *op. cit.* Ian Fraser, *Guida all'applicazione della direttiva "macchine" 2006/42/CE*.

[99] *Op. cit.* Ian Fraser, *Guida all'applicazione della direttiva "macchine" 2006/42/CE*.

L'inclusione dei robot nella categoria delle macchine o in quella delle quasi-macchine ("prodotti destinati a costituire una macchina disciplinata dalla direttiva dopo l'incorporazione"[100]), consentirebbe di estendere le disposizioni richiamate anche per la fabbricazione e commercializzazione di robot.

3.2. La Direttiva n. 01/95/CE.

La direttiva sulla sicurezza generale dei prodotti (o DSGP) costituisce una *lex generalis* rispetto alla precedente direttiva "macchine"; pertanto, quand'anche non si volessero assimilare i robot alle macchine o quasi macchine, comunque saranno sottoposti alla disciplina di tale direttiva, parimenti volta a garantire la sicurezza dei prodotti immessi sul mercato[101].

La possibile applicazione di questa disciplina alle varie manifestazioni dell'intelligenza artificiale si ricava dalle definizioni poste nell'art. 2, lett. a): per "prodotto" si intende un qualsiasi prodotto destinato ai consumatori o suscettibile di essere utilizzato dai consumatori, anche se non loro destinato, fornito o reso disponibile a titolo oneroso o gratuito nell'ambito di un'attività commerciale. Tale definizione ricomprende sia i robot (prodotto destinato al consumatore) sia quelle espressioni digitali delle IA meramente software, quali chatbot o assistenti vocali (prodotto utilizzato dal consumatore, ma non a lui destinato[102]).

Per quanto concerne la sicurezza del prodotto, da un lato l'art. 2, lett. b) definisce "prodotto sicuro" qualsiasi prodotto che "in condizioni di uso normali o ragionevolmente prevedibili […] non presenti alcun rischio oppure presenti unicamente rischi minimi, compatibili con l'impiego del prodotto e considerati accettabili". In

---

[100] *ibid.*

[101] Cfr. Dir. 2001/95/CE art. 1, par. 1: "La presente direttiva è intesa a garantire che i prodotti immessi sul mercato siano sicuri."

[102] È questo il caso dei chatbot presenti nella maggior parte dei siti web delle imprese: assistenti virtuali che hanno lo scopo di comunicare e fornire informazioni al consumatore, ma che non sono di sua proprietà.
È, ancora, il caso degli assistenti vocali presenti nei moderni smartphone: titolare della proprietà dell'intelligenza artificiale è sempre l'azienda che la produce, ma è destinata all'utilizzo da parte del consumatore.

ossequio al principio *lex specialis derogat generali*, la DSGP non si applica qualora vi siano disposizioni comunitarie specifiche sulla sicurezza dei prodotti (come può essere la direttiva "macchine"); in assenza di specifiche disposizioni comunitarie, un prodotto è sicuro quando è conforme alle normative nazionali specifiche dello Stato membro nel cui territorio è commercializzato[103].

Gli obblighi dei produttori o fornitori - il cui mancato rispetto è fonte di responsabilità - sono contenuti nell'art. 5 e riguardano, in primo luogo, l'impossibilità di immettere nel mercato prodotti che non rispettano il requisito generale di sicurezza; sono presenti, poi, obblighi di informazione al consumatore circa i rischi inerenti l'utilizzo del prodotto e obblighi di comunicazione alle autorità competenti qualora essi ritengano, sulla base delle informazioni di cui sono in possesso o di cui dovrebbero essere in possesso, che un prodotto immesso nel mercato non sia più compatibile con l'obbligo generale di sicurezza.

Specularmente, per gli Stati Membri vige, tra l'altro, l'obbligo espresso nell'art. 6 di "istituire o nominare le autorità competenti preposte al controllo della conformità dei prodotti con l'obbligo generale di sicurezza".

3.3. La Decisione n. 768/2008/CE e il Regolamento n. 765/2008/CE.

La Decisione 768/2008 funge da quadro generale e comune per la commercializzazione dei prodotti. La sua importanza risiede nell'apporre alcune fondamentali definizioni e nell'identificare alcuni obblighi per gli operatori economici.

In particolare vengono definiti come "operatore economico" il fabbricante, il rappresentante autorizzato, l'importatore e il distributore, mentre per "immissione nel mercato" si intende la prima messa a disposizione di un prodotto sul mercato comunitario[104].

---

[103] Cfr. Dir. 2001/95/CE art. 3, par. 2: "Un prodotto è considerato sicuro, per quanto concerne gli aspetti disciplinati dalla pertinente normativa nazionale, quando in mancanza di disposizioni comunitarie specifiche che ne disciplinano la sicurezza, è conforme alle normative nazionali specifiche dello Stato membro nel cui territorio è commercializzato".

[104] Cfr. Decisione 768/2008/CE, Allegato I, art. R1.

Tali definizioni assumono rilevanza per l'attribuzione di responsabilità: in particolare, secondo l'art. 1, all'atto dell'immissione gli operatori economici, in funzione dei loro rispettivi ruoli, sono responsabili della conformità dei loro prodotti e si assumono la responsabilità di garantire che le informazioni ad essi relative ai prodotti siano accurate e complete. Più nello specifico, il fabbricante, all'atto dell'immissione del prodotto sul mercato, garantisce che esso sia stato progettato e fabbricato conformemente alla normativa di riferimento; qualora sorga il dubbio che il prodotto già immesso non abbia i requisiti di conformità, il fabbricante è obbligato a ritirarlo e, qualora esso presenti un rischio, deve informare immediatamente le autorità nazionali competenti[105]. La conformità dei prodotti alla normativa dovrà essere effettuata sulla base delle procedure di valutazione contenute nell'Allegato II (tra le quali, a livello esemplificativo, rientrano il controllo interno, il controllo interno unito a prove ufficiali, il controllo interno unito a controlli ufficiali effettuati a intervalli casuali, conformità fornita dalla garanzia della qualità fornita dall'ispezione e dalla prova del prodotto finale). Il distributore, dal canto suo, deve verificare che il prodotto rechi la marcatura o le marcature di conformità e, mentre il prodotto è sotto la sua responsabilità, deve garantire che le condizioni di immagazzinamento o di trasporto non mettano a rischio la conformità del prodotto[106].

Il Regolamento 765/2008 integra quanto disposto dalla Decisione, stabilendo norme riguardanti l'organizzazione e il funzionamento dell'accreditamento degli organismi di valutazione della conformità[107]. Il Regolamento definisce l'accreditamento come "attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare".

La disciplina contenuta nel regolamento è per lo più rivolta agli Stati membri, ai quali è richiesto di istituire un unico organismo di accreditamento, che avrà il compito di

---

[105] Cfr. Decisione 768/2008/CE, Allegato I, art. R2, par. 1 e 8.

[106] Cfr. Decisione 768/2008/CE, Allegato I, art. R5.

[107] Cfr. Regolamento 765/2008/CE, art. 1, par. 1: "Il presente regolamento stabilisce norme riguardanti l'organizzazione e il funzionamento dell'accreditamento degli organismi di valutazione della conformità nello svolgimento di attività di valutazione della conformità".

valutare se un organismo di valutazione della conformità sia competente a svolgere la sua attività[108].

Gli Stati Membri, secondo quanto stabilito dall'art. 18, hanno l'obbligo di istituire meccanismi di coordinamento e comunicazioni tra le varie autorità che vigilano sui propri mercati nonché di istituire procedure per dare seguito ai reclami, per monitorare gli eventuali infortuni e danni alla salute provocati dai prodotti non conformi e per seguire gli sviluppi scientifici e tecnici in materia di sicurezza.

3.4. Aspetti critici della normativa europea.

Conclusa l'analisi delle fonti europee in materia di sicurezza e immissione nel mercato dei prodotti, si può affermare che tale normativa sia applicabile anche alle intelligenze artificiali. I robot e le IA, prima ancora di agire nello stesso contesto degli uomini, devono essere prodotti: in questa fase l'intero *corpus* di regole predisposto dalla direttiva n. 01/95/CE, dalla decisione n. 768/2008/CE e dal reg. n. 765/2008/CE garantisce comunque una tutela generale per questi peculiari prodotti; una tutela poi in parte approfondita dalla normativa speciale, quale quella delineata dalla direttiva 2006/42/CE, e, qualora il prodotto appartenga ad una classe specifica, dalla normativa di settore, come quella stabilita per i dispositivi medici dal Regolamento 2017/745/UE.

Ad una più attenta analisi, tuttavia, emerge che la normativa è carente per la regolamentazione di settore. In altre parole, il *corpus* di norme comunitarie è efficace nel regolare solo alcune delle possibili manifestazioni dell'intelligenza artificiale: si tratta, in particolare, delle IA meramente software (i già citati chatbot o assistenti vocali) o quelli che sono stati definiti come robot tele-operati. Mancano, invece, norme specifiche per le c.d. macchine intelligenti, per i robot autonomi e cognitivi, la cui introduzione è necessaria in quanto "appare piuttosto difficile ritenere che un robot autonomo, se non cognitivo, venga semplicemente sottoposto allo stesso sistema di

---

[108] Cfr. Regolamento 765/2008/CE, art. 5, par. 1: "Un organismo nazionale di accreditamento che ne abbia ricevuto domanda da un organismo di valutazione della conformità valuta se quest'ultimo sia competente a svolgere una determinata attività di valutazione della conformità. In caso affermativo, l'organismo nazionale di accreditamento rilascia un certificato di accreditamento".

verifica interna che viene richiesto per una gru o per un trattore agricolo. Le capacità di reazione e di apprendimento di un robot dovrebbero meritare una controllo qualitativamente più incisivo, tenuto conto dei rischi che possono derivare"[109].

Non si può parlare, tuttavia, di un vero e proprio vuoto normativo, in quanto i principi generali espressi nelle direttive e nel regolamento necessitano semplicemente di un adattamento alle specificità e ai possibili maggiori rischi che le intelligenze artificiali più avanzate e incorporate in robot potrebbero comportare.

Lo scheletro della normativa europea, in particolare, è composto da: definizioni generali, requisiti di sicurezza, obblighi di informazione e comunicazione, presenza di una autorità competente per le procedure di valutazione di conformità.

Tale schema deve essere adattato alle IA più evolute.

Occorrerebbe, in primo luogo, introdurre una normativa specifica per i robot "autonomi" o "cognitivi", secondo la catalogazione del citato Glossario Tecnico, ossia capaci di svolgere un compito senza nessun intervento umano ed in grado di adempiere alla propria "missione" valutando autonomamente il miglior percorso d'azione, grazie anche all'abilità di percepire l'ambiente circostante o ad abilità, quali il ragionamento e la pianificazione, paragonabili a quelle umane. Non sarebbe requisito essenziale che il robot presenti caratteristiche antropomorfe (potendo quindi un veicolo a guida autonoma essere ricompreso nella categoria), ma è necessario che esso incorpori una IA al suo interno: per questa tipologia di robot, la macchina è il corpo, l'IA è la mente.

Quanto ai requisiti di sicurezza, sebbene possano essere richiamati alcuni di quelli presenti nell'allegato I alla direttiva 2006/42/CE (es. sicurezza dei materiali usati per la produzione), l'elevata autonomia del robot non ne consente una totale equiparazione (veri e propri sistemi di comando non esisterebbero per questi robot e, di conseguenza, non è possibile richiedere una loro sicurezza ed affidabilità). Posto che, come si è illustrato nel capitolo terzo, una totale autonomia del robot è sconsigliabile, tra i requisiti di sicurezza dovrebbe essere preso in considerazione il c.d. *human-governing-the-loop*. Il fabbricante dovrebbe dotare qualunque robot di un *master switch*, di un

---

[109] *op. cit.* Amedeo Santosuosso, Chiara Boscarato, Franco Caroleo, *Robot e diritto: una prima ricognizione*, p. 13.

comando fisico o digitale capace di arrestare forzatamente la macchina ogniqualvolta se ne presenti la necessità, anche al costo di danneggiarla irreparabilmente. Dal canto loro, gli sviluppatori del software avrebbero l'obbligo di implementare nelle capacità cognitive del robot il rispetto di quei principi fondamentali di cui si è parlato sempre nel terzo capitolo.

Fra gli obblighi di informazione al consumatore dovrebbe essere data particolare enfasi al livello di autonomia della macchina: se, infatti, tanto maggior è l'autonomia dell'IA, tanto minore è il controllo umano, allora, in astratto, tanto maggiori potrebbero essere i rischi. Il consumatore deve esser posto nella condizione di conoscere i rischi che l'autonomia del robot cui è interessato presenta e, inoltre, gli dovrebbero essere prospettate diverse opzioni di acquisto correlate a diversi gradi di autonomia del robot.

Nessuna particolare specificazione appare, invece, necessaria con riferimento agli obblighi di comunicazione.

Da ultimo, gli Stati Membri dovrebbero dotarsi di enti autonomi specifici, che effettuino la valutazione di conformità di questi peculiari robot. Oltre all'apposizione della marchiatura CE, l'autorità dovrebbe essere posta in condizione di rilasciare un ulteriore certificato di sicurezza periodicamente rinnovabile. Ulteriormente, l'ente dovrebbe essere dotato di autonomi poteri di ispezione e controllo sull'operato dei fabbricanti e sviluppatori presenti sul territorio nazionale e dovrebbe poter procedere al ritiro e/o distruzione di quelle macchine che presentino rischi per la sicurezza.

4. La responsabilità civile nelle controversie che coinvolgono robot e IA.

Esaminato l'aspetto giuridico relativo alla fase di realizzazione delle intelligenze artificiali (siano esse software o incorporate in robot), passiamo ora a considerare quelle situazioni pratiche che coinvolgono o potrebbero coinvolgere i robot, tenendo ben presente la distinzione fra robot-oggetti (e IA meramente software) e robot-agenti. Anche in questa sede occorre verificare se la normativa vigente, iniziando dalle figure civilistiche, sia adeguata o necessiti di modifiche; ulteriormente, è necessario distinguere la responsabilità civile nelle sue varianti di responsabilità contrattuale, che

sanziona l'inadempimento di una obbligazione, e responsabilità extracontrattuale o aquiliana, che sanziona un fatto illecito dannoso.

4.1. La responsabilità contrattuale. Robot-oggetti.

Consideriamo, innanzitutto, la prospettiva dei robot-oggetti, ribadendo che la disciplina applicabile a questi ultimi vale anche per le IA meramente software, poiché se il software è direttamente acquistato dal consumatore si parlerà comunque di vendita di beni (il consumatore medio acquisterà un c.d. software standardizzato, cioè realizzato in serie, la cui disciplina ricade nella cessione di beni; nella remota ipotesi in cui dovesse richiedere un prodotto realizzato sulle sue specifiche esigenze, c.d. software personalizzato, si parlerà di prestazione di servizi[110]), se il software è semplicemente utilizzato dal consumatore ricadrà nella disciplina della direttiva n. 01/95/CE (*v. supra*).
In questo contesto, il robot è oggetto del contratto di compravendita che intercorre fra consumatore e produttore/distributore. Quest'ultimo, in particolare, sarà tenuto al rispetto della normativa nazionale specifica per tale tipologia di contratto. Escluso che si possa, in questa sede, effettuare un'analisi dettagliata e comparatistica del contratto di compravendita così come disciplinato nel mondo, ci si può soffermare su di alcuni aspetti generali del diritto dei contratti condivisi in ambito europeo ed extra-UE, in particolare sul concetto di "inadempimento" e sui possibili rimedi ad esso.
Sebbene non esista un vero e proprio codice civile comunitario, l'interesse per una fonte normativa ad esso assimilabile è in voga nelle istituzioni europee già dagli anni ottanta; in particolare nel 1982 fu istituita la "commissione sul diritto contrattuale europeo", anche nota come "commissione Lando" (dal nome del suo presidente, Ole Lando), che pubblicò i "principi di diritto europeo dei contratti" (o PECL), la prima parte nel 1995, la seconda nel 1999 e la terza ed ultima nel 2003.

---

[110] Marco Peirolo, "Le forniture di software in ambito intra-UE ed extra-UE", *Euroconference News Retrieved*, edizione del 31 luglio 2017, https://www.ecnews.it/wp-content/uploads/pdf/2017-07-31_le-forniture-software-ambito-intra-ue-ed-extra-ue.pdf (ultimo accesso 25 settembre 2020).

I PECL definiscono l'inadempimento come la mancata esecuzione della prestazione dovuta in base al contratto, che sia fonte di responsabilità o meno, incluso il ritardato o inesatto adempimento e la violazione dell'obbligo di cooperazione al fine di dare piena esecuzione al contratto[111]. L'inadempimento è considerato "grave" quando la stretta osservanza dell'obbligazione appartiene alla natura del contratto; l'inadempimento priva sostanzialmente il creditore insoddisfatto di ciò che esso ha il diritto di ricevere in base al contratto; l'inadempimento è dovuto a dolo[112].

Qualora il debitore non adempia alla propria obbligazione, il capitolo nono dei PECL offre una pluralità di rimedi che possono essere ricondotti ai mezzi di tutela tradizionali presenti nel diritto italiano: richiesta di adempimento, eccezione di inadempimento, risoluzione del contratto, riduzione del prezzo, risarcimento del danno.

Gli ordinamenti di *common law*, in particolare quello americano, non presentano peculiari differenze quanto ai concetti poc'anzi richiamati.

L'inadempimento (o *breach of contract*) è definito come il mancato rispetto, totale o parziale, di qualunque promessa dovuta dal contratto[113]. I concetti di ritardato e inesatto adempimento possono essere ricondotti, rispettivamente, agli istituti del *minor breach of*

---

111 Cfr. The Principles Of European Contract Law 2002, art. 1:301, n. 4): " *'non-performance' denotes any failure to perform an obligation under the contract, 40 whether or not excused, and includes delayed performance, defective performance and failure to co-operate in order to give full effect to the contract*".

112 Cfr. The Principles Of European Contract Law 2002, art. 8:103: "*A non-performance of an obligation is fundamental to the contract if: (a) strict compliance with the obligation is of the essence of the contract; or (b) the non-performance substantially deprives the aggrieved party of what it was entitled to expect under the contract, unless the other party did not foresee and could not reasonably have foreseen that result; (c) the non-performance is intentional and gives the aggrieved party reason to believe that it cannot rely on the other party's future performance*".

113 Cfr. "*A breach of contract is a failure, without legal excuse, to perform any promise that forms all or part of the contract*", "*Breach of Contract*", Judicial Education Center, University of New Mexico, http://jec.unm.edu/education/online-training/contract-law-tutorial/breach-of-contract (ultimo accesso 25 settembre 2020).

contract e del *material breach of contract*[114]. L'inadempimento grave è, invece, riconducibile all'istituto del *repudiatory breach* (anche noto come *fundamental breach*, anche se quest'ultima terminologia ha perso la sua valenza legale), in quanto la condotta della parte inadempiente priva l'altra parte sostanzialmente di qualunque beneficio che attendeva si sensi del contratto, si tratta di un inadempimento che mina *the root of the contract*. I rimedi offerti sono in larga parte coincidenti con quanto espresso nel capitolo nove dei PECL: risarcimento danni, risarcimento in forma specifica, rescissione e restituzione[115].

Finora si è considerato il robot come semplice oggetto di compravendita, ma si è in precedenza detto come esso ben possa essere ricompreso nella categoria dei "prodotti", dei "beni di consumo", nei confronti dei quali diventa rilevante, quantomeno in ambito europeo, la direttiva 1999/44/CE su taluni aspetti della vendita e delle garanzie concernenti i beni di consumo. Tale direttiva introduce ulteriori specificazioni della disciplina del contratto e dei diritti del consumatore.

Secondo l'art. 2 della direttiva, i beni consegnati al consumatore devono essere conformi al contratto, presumendosi conformi quei beni che sono conformi alla descrizione fatta dal venditore, che presentino caratteristiche tipiche di un bene dello stesso tipo che il consumatore può ragionevolmente aspettarsi, che sono idonei al loro

---

[114] Cfr. "*A breach is minor if, even though the breaching party failed to perform some aspect of the contract, the other party still receives the item or service specified in the contract. A breach is material if, as a result of the breaching party's failure to perform some aspect of the contract, the other party receives something substantially different from what the contract specified*", Breach of Contract, Judicial Education Center, University of New Mexico, http://jec.unm.edu/education/online-training/contract-law-tutorial/breach-of-contract (ultimo accesso 25 settembre 2020).

[115] Cfr. "*There are several remedies for breach of contract, such as award of damages, specific performance, rescission, and restitution*", Remedies for Breach of Contract, Judicial Education Center, University of New Mexico, http://jec.unm.edu/education/online-training/contract-law-tutorial/remedies-for-breach-of-contract (ultimo accesso 25 settembre 2020).

uso abituale o uso speciale voluto dal consumatore[116]. Il venditore risponderà di qualunque difetto di conformità esistente al momento della consegna del bene e, secondo quanto disposto dall'art. 5, "è responsabile […] quando il difetto di conformità si manifesta entro il termine di due anni dalla consegna del bene".

L'art. 3 disciplina i diritti del consumatore in presenza di un difetto di conformità. In primo luogo il consumatore potrà richiedere la riparazione o sostituzione senza spese del prodotto, a meno che ciò sia impossibile o sproporzionato[117]. Se il consumatore non ha diritto né alla ripartizione né alla sostituzione o se il venditore non ha esperito il rimedio entro un periodo ragionevole ovvero non ha esperito il rimedio senza notevoli inconvenienti per il consumatore, allora quest'ultimo potrà richiedere una congrua riduzione del prezzo o la risoluzione del contratto il diritto di chiedere la risoluzione del contratto.

Analizzato il robot nella sua "dimensione statica, guardando il robot quale mero oggetto di scambio"[118], non sembrano emergere particolari criticità o lacune che facciamo ritenere necessario l'elaborazione di regole specifiche. Il diritto dei contratti appare nei diversi sistemi giuridici pronto per accogliere le sfide presentate da queste tecnologie.

---

[116] Cfr. Dir. 1999/44/CE art. 2, par. 2: "Si presume che i beni di consumo siano conformi al contratto se: a) sono conformi alla descrizione fatta dal venditore e possiedono le qualità del bene che il venditore ha presentato al consumatore come campione o modello; b) sono idonei ad ogni uso speciale voluto dal consumatore e che sia stato da questi portato a conoscenza del venditore al momento della conclusione del contratto e che il venditore abbia accettato; c) sono idonei all'uso al quale servono abitualmente beni dello stesso tipo; d) presentano la qualità e le prestazioni abituali di un bene dello stesso tipo, che il consumatore può ragionevolmente aspettarsi, tenuto conto della natura del bene e, se del caso, delle dichiarazioni pubbliche sulle caratteristiche specifiche dei beni fatte al riguardo dal venditore, dal produttore o dal suo rappresentante, in particolare nella pubblicità o sull'etichettatura".

[117] Quanto alla definizione di "sproporzionato", cfr. Dir. 1999/44/CE art. 3, par. 3: "Un rimedio è da considerare sproporzionato se impone al venditore spese irragionevoli in confronto all'altro rimedio".

[118] *op. cit.* Amedeo Santosuosso, Chiara Boscarato, Franco Caroleo, *Robot e diritto: una prima ricognizione.*

4.2. La responsabilità contrattuale. I robot-agenti e il *peculium* robotico.

Diverso è il discorso se si considerano i robot nella loro "dimensione dinamica", quali attori principali della società umana. Si è fatto in precedenza riferimento alla possibilità di un robot commesso, che agisce in nome e per conto di altri, ma non è fantascientifico ipotizzare che un robot possa concludere contratti in nome proprio e per conto di altri o, addirittura, sia capace di concludere contratti e assumere obbligazioni per sé stesso.

Se quindi il robot è capace di assumere obbligazioni per conto proprio, sorge il problema di stabilire chi sia effettivamente responsabile per quelle stesse obbligazioni.

A ben vedere, tuttavia, l'idea che una cosa possa essere ritenuta direttamente responsabile delle proprie azioni presenta un precedente nell'antica Roma, in particolare nell'istituto del *peculium servile*, che consentiva agli schiavi, privi di personalità, di gestire autonomamente taverne o negozi. L'idea di assimilare i robot agli schiavi è da tempo in voga: già nel 1950 Norbert Weiner, matematico e statistico americano ritenuto dai più padre fondatore della cibernetica moderna, affermava che "*the automatic machine, whatever we think of any feelings it may have or may not have, is the precise economic equivalent of slave labor*"[119]; nel 1992, Leon E. Wein riconosce che l'intelligenza artificiale "*is bringing the conception of slavery back on the scene as employees who replaced slaves are themselves replaced by mechanical 'slave'* "[120]. Lo stesso termine "robot", deriva dal cèco *robota*, che significa "lavoro servile", nome utilizzato per la prima volta dallo scrittore Karel Čapek, per denominare gli automi che lavorano al posto degli operai nel suo dramma fantascientifico *R.U.R.* del 1920[121].

Tornando all'istituto romano del *peculium*, esso stava ad indicare una somma di denaro (non necessariamente di esigua entità) che il *pater familias* concedeva al *filius familias*. L'istituto in questione risolveva un problem collegato alla patria potestà, per cui il *filius*

---

[119] Norbert Wiener, "*The Human Use Of Human Beings Cybernetics And Society*" (Boston: Houghton Mifflin, 1950), p. 162.

[120] Leon E. Wein, "*The Responsibility Of Intelligent Artifacts: Toward An Automation Jurisprudence*", Harvard Journal of Law & Technology, Volume 6 (Autunno 2017).

[121] *Treccani.it*, s.v., "robòt" ultima consultazione il 25 settembre 2020, https://www.treccani.it/vocabolario/robot.

non poteva avere nulla di proprio: grazie al *peculium*, il *pater* affidava in godimento e amministrazione il denaro, mantenendone la proprietà. Tuttavia, la caratteristica principale di questo istituto era costituita dal fatto che il *pater* era sì responsabile delle obbligazioni contratte dal *filius*, ma solo nei limiti della somma che costituisce il *peculium*. Tale istituto veniva anche utilizzato per concedere in amministrazione somme di denaro agli schiavi; quando il *peculium* veniva affidato al *filius* assumeva il nome di *peculium profecticium*, se veniva affidato al servo era chiamato *peculium servile*[122].

L'effetto pratico del *peculium* è oggi conseguibile tramite la costituzione di società a responsabilità limitata[123]. La società a responsabilità limitata, infatti, è una società di capitali nella quale "per le obbligazioni sociali risponde soltanto la società col suo patrimonio. […] In questo tipo di società tutti i soci godono del beneficio della responsabilità limitata e nessuna pretesa possono perciò avanzare nei loro confronti i creditori della società"[124]. Ciononostante, fra l'istituto romano e l'odierno istituto commerciale vi è una differenza che rende preferibile applicare ai robot il primo piuttosto che il secondo: il *peculium*, infatti, era concesso anche agli schiavi, generalmente considerati soggetti privi di personalità; la srl, invece, è dotata di personalità giuridica.

Considerato che al momento i robot, nella loro veste di agenti, sono privi di personalità, *de iure condendo* sarebbe preferibile riprendere la struttura base del *peculium* e modernizzarla in una sorta di *peculium* robotico. Sebbene, in astratto, sia possibile dotare il robot di un "portafoglio", appare maggiormente calzante la scelta di introdurre un sistema assicurativo apposito per le persone fisiche o giuridiche che intendano utilizzare intelligenze artificiali per gestire i propri rapporti commerciali. Superflua

---

[122] Cfr. *Treccani.it*, s.v., "PECULIO" ultima consultazione il 25 settembre 2020, https://www.treccani.it/enciclopedia/peculio_%28Enciclopedia-Italiana%29/. Cfr. anche Luigi Mastrangelo, "Il *peculium quasi castrense* - Privilegio dei *palatini* in età tardo antica" (luglio 2004).

[123] In verità, tale effetto può essere raggiunto anche mediante la costituzione di società per azioni. Tuttavia, i minori requisiti di capitale, i minori costi di funzionamento e di costituzione e la possibilità di prevedere una struttura organizzativa con maggiore flessibilità, rendono la società a responsabilità limitata il tipo di società di capitali di gran lunga più diffuso e, dunque, maggiormente meritevole di esame.

[124] Gian Franco Campobasso, Mario Campobasso, "Diritto Commerciale" (nona ed., Vol. 2. Diritto delle società, Torino: UTET giuridica, 2015).

diventerebbe quindi la distinzione fra mandato con rappresentanza (o procura) e mandato senza rappresentanza, in quanto, in entrambi i casi, i terzi avrebbero rapporti solo con il "mandatario robotico". In questo modo verrebbe risolta la spinosa questione di stabilire a chi attribuire la responsabilità per i danni da inadempimento contrattuale, poiché "*legal systems may sever the responsibility of designers, manufacturers, operators and users of robots dealing with third parties, so that, on the basis of the warranty of their own peculium, only robots would be held liable for damages caused by them*"[125].

Il sistema del *peculium* robotico appare consigliabile per affrontare alcune questioni legali poste dalle intelligenze artificiali e costituisce un buon punto di partenza per individuare i robot come autonomi centri di responsabilità. D'altra parte, si deve valutare anche se tale nuovo istituto possa essere idoneo a disciplinare ulteriori vicende legate all'uso di tali tecnologie, con particolare riferimento ai danni che possano causare.

In vista di nuove generazioni di robot, non ci si può più cullare sulla realizzabilità esclusivamente fantascientifica di queste macchine: quando negli sessanta andava in onda la sitcom animata "i pronipoti" ("*The Jetsons*" nel suo titolo originale), nessuno si sarebbe mai aspettato che il personaggio di Rosie, la cameriera robotica e governante della famiglia Jetson, avrebbe mai potuto avere una controparte nella vita reale. Tuttavia, ad oggi, la creazione di queste macchine non è più impensabile: si pensi, infatti, ad "iPal", un robot antropomorfo da compagnia pensato per intrattenere i bambini, aiutare gli insegnati a scuola o, addirittura, aiutare le persone di una certa età nelle loro attività quotidiane. Nonostante gli importanti benefici apportati da tali tecnologie, non si può prescindere dal considerare alcuni aspetti legali: quali sarebbero le conseguenze se iPal o un veicolo a guida autonoma dovesse provocare un danno ad oggetti o persone? Tali vicende giuridiche vanno oltre la mera responsabilità contrattuale e l'istituto del *peculium* non sembra adatto per poterle fronteggiare. La responsabilità contrattuale cede, infatti, il passo ad un altro istituto, sempre di origine romana, quello della responsabilità aquiliana (o extracontrattuale).

---

[125] *op. cit.* Ugo Pagallo. *The Laws of Robots Crimes, Contracts, and Torts*, p. 105.

L'ulteriore domanda da porsi, quindi, è come poter disciplinare situazioni che vedono coinvolte intelligenze artificiali alla luce di questa forma di responsabilità.

4.3. La responsabilità extracontrattuale. I robot-oggetti.

Anche in tema di responsabilità extracontrattuale occorre riprendere la distinzione, già utilizzata per la responsabilità contrattuale, fra robot-oggetti e robot-agenti.
Va premesso che la maggior parte delle intelligenze artificiali meramente software non sono in grado di causare danni rilevanti ai fini di una responsabilità aquiliana. Tali IA, quali i chatbot o gli assistenti vocali, suscitano più che altro dubbi in materia di sicurezza e privacy, aspetti che, per amor di brevità, non saranno affrontati in questa sede.
Nei prossimi paragrafi si farà, quindi, riferimento ai soli robot, ricordando comunque che nei robot-agenti la presenza dell'intelligenza artificiale è data per scontata; di conseguenza, regolare i robot-agenti vuole dire regolare, almeno in parte, l'intelligenza artificiale. D'altra parte, è possibile che anche nei robot-oggetti sia presente una intelligenza artificiale, intesa, peró, in senso lato, come capacità di emulare alcuni tratti dell'essere umano: così, iPal è dotato di una intelligenza artificiale che parla più lingue, è capace di dare lezioni di matematica e raccontare barzellette, ma non può essere definita come IA *strictu sensu* (*v. supra* capitolo I).

4.3.1. La responsabilità da prodotto difettoso.

Ipotizziamo che iPal, a causa di un difetto alle sue articolazioni artificiali, abbia un cedimento e che, nel cadere, urti, ferendolo, il bambino che stava intrattenendo; ipotizziamo, poi, la diversa situazione in cui il braccio meccanico di iPal, a causa di un bug nel software, si azioni ed urti un tavolino, rompendo un prezioso vaso. In entrambi i casi è un difetto del prodotto a provocare il danno; si tratta, però, di un prodotto molto particolare, composto da una parte meccanica e da una parte digitale (il sistema

operativo) che sono realizzate da due diverse compagnie (rispettivamente la Avatarmind e Google).

Per porre rimedio alle conseguenze dannose dovute a prodotti difettosi, sia nell'ordinamento comunitario che in quello americano, si possono rinvenire delle regole in tema di "responsabilità da prodotto".

Nella *common law* statunitense la *products liability* è governata da una pluralità di fonti statali e federali, potendo ogni Stato definire in maniera autonoma gli estremi della responsabilità. Tuttavia, una disciplina generale in tema di responsabilità extracontrattuale, può essere rinvenuta nel *Restatement (Second) of Torts* (1965), sezione 402A, rubricato "*special liability of seller of product for physical harm to user or consumer*", secondo cui chiunque venda un prodotto difettoso, che ponga un irragionevole pericolo per l'utente o il consumatore o per la sua proprietà *"is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if (a) the seller is engaged in the business of selling such a product, and (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold*"; il secondo paragrafo dispone poi che la responsabilità incombe sul venditore anche qualora "*the seller has exercised all possible care in the preparation and sale of his product*" e/o il consumatore "*has not bought the product from or entered into any contractual relation with the seller*".

L'onere di prova non è direttamente regolato dalla norma, ma si evince dalle disposizioni processuali generali: la vittima dovrà provare tutti gli elementi essenziali del proprio caso, in particolare il difetto del prodotto.

La disciplina così espressa, tuttavia, sembra essere efficace solo parzialmente: è dubbio, infatti, che essa possa applicarsi anche a danni causati a persone diverse dal consumatore o al rivenditore di un componente di un prodotto da assemblare[126].

---

[126] È lo stesso *American Law Institute*, che ha redatto il *Restatement,* a non poter esprimere una valida opinione "*as to whether the rules stated in this Section may not apply (1) to harm to persons other than users or consumers; (2) to the seller of a product expected to be processed or otherwise substantially changed before it reaches the user or consumer; or (3) to the seller of a component part of a product to be assembled*".

Diversa invece è la situazione nel diritto europeo, ove, grazie alla direttiva n. 85/374/CEE in materia di responsabilità per danno da prodotti difettosi, si è riusciti a creare una disciplina ben più estesa di quella statunitense.

L'art. 1 sancisce il principio generale in base al quale il produttore è responsabile del danno causato da un difetto del suo prodotto[127]. Per "prodotto" (art. 2), secondo la modifica apportata dalla direttiva 1999/34/CE alla direttiva 85/374/CEE, si intende "ogni bene mobile, anche se forma parte di un altro bene mobile o immobile". Un prodotto è poi definito "difettoso" (art. 6) quando "non offre la sicurezza che ci si può legittimamente attendere", considerando tutte le circostanze, tra cui "la presentazione del prodotto; l'uso al quale il prodotto può essere ragionevolmente destinato; il momento della messa in circolazione del prodotto". D'altra parte, un prodotto non può essere considerato difettoso quando "un prodotto più perfezionato sia stato messo in circolazione successivamente ad esso".

Qualora un danno, per tale intendendosi sia un danno alla persona che alla cosa[128], fosse conseguenza del difetto di un prodotto, per ottenere il risarcimento, la vittima del sinistro deve provare il danno, il difetto e la connessione causale tra difetto e danno (art. 4). Di detto danno dovrà rispondere il produttore[129], definito dall'art. 3 come "il fabbricante di un prodotto finito, il produttore di una materia prima o il fabbricante di una parte componente".

---

[127] La formulazione di questa norma già scioglie in negativo il dubbio circa la necessità che il danno sia subito direttamente dal consumatore. Sul punto si è espressa la Corte di Cassazione italiana, stabilendo che "legittimati ad agire sulla base delle specifiche disposizioni dettate dalla suddetta disciplina sono, dunque, tutti i soggetti che in qualche modo si sono trovati esposti, anche in maniera occasionale, al rischio derivante dal prodotto difettoso" (cfr. Cass. civ., sez. III, 29 maggio 2013, n. 13458).

[128] Cfr. Dir. 85/374/CEE, art. 9: "per « danno » si intende: a) il danno causato dalla morte o da lesioni personali; b) il danno o la distruzione di una cosa diversa dal prodotto difettoso"

[129] Se non fosse possibile identificare il produttore o quest'ultimo risiedesse al di fuori dell'Unione Europea, allora la responsabilità ricadrebbe, rispettivamente, sul fornitore o sull'importatore (cfr. Dir. 85/374/CEE, art. 3).

4.3.2. Le caratteristiche dei prodotti robotici e la separazione fra hardware e software.

Riprendiamo ora gli esempi poc'anzi proposti sui danni causati da iPal e verifichiamo se la normativa sui prodotti difettosi sia ad essi applicabile.

Nella prima situazione (cioè il difetto alle articolazioni artificiali) non si pone nessun problema nel richiedere il risarcimento al produttore: il difetto (ad esempio l'utilizzo di materiali scadenti o inidonei) è agevolmente verificabile mediante una perizia; provato il difetto, allora potrà provarsi il nesso di causalità (ovvero che il cedimento delle "gambe" del robot ha causato la ferito, ossia il danno).

La seconda situazione (il bug del software) risulta maggiormente problematica, in quanto il danno non è direttamente collegato ad un difetto del prodotto (inteso come fisicamente percepibile), ma ad un bug (appunto, un difetto) nel suo software. Ci si deve innanzitutto chiedere se il software possa essere considerato come un prodotto ai fini dell'applicazione della relativa disciplina. Mentre il *Restatement (Second) of Torts* non si espone sul significato del termine[130], la direttiva europea sulla responsabilità da prodotto difettoso lo definisce come ogni bene mobile, anche se forma parte di un altro bene mobile o immobile, inclusa l'elettricità.

Orbene come inserire il software fra i prodotti? Nonostante la non concordanza sulla definizione di prodotto, la pragmaticità delle corti di *common law* ha elaborato l'"*essential nature test*", in base al quale la questione se il software comporti la prestazione di un servizio o la vendita di un prodotto è risolta guardando all'essenza del contratto, esaminando "*whether [the contract] constitutes the provision of a service, in which case the software is a service, or the delivery of a product, in which case it is*

---

[130] In questo senso, Charles E. Cantú, professore di diritto alla *St. Mary's University School of Law*, sostiene che "*Courts interpreted some terms of Section 402A to include individuals and events not originally mentioned, while other terms, which at first were thought to be clear and concise, proved quite illusive. One such term is 'product'* " (cfr. Charles E. Cantú, "*The Illusive Meaning of the Term 'Product' Under Section 402A of the Restatement (Second) of Torts*", Vol. 44, 1991 (Oklahoma Law Review, 1991)) e che "*Courts continue to employ a line of reasoning that disregards any initial attempt at defining the item in controversy*" (cfr. Charles E. Cantú, "*A Continuing Whimsical Search for the True Meaning of the Term "Product" in Products Liability Litigation*" (33 St. Mary's L.J. 455 (2004)).

regarded as a product"[131]. Seguendo questo test, alcuni autori ritengono che l'essenza del contratto "*is always precisely the tailored software which is delivered, and therefore software always remains a product although the 'making available' of the software may be in the form of a service*"[132]. Parte della dottrina comunitaria non è dello stesso avviso, in quanto ritiene che il software non possa mai essere considerato prodotto, a causa della sua immaterialità (o intangibilità); questa conclusione è tratta dal fatto che l'elettricità, quale bene immateriale, è esplicitamente inserita fra i prodotti dalla direttiva 1999/34/CE, inferendo che "le altre cose immateriali siano escluse dall'ambito di applicazione della normativa per via del principio *unius inclusio est alterius exclusio*"[133]. Altri autori invece sostengono che l'elettricità è menzionata meramente come un "*example of a non-corporeal object that is to be treated like a corporeal asset, and that software is another, and even better example. On this view, the Products Liability Directive, already in its current form, does apply to software 'products'*"[134].

Peraltro la questione della protezione del consumatore da danni derivanti dal software può essere affrontata prescindendo da queste diatribe dottrinali e guardando alla norma dell'art. 3 della direttiva n. 85/374/CEE: con produttore, fra l'altro, si identifica anche il fabbricante di una parte componente. Il mancato riferimento al termine prodotto nella frase "parte componente" permette, a mio avviso, di operare una interpretazione estensiva del concetto, in modo tale da includervi anche i software; ciò in quanto, per tutti quei robot come iPal e tecnologie similari, il software è parte componente (e necessaria) della macchina.

Se, dunque, l'obbligo di risarcire la parte lesa grava non solo sul produttore quale fabbricante del prodotto finito, ma anche sul fabbricante della parte componente e se consideriamo lo sviluppatore del software come fabbricante della parte componente, è

---

[131] K. Alhelt, "*The Applicability of the EU Product Liability Directive to Software*", Comparative and International Law Journal of Southern Africa 34, no. 2 (2001): 188-209.

[132] *ibid*.

[133] Pier Giorgio Chiara, "Software e responsabilità da prodotto: Il caso del Boeing 737 MAX 8", (28 aprile 2018). Disponibile in https://www.cyberlaws.it/2019/software-responsabilita-prodotto-caso-boeing/ (ultimo accesso 25 settembre 2020).

[134] Gerhard Wagner, "*Robot Liability*", Working Paper No. 2 dell'Istituto di ricerca per il diritto e la trasformazione digitale (2019).

possibile separare la responsabilità dei due soggetti, in modo tale che il consumatore possa procedere con azione risarcitoria esclusivamente e direttamente nei confronti dello sviluppatore?

Per rispondere a tale quesito, occorre richiamare quanto detto nel primo capitolo circa la differenza fra il "modello Apple" e il "modello Android". Nel "modello Apple" vi è unità fra produttore hardware e software, nel "modello Android", le due tipologie di produttori sono separate.

Il "modello Apple" non pone alcuna difficoltà: se il produttore dell'hardware e del software è lo stesso, l'azione risarcitoria, indipendentemente dal fatto che il difetto sia relativo al primo o al secondo, verrà esercitata nei confronti di un unico soggetto.

Nel "modello Android", una rigida applicazione della normativa sul prodotto difettoso non consentirebbe di far valere la responsabilità dello sviluppatore del software. Per poter risolvere tale inconveniente, possono essere prospettate due soluzioni alternative: considerare produttore e sviluppatore come corresponsabili in via solidale per i danni derivati dal difetto (hardware o software) del prodotto; individuare lo sviluppatore come unico responsabile qualora il difetto sia riscontrabile nel software.

I sostenitori della prima soluzione ritengono che la corresponsabilità sia l'unica via praticabile, in quanto una responsabilità cosi tratteggiata è l'unica "in linea con quello che è già un principio fissato nella Direttiva: «se dello stesso danno sono responsabili più persone, la protezione del consumatore implica che il danneggiato possa chiedere il risarcimento integrale ad uno qualsiasi dei responsabili». […] La così delineata responsabilità non […] sarebbe in contrasto con quella responsabilità cumulativa prevista dalla Direttiva (e non alternativa) dei soggetti coinvolti nella catena produttiva e abbasserebbe gli standard di tutela del consumatore"[135].

Peraltro, a mio giudizio, tale tesi è facilmente confutabile: la direttiva parla esplicitamente di danno per cui "sono responsabili più persone", mentre nel caso di un danno collegato esclusivamente ad un bug nel software, di detto danno può essere responsabile esclusivamente lo sviluppatore. Un esempio potrebbe essere chiarificatore: si consideri un computer Toshiba che monta, come sistema operativo, Windows e che, a

---

[135] *op. cit.* Laura Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*.

seguito di un aggiornamento del software, alcuni programmi cessino di funzionare[136]; il fatto che l'utilizzo di questi programmi sia impedito non può essere ascritto a Toshiba, in quanto l'unico responsabile è Microsoft, casa produttrice del software. Orbene, applicando questo esempio alla situazione in cui iPal, a causa di un bug nel software, determini un danno, allora responsabile potrà essere solo lo sviluppatore.

Con ciò non si vuole escludere a priori qualunque possibilità di corresponsabilità fra produttore e sviluppatore; simili scenari potrebbero configurarsi principalmente in due situazioni: difetto sia della parte meccanica sia di quella digitale e ipotesi di *culpa in eligendo*.

La prima fattispecie si verifica quando al danno concorrono un difetto imputabile sia al produttore che allo sviluppatore: si prenda nuovamente ad esempio iPal e si consideri che, a causa di un bug nel software, venga azionato il suo braccio meccanico e che, a causa di materiali scadenti utilizzati per la costruzione, il braccio si distacchi dal corpo e, cadendo, urti una persona, ferendola. L'evento danno non si sarebbe verificato se il produttore avesse utilizzato materiali di prima qualità; parimenti, l'evento danno non si sarebbe verificato se il software non avesse fatto azionare il braccio di iPal. In questa ipotesi fabbricante e sviluppatore sono entrambi responsabili per il danno causato dal prodotto e il consumatore potrà esercitare l'azione risarcitoria verso uno o entrambi i soggetti, in ossequio al principio fissato nella direttiva 85/374/CEE.

La seconda fattispecie, di più rara applicazione, potrebbe verificarsi quando il produttore, per ragioni di risparmio economico, decida di affidare la componente software del proprio prodotto ad un operatore che sa o poteva sapere essere meno affidabile di altri presenti sul mercato. Qualora un danno dovesse verificarsi a causa di un difetto del sistema operativo, responsabile sarebbe sì lo sviluppatore, ma la negligenza del produttore consentirebbe di far valere l'azione risarcitoria anche nei suoi confronti.

---

[136] Problema già riscontrato in uno degli ultimi aggiornamenti del sistema operativo Windows 10. Sul punto cfr. Simone Pettine, "Windows 10, gli aggiornamenti recenti impediscono ai programmi di funzionare a dovere" (13 giugno 2020), disponibile in https://multiplayer.it/notizie/windows-10-aggiornamenti-recenti-impediscono-programmi-funzionare-a-dovere.html (ultimo accesso 25 settembre 2020).

La questione più spinosa, tuttavia, è quella di un possibile abbassamento degli standard di tutela del consumatore. In effetti, secondo quanto riportato nel *White Paper on AI* della Commissione Europea "*in the case of an AI based system […] it may be difficult to prove that there is a defect in the product, the damage that has occurred and the causal link between the two*"[137]. Premesso che una perizia informatica ben potrebbe determinare se il sistema operativo abbia o meno subito delle alterazioni e, di conseguenza, dimostrare il "difetto", ma considerato che l'azienda sviluppatrice è in grado di accedere alle informazioni rilevanti in maniera più rapida ed efficace, potrebbe trovare applicazione il c.d. "principio della vicinanza della prova", in base al quale l'onere della prova grava sulla parte che più agevolmente è in grado di assolverlo[138] (nel nostro caso, lo sviluppatore). In capo al consumatore graverebbe comunque l'onere di provare il danno e il nesso di causalità, ma, qualora vi siano sufficienti ragioni per ritenere che il danno non sia dovuto al prodotto fisico, sussisterebbe una presunzione di difetto del software; la compagnia sviluppatrice sarà quindi chiamata a fornire la prova contraria, allegando le ragioni per cui il software non presenta alterazioni in grado di determinare un simile comportamento della macchina.

In tema di responsabilità da prodotto difettoso in cui sono presenti sia hardware che software è necessario, da ultimo, esaminare alcuni profili critici quanto all'esonero della responsabilità del produttore.

La direttiva comunitaria, fra le varie ipotesi di esonero da responsabilità[139], annovera la prova del fatto che il difetto che ha causato il danno non esistesse quando il prodotto è

---

[137] *op. cit. WHITE PAPER On Artificial Intelligence.*

[138] In tal senso vedi *op. cit.* Andrea Torrente, *Manuale di Diritto Privato*, p. 253. Cfr. anche Cass. civ., sez. L, 25 luglio 2008, n. 20484.

[139] Cfr. Dir. 85/374/CEE, art. 7: "Il produttore non è responsabile ai sensi della presente direttiva se prova: a) che non ha messo il prodotto in circolazione; b) che, tenuto conto delle circostanze, è lecito ritenere che il difetto che ha causato il danno non esistesse quando l'aveva messo in circolazione o sia sorto successivamente; c) che non ha fabbricato il prodotto per la vendita o qualsiasi altra forma di distribuzione a scopo economico, né l'ha fabbricato o distribuito nel quadro della sua attività professionale; d) che il difetto è dovuto alla conformità del prodotto a regole imperative emanate dai poteri pubblici; e) che lo stato delle conoscenze scientifiche e tecniche al momento in cui ha messo in circolazione il prodotto non permetteva di scoprire l'esistenza del difetto; f) nel caso del produttore di una parte componente, che il difetto è dovuto alla concezione del prodotto in cui è stata incorporata la parte o alle istruzione date dal produttore del prodotto".

stato messo in circolazione o sia sorto successivamente (art. 7). Tuttavia, "*the integration of software, including AI, into products can modify the functioning of such products and systems during their lifecycle. This is particularly true for systems that require frequent software updates […]. These features can give rise to new risks that were not present when the system was placed on the market. These risks are not adequately addressed in the existing legislation which predominantly focuses on safety risks present at the time of placing on the market*"[140]. Per far in modo che le persone possano godere dello stesso livello di protezione "*as persons having suffered harm caused by other technologies*"[141], è necessaria una ulteriore modifica alla direttiva 85/374/CEE, che tenga conto del fatto che talune tecnologie (quali iPal) possano, sotto alcuni aspetti, mutare nel tempo. Per evitare che il consumatore sia lasciato in balia degli sviluppatori e dei loro aggiornamenti software, è necessario provvedere, nuovamente, ad una separazione tra questi ultimi e il produttore: al produttore della parte fisica si applicherà la norma di cui all'art. 7; allo sviluppatore una simile disciplina non potrà essere estesa, in quanto non compatibile con le esigenze di tutela del consumatore.

4.3.3. La responsabilità dell'operatore di robot-oggetti.

Finora si è analizzata una specifica figura di responsabilità extracontrattuale, cioè la responsabilità oggettiva da prodotto difettoso. Tuttavia, tale disciplina non è esauriente: i molteplici campi di applicazione ed utilizzo dei robot-oggetti impongo di guardare alla responsabilità aquiliana a trecentosessanta gradi, illustrando, in primo luogo, gli elementi fondamentali dell'istituto sia nella *common law* statunitense sia nel diritto comunitario.

In America la disciplina della responsabilità da fatto illecito è contenuta nella *tort law*. La disciplina generale dei *torts* è per la maggior parte contenuta nella *common law*, non

---

[140] *op. cit. WHITE PAPER On Artificial Intelligence*

[141] *ibid.*

essendo completamente disciplinati in statuti o codici statali; ciò significa che essi sono in continua evoluzione, in particolare grazie alle *legal opinions* espresse dai giudici.

Ciò premesso, in generale un *tort* si verifica quando qualcuno, intenzionalmente o per negligenza, causi lesioni ad un'altra persona o alla sua proprietà. Alla luce di questa definizione, i *torts* possono essere racchiusi in tre principali categorie: *torts* intenzionali (*intentional*), negligenza (*negligence*) e *strict liability torts*.

Gli *intentional torts* riguardano situazioni in cui il soggetto agente desidera o ritiene con un elevato grado di probabilità che il suo atto causerà danni ad altri.

La *negligence* si fonda sul mancato rispetto del dovere di diligenza che appartiene ad una persona ragionevole che è la causa effettiva del danno. In altre parole, in assenza dell'atto o dell'omissione del soggetto agente che poteva ragionevolmente prevedere che la sua condotta avrebbe causato il danno, quest'ultimo non si sarebbe verificato.

Gli *strict liability torts* (fra i quali rientra la *products liability*) riguardano, invece, quelle condotte del soggetto attivo che determinano un danno, prescindendo dalle intenzioni dolose o colpose del soggetto agente; possono anche riguardare lesioni determinate durante lo svolgimento di attività particolari, per le quali il soggetto agente sarà ritenuto responsabile anche se, da parte sua, non vi è stata negligenza.

Perché il danneggiante possa sollevarsi dall'attribuzione di responsabilità, dovrà provare che la condotta è stata tenuta per provvedere alla difesa personale, alla difesa di altri, alla difesa della proprietà, che vi sia stata provocazione o consenso della vittima e, per alcuni *torts*, lo stato di necessità[142].

Dal suo canto il danneggiato, per poter intentare l'azione risarcitoria, avrà l'onere di provare: il danno; il dolo o la colpa del danneggiante (rispettivamente negli *intentional torts* o in casi di *negligence*; negli *strict liability torts* la colpa non necessita di prova); il nesso di causalità (*causation*) fra il danno e la condotta del danneggiante[143].

---

[142] La necessità viene, qui, intesa in maniera differente dagli ordinamenti di civil law: si distinguono infatti la *private necessity*, cioè l'utilizzo della proprietà privata altrui per ragioni personali, e la *public necessity*, cioè l'uso della proprietà privata da parte di un pubblico ufficiale per un ragioni di pubblico interesse.

[143] per approfondimenti sul tema della *torts law* cfr. "*Overview Of Torts*", Judicial Education Center, University of New Mexico, http://jec.unm.edu/education/online-training/torts-tutorial. Cfr. anche "*United States tort law*", Wikipedia, L'enciclopedia libera, https://en.wikipedia.org/wiki/United_States_tort_law. (ultimo accesso il 25 settembre 2020).

Nell'Unione Europea, come avvenuto per il diritto dei contratti, si è provato a ricercare principi comuni di responsabilità extracontrattuale per definire un sistema giuridico uniforme. In tal senso, ammirevole è stato il lavoro dello *European Group on Tort Law*, che, nel 2005, ha pubblicato i "*Principles of European Tort Law*" (o PETL). Nonostante si tratti di uno strumento giuridico di elevata utilità (anche in chiave di un effettivo codice civile europeo), è opportuno notare fin da subito come la disciplina in essi contenuta risulti piuttosto generica; per tal motivo, si farà riferimento anche alla normativa italiana, che risulta sicuramente più articolata e specifica.

L'art. 1:101 dei PETL, rubricato "norma fondamentale", stabilisce che "il soggetto a cui un danno subito da altri è a lui giuridicamente imputabile dal diritto, è tenuto a risarcirlo". Tale danno, definito come una lesione materiale o immateriale di un interesse[144] giuridicamente protetto (art. 2:101), è imputabile al soggetto "a) la cui condotta colposa o dolosa ha causato il danno; o b) la cui attività straordinariamente pericolosa ha causato il danno; o c) i cui ausiliari hanno causato il danno nell'ambito delle proprie attribuzioni". Anche per i PETL rileva, dunque, la distinzione fra un comportamento doloso, cioè intenzionale, e colposo, cioè in violazione dello standard di condotta richiesto ad una persona ragionevole nelle circostanze del caso concreto (artt. 4:101 e 4:102). Parimenti assume importanza, come autonoma categoria, la responsabilità oggettiva (che trova il suo corrispettivo nella *strict liability* di *common law*), quale responsabilità di chi eserciti un'attività straordinariamente pericolosa, intendendosi una attività che "crea un rischio particolarmente significativo e prevedibile di danno anche quando sono esercitate tutte le attenzioni nel suo esercizio e non corrisponda a pratiche di uso comune" (art. 5:101).

Quanto alla prova dei fatti da parte del danneggiato, con formula generica, l'art. 2:105 dispone che "il danno deve essere provato secondo i normali standard". Più elaborato è invece il sistema delle cause di esclusione della responsabilità: il danneggiante sarà

[144] Per una elencazione degli interessi protetti (ad es. vita, dignità umana, libertà, proprietà, ecc.) cfr. The Principles Of European Tort Law 2005, art. 2:102.

giustificato qualora abbia agito per legittima difesa, stato di necessità, auto-tutela[145], con il consenso del danneggiato o nell'adempimento di un dovere (art. 7:101).

Come anticipato, la normativa dei PETL non risulta esauriente. Appare utile, quindi, procedere ad una specificazione dei medesimi concetti alla luce del sistema giuridico italiano.

In ossequio al principio romano del *neminem laedere*, l'art 2043 del codice civile italiano dispone che "qualunque fatto doloso o colposo, che cagioni ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno". Da detta norma è possibile dedurre i presupposti che dovranno essere provati dal danneggiato (secondo il brocardo *onus probandi incumbit ei qui dicit*) per ottenere il risarcimento del danno: il fatto (cioè ciò che cagiona il danno); l'imputabilità del fatto al danneggiante; il dolo, per tale intendendosi l'intenzionalità della condotta, o la colpa, ossia il difetto della diligenza (cioè la negligenza, o mancanza dell'attenzione richiesta), della prudenza (cioè l'imprudenza, o mancanza delle necessarie misure di cautela), della perizia (cioè l'imperizia, o inosservanza delle regole tecniche di una determinata attività) richieste, del danneggiante; il nesso di causalità fra il fatto e l'evento dannoso; il danno.

Perché un danno possa essere rilevante ai fini dell'attribuzione di responsabilità esso deve essere un danno ingiusto. Un danno è definito come ingiusto, quando è "cagionato *non iure*: cioè, non nell'esercizio di un diritto dall'ordinamento riconosciuto al danneggiante"[146], secondo il principio *qui iure suo utitur neminem laedit*. Allo stesso modo non può essere ritenuto ingiusto il danno che è causato nell'adempimento di un dovere, cioè imposto da una norma giuridica o da un ordine derivante dalla pubblica autorità. Ancora, gli artt. 2044-2045 sono dedicati alle cause di giustificazione: in

---

[145] Circa la differenza fra legittima difesa e auto-tutela (*self-help* nella versione inglese), la prima riguarda la difesa dei propri interessi protetti contro una aggressione ingiustificata, la seconda, l'aver commesso il fatto perché l'intervento delle autorità non poteva essere ottenuto in tempo

[146] Andrea Torrente, Piero Schlesinger, & Franco Anelli, Carlo Granelli, *Manuale di Diritto Privato* (ventiduesima ed., 2015 Milano: Giuffrè), p. 912.

particolare, l'ingiustizia del danno è esclusa quando quest'ultimo è arrecato per legittima difesa o in stato di necessità[147].

Quanto alla responsabilità oggettiva, essa si caratterizza in quanto il soggetto danneggiante risponde del danno anche in assenza di dolo e di colpa. In questa evenienza, il danneggiato non avrà l'onere di provare la colpa del danneggiante e quest'ultimo non potrà sottrarsi a responsabilità.

Il legislatore italiano, oltre alle ipotesi di responsabilità oggettiva, ha previsto una serie di ipotesi in cui il danneggiato è maggiormente tutelato e il danneggiante, di contro, vede la sua posizione aggravata. A tal proposito si parla, infatti, di responsabilità "aggravata", nella quale il danneggiato non dovrà fornire la prova della colpa del danneggiante; quest'ultimo sarà chiamato a fornire la c.d. "prova liberatoria", la quale non si riduce alla dimostrazione di aver operato secondo diligenza, prudenza o perizia, ma richiede un qualcosa in più, diverso per ogni fattispecie di responsabilità.

È proprio nella disciplina della responsabilità "aggravata" che rileva la fattispecie delle "attività pericolose" (che, invece, nei PETL e nella *common law* statunitense è pura responsabilità oggettiva). In base all'art. 2050 del codice civile italiano "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". D'altra parte, la giurisprudenza italiana[148] non si limita a richiedere, per l'esonero di responsabilità, la prova dell'assenza di colpa, ma richiede la prova positiva dell'imprevedibilità di una causa esterna[149].

Indipendente dalla qualifica di oggettiva o di aggravata della responsabilità, i vari ordinamenti concordano nel ritenere che fra le attività pericolose rientri l'attività medica. È opportuno, poi, notare che il campo medico, e in particolare quello

---

[147] Stato di necessità qui riguarda l'ipotesi in cui "chi ha compiuto il fatto dannoso vi è stato costretto dalla necessità di salvare sé o altri dal pericolo attuale di un danno grave alla persona" (art. 2045 c.c. it.).

[148] Cass. civ., Sez. III, 22 dicembre 2011, n. 28299.

[149] Tale prova ulteriore fa ritenere alcuni autori che per le attività pericolose debba parlarsi di responsabilità oggettiva, piuttosto che di responsabilità "aggravata".

chirurgico, è uno dei settori che maggiormente vede la presenza dei robot. Occorre quindi domandarsi come questi ultimi siano regolamentati.

Fra i robot-chirurgici più famosi al mondo, grazie anche a caratteristiche tecniche innovative, vi è il "Da Vinci" di Intuitive Surgical Inc. Un uso intensivo di questi robot negli Stati Uniti ha fatto emergere una pluralità di casi e correlativi problemi giuridici.

In primo luogo, occorre tener presente che i sistemi "Da Vinci" rientrano nella categoria dei robot-teleoperati, in quanto sempre telecomandati da un operatore umano, e sono passabili di rientrare nella categoria dei prodotti, sia negli USA che in Europa[150].

Ciò considerato, nell'eventualità in cui si verifichi un danno è necessario stabilire se questo sia stato causato da un difetto del prodotto, dalla negligenza del medico-operatore o da entrambi. A tal proposito, appare utile riportare il caso *Mracek v. Bryn Mawr Hosp.* della *District Court, E.D.* della Pennsylvania, avente per oggetto proprio un robot "Da Vinci".

Il 9 giugno 2005, Roland C. Mracek è stato sottoposto ad una prostatectomia mediante un robot "Da Vinci". L'utilizzo del robot era stato fortemente consigliato dal Dr. McGinnis "*as to minimize the risk of erectile dysfunction*"[151]. Nella fase iniziale della procedura il robot ha iniziato a mostrare messaggi di errore; dopo un tentativo da parte del team chirurgico di riavviarlo, il robot è stato portato fuori dalla sala operatoria e i medici hanno proseguito l'intervento. Una settimana dopo il completamento dell'intervento, Mracek ha sofferto una ematuria che ha condotto ad un nuovo ricovero in ospedale. Egli ha quindi intentato una causa sia per responsabilità da prodotto difettoso sia pere negligenza del medico, sostenendo che, come risultato diretto della procedura, ora soffre di disfunzione erettile.

Particolarmente interessanti sono state le conclusioni della Corte in relazione ai vari capi di accusa: quanto alla responsabilità da prodotto difettoso, Mracek non ha offerto una perizia tecnica a sostegno della tesi del difetto del prodotto, sostenendo l'ovvietà del difetto dovuto al fatto che il robot ha mostrato diversi messaggi di errore; la Corte non è

---

[150] Tuttavia, non possono essere considerati macchine secondo la direttiva 2006/42/CE, ma come dispositivi medici sulla scorta della direttiva 93/42/EEC.

[151] Mracek *v.* Bryn Mawr Hosp., 610 F. Supp. 2d 401 (E.D. Pa. 2009).

stata dello stesso avviso, affermando non solo che, in assenza di una relazione di un esperto, il messaggio di errore non poteva essere assimilato ad un vero e proprio difetto ai fini della responsabilità oggettiva per prodotti, ma anche che quest'ultima non poteva essere attivata, avendo Mracek mancato di dimostrare il nesso di causalità tra ciò che è accaduto in sala operatoria con il robot "Da Vinci" e la sua disfunzione erettile.

Quanto alla questione della negligenza del Dr. McGinnis, la Corte ha prima segnalato che "*a* prima facie *negligence claim requires the plaintiff to show that: (1) the defendant had a duty to conform to a certain standard of conduct; (2) the defendant breached that duty; (3) such breach caused the injury in question; and (4) the plaintiff incurred actual loss or damage*"[152] e che è proprio l'assenza di prove allegata da Mracek circa il nesso di causalità che esclude la responsabilità medica.

Le caratteristiche dei sistemi "Da Vinci" e alcune scelte aziendali della Intuitive Surgical Inc. impongono una rimodulazione dell'attribuzione di responsabilità, anche alla luce di quanto detto in tema di prodotto difettoso.

Proprio per quanto riguarda il prodotto difettoso, un semplice malfunzionamento (come avvenuto nel caso Mracek) non potrà dare adito a responsabilità. Tuttavia, "*a system malfunction could even injure the organs of the patient, for example, with a sudden and uncontrolled movement of the robot's arm which has not been put into action by the surgeon*"[153]; in questa eventualità il danneggiato dovrà dare prova del danno, del difetto e del nesso di causalità. D'altra parte, "*under the current terms of sale for the Da Vinci these data are not accessible to any of the patient, the surgeon and the hospital, even in the case where the latter was the owner of the robot; they can be extracted only by a technician from Intuitive Surgical Inc*"[154].

Se, invece, si verifica un danno nonostante un corretto funzionamento della macchina, allora si tratterà di un caso di responsabilità medica. Tuttavia, in una operazione

---

[152] *ibid.*

[153] Erica Palmerini, F. Azzarri, F. Battaglia, A. Bertolini, A. Carnevale, J. Carpaneto, F. Ca- vallo, A. Di Carlo, M. Cempini, M. Controzzi, B.J. Koops, F. Lucivero, N. Mukerji, L. Nocco, A. Pirni, H. Shah, P. Salvini, M. Schellekens, K. Warwick, "*RoboLaw project*" (D6.2 Guidelines on Regulating Robotics, 2014), p. 95.

[154] Chiara Boscarato, "*Robotics, Innovation and Law*", in A. Santosuosso (ed.), "*The challenge of Innovation in Law*" (Pavia, 2015), p. 232.

chirurgica manuale, è presente un team in cui ciascun membro ha dei compiti e per quelli è responsabile; inoltre, ogni membro del team dovrà controlla la condotta degli altri, avendo il dovere di intervenite se ritiene che stia per essere commesso un errore.
La situazione cambia se vengono introdotti sistemi come quello "Da Vinci": solo un operatore può manovrare i bracci meccanici del robot, mentre gli altri chirurghi osservano l'intervento; l'operatore si trova, quindi, in una posizione privilegiata rispetto agli altri membri del team. Ciò significa, però, che "*the civil liability due to an error in the movement of the robot arm or a bad judgment on how to proceed should be attributed exclusively to the operating surgeon. Other surgeons are exempt from responsibility because they are not physically able to work, being bound to a subordinate position*"[155].

4.3.4. Considerazioni conclusive in tema di responsabilità extracontrattuale dei robot-oggetti.

La sempre maggiore presenza di robot in ambiti sia ludico-educativi (ad es. iPal) che in ambiti professionali (ad es. i sistemi "Da Vinci") richiede un aggiornamento della disciplina della responsabilità extracontrattuale.
Nei prodotti potenzialmente dannosi composti da una parte hardware ed una software, è opportuno considerare la responsabilità dello sviluppatore come separata rispetto al produttore della parte fisica; la caratterizzazione del consumatore quale "soggetto debole", invita ad una rimodulazione dell'onere della prova, soprattutto quando una serie di informazioni siano di difficile reperimento. Se da una parte, "*for these reasons, the suggestion has been advanced for an European law that imposes an obligation on the manufacturer to implement software that allows access and use of its data by the user – or, at least, the obligation to provide such data on request*"[156], appare maggiormente utile invertire l'onere di prova, di modo tale che sia lo sviluppatore del software a dover fornire la prova contraria circa l'esistenza del difetto.

---

[155] *ibid.* p. 233.

[156] *ibid.* p. 232.

Qualora il robot venga utilizzato per lo svolgimento di determinate attività, il suo impiego dovrebbe essere circoscritto nel campo della "*extrema ratio*". Ciò è tanto più vero qualora si considerino le attività "pericolose", quale è quella medica. Nello svolgimento di simili attività, l'uso di robot dovrebbe essere raccomandato soltanto qualora sia assolutamente migliore del metodo manuale (come avvenuto in Mracek, ove il Dr. McGinnis aveva fortemente consigliato l'uso del "Da Vinci" per minimizzare possibili complicazioni della procedura); l'utente (nel caso medico, il paziente), poi, dovrà essere informato non solo del fatto che si procederà con modalità non tradizionali (cioè tramite robot), ma anche dei maggiori rischi che la modalità robotica possa comportare.

Se poi il robot venisse effettivamente utilizzato ed un danno fosse causato per un errore dell'operatore, la responsabilità ricadrà esclusivamente su quest'ultimo, in quanto unico soggetto che si trovava alla *master console*; come chiarito poco fa in ambito chirurgico, "*the liability rules concerning computer-assisted surgery should be excluded for the surgeons who are not at the master console, whenever the damage to the patient was provoked by an action of the robot triggered by the user*"[157].

4.4. La responsabilità extracontrattuale fra robot-oggetti e robot-agenti.

La disciplina finora tratteggiata faceva particolare riferimento ai robot-oggetti, ma cosa cambia se questi sistemi vengono dotati di una intelligenza artificiale? Di nuovo, non è fantascientifico pensare che fra qualche anno, fra le corsie di un ospedale, non possa circolare un robot chirurgo. È sicuramente questo l'obiettivo ultimo di Google e Johnson & Johnson che, nel 2015, hanno creato la startup "Verb Surgical"; caratterizza alcuni sistemi robotici di questa compagnia la presenza del *machine learning* (che, si ricorderà, è uno dei tratti caratteristici delle IA), aspetto particolarmente interessante,

[157] *op. cit.* Erica Palmerini, "*RoboLaw project*", p. 96.

considerato che "*existing commercial surgical robots have mostly steered far away from any kind of learning behaviors or anything that is in the least bit autonomous*"[158].

La presenza di intelligenza artificiale e di autonomia sono concetti che vanno di pari passo, ma è necessario considerare che è proprio il grado di autonomia che interessa l'attribuzione di responsabilità. In altre parole, tanto maggiore è l'autonomia dell'IA, tanto minore sarà il controllo umano, tanto meno potrà essere richiesto a quest'ultimo di assumersi responsabilità per i comportamenti della prima. Di conseguenza, occorre in primo luogo distinguere i vari livelli di autonomia delle IA.

Sebbene siano presenti una pluralità di livelli per ogni diversa applicazione delle intelligenze artificiali[159], ritengo che una buona base di partenza possano essere i sei livelli di autonomia per gli autoveicoli a guida autonoma definiti dalla *Society of Automotive Engineers* (SAE):

- Livello 0 (*No Driving Automation*): assenza di automazione, il veicolo è controllato interamente dall'uomo. Possono, tuttavia, esistere in questo livello sistemi in grado di aiutare il guidatore, quali sistemi di frenata d'emergenza.
- Livello 1 (*Driver Assistance*): minima automazione, il sistema controlla solo alcuni aspetti della guida, ma la maggior parte dei compiti è svolta dall'uomo. I sistemi di *cruise control* rientrano in questa categoria.
- Livello 2 (*Partial Driving Automation*): si tratta si sistemi avanzi che assistono la guida (o ADAS), ma non si può parlare propriamente di guida autonoma in quanto, sebbene il sistema controlli frenata/accelerazione/ostacoli, l'essere umano può

---

158 Evan Ackerman, "*Google and Johnson & Johnson Conjugate to Create Verb Surgical, Promise Fancy Medical Robots*" *IEEE Spectrum*, 17 dicembre 2015, disponibile presso https://spectrum.ieee.org/automaton/robotics/medical-robots/google-verily-johnson-johnson-verb-surgical-medical-robots (ultimo accesso 25 settembre 2020).

159 A titolo esemplificativo, l'informatico Noel Sharkey distingue cinque livelli di autonomia per i *Lethal Autonomous Weapons Systems*: 1. L'essere umano determina l'obiettivo prima di iniziare qualsiasi attacco; 2. il programma fornisce un elenco di obiettivi e l'uomo sceglie quale attaccare; 3. il programma seleziona l'obiettivo e l'uomo deve approvare prima dell'attacco; 4. il programma seleziona l'obiettivo e l'uomo ha un limitato tempo di veto; 5. Il programma seleziona il bersaglio e avvia l'attacco senza il coinvolgimento umano. Sul punto cfr. Noel Sharkey, "*Towards a principle for the human supervisory control of robot weapons*", Special Issue on "*Investigating the Relationship between Future Technologies, Self and Society*" (Politica & Società, No. 2, maggio-agosto 2014); cfr. anche Expert meeting, "*Autonomous weapon systems: Technical, military, legal and humanitarian aspects*" (Geneva, Switzerland, 26-28 marzo 2014).

sempre riprendere il controllo della macchina (ad es. i sistemi di guida autonoma Tesla rientrano in questa categoria).

- Livello 3 (*Conditional Driving Automation*): il passaggio a questo livello è sostanziale dal punto di vista tecnologico, ma sottile se non trascurabile dal punto di vista umano. Tali veicoli, infatti, hanno capacità di "rilevamento ambientale" e possono prendere decisioni informate da soli, come accelerare davanti a un veicolo che si muove lentamente, ma l'*override* umano è sempre possibile e, di conseguenza, il conducente deve rimanere vigile e pronto a prendere il controllo se il sistema non è in grado di eseguire l'attività (un simile sistema è stato implementato nell'Audi A8, con il *Traffic Jam Pilot*)
- Livello 4 (*High Driving Automation*): tali veicoli possono intervenire se le cose vanno male o si verifica un guasto del sistema. In tal senso, queste auto non richiedono l'interazione umana nella maggior parte delle circostanze, ma l'essere umano ha ancora la possibilità di eseguire l'*override* manualmente. Veicoli di livello 4, considerato che le infrastrutture non sono ancora in grado di accoglierli su larga scala, si prestano ad essere utilizzati in aree limitate, in particolare in aree urbane (ad es. NAVYA, società francese, costruisce e vende navette e taxi di livello 4 negli Stati Uniti che funzionano completamente con energia elettrica e possono raggiungere una velocità massima di 55 mph).
- Livello 5 (*Full Driving Automation*): l'attenzione e il controllo umani sono totalmente eliminati, tant'è vero che non sono presenti né volante né pedali di accelerazione/frenata. Il sistema è in grado di guidare come un pilota esperto, anche al di fuori di aree limitate. Veicoli di livello 5, sebbene in fase di sperimentazioni, non sono ancora disponibili al pubblico.

Sulla scorta di questa divisione, estendendola anche a campi diversi dai veicoli, possono distinguersi tre fasce di autonomia delle IA: una prima fascia (livelli 0 e 1) in cui non si può parlare di IA *strictu sensu* e la cui disciplina ricade per la maggior parte o nella responsabilità da prodotto difettoso o nelle regole generali della responsabilità extracontrattuale (*v. supra*). Una seconda fascia (livelli 2 e 3) in cui la parziale autonomia potrebbe richiedere una revisione delle regole generali. Infine, una terza

fascia (livelli 4 e 5) in cui la piena autonomia impone una rimodulazione totale delle regole preesistenti o l'introduzione di nuove norme. Considerato che l'analisi della prima fascia è racchiusa nei precedenti paragrafi, è possibile passare subito a considerare le intelligenze artificiali della seconda e terza fascia.

4.5. La responsabilità extracontrattuale dei robot-agenti della seconda fascia.

Consideriamo, in primo luogo, le intelligenze artificiali della seconda fascia e cerchiamo di estrapolare le loro caratteristiche principali, basandoci sui livelli di autonomia dei veicoli. Sebbene si tratti di un ovvietà, tali IA devono essere autonome: per autonomia si può intendere sia la capacità di decidere per sé sia la capacità di muoversi liberamente nello spazio; devono, poi, essere in grado quantomeno di percepire l'ambiente circostante ed essere in grado di apprendere dallo stesso. D'altra parte, deve trattarsi di sistemi nei cui confronti l'essere umano possa esercitare un elevato grado di controllo. Tali qualità, caratterizzano, come detto prima, le odierne auto a guida autonoma, ma potrebbero anche appartenere ad una versione più evoluta di iPal, in grado di interagire con un bambino in maniera molto più simile a quella di un suo coetaneo, oppure, secondo l'esempio fornito da A. Santosuosso *et al.*, ad un Ro-Dog, un robot che emuli le sembianze e il comportamento di un animale.

Ci se deve, dunque, interrogare se le normative tradizionali possano essere adatte a queste forme di intelligenza artificiale o necessitino di adattamenti. In considerazione degli esempi poc'anzi proposti, possono fungere da punto di partenza le regole in tema di responsabilità per fatto altrui e/o di danno cagionato dall'animale. Nell'analisi di queste discipline si farà nuovamente riferimento alla *common law* statunitense, ai PETL e all'ordinamento italiano.

4.5.1. (Segue): la responsabilità per danni cagionati da animali.

Analizziamo, innanzitutto, la disciplina dei danni cagionati dagli animali e prendiamo ad esempio la seguente situazione: Ro-Dog, grazie ad una molteplicità di sensori, è in grado di aiutare le persone anziane, che hanno difficoltà a chinarsi, a raccogliere oggetti da terra; nell'accompagnare il suo proprietario, i sensori di Ro-Dog confondono un semplice pezzo di carta con un giornale e si dirigono a raccoglierlo, ma in quello momento sta passando un ragazzo in bici; non potendo evitarlo, il ragazzo si scontra con Ro-Dog e, cadendo, si frattura il polso. Una simile vicenda è assimilabile a quella di un cane domestico che, scambiando una mano che si avvicina per una carezza con un gesto di aggressione, morde, ferendo, un passante. Orbene, in entrambi i casi, la domanda da porsi è la medesima: chi è responsabile per il danno causato?

Negli Stati Uniti, ai fini della responsabilità per danni diversi dal *trespass*[160], la legge distingue fra animali domestici e animali selvatici. Il detentore di animali domestici (quali cani, gatti, cavalli, ecc.) è responsabile oggettivamente per il danno da essi causato solo se era effettivamente a conoscenza che l'animale presentava un particolare tratto o propensione a causare un simile danno[161]. I detentori di specie considerate "selvatiche" sono oggettivamente responsabili dei danni provocati, indipendentemente dal fatto che l'animale in questione sia noto o meno come pericoloso. La distinzione si fonda sul fatto che "*because such animals are known to revert to their natural tendencies, they are considered to be wild no matter how well trained or domesticated*"[162].

Dal canto loro i PETL non disciplinano autonomamente la responsabilità dei danni causati dagli animali, quindi si farà direttamente riferimento alla normativa italiana.

---

[160] La violazione, ad oggi, consiste in un ingresso non autorizzato sulla terra altrui. Una simile violazione conferisce alla parte lesa il diritto di intentare una causa civile e di ottenere il risarcimento dei danni per l'interferenza e per qualsiasi altro danno subito.

[161] È bene notare come alcuni Stati abbiano emanato degli statuti che attribuiscono la responsabilità per i morsi di un cane al padrone, anche in assenza della conoscenza della ferocia del cane.

[162] Law Library - American Law and Legal Information, "*Strict Liability*", disponibile presso https://law.jrank.org/pages/10551/Strict-Liability.html (ultimo accesso 25 settembre 2020).

Mentre in America la responsabilità per danni cagionati da animali è configurata come responsabilità oggettiva, in Italia rientra nella categoria della responsabilità "aggravata"; il dispositivo dell'art. 2052 del codice civile stabilisce che "il proprietario di un animale o chi se ne serve per il tempo in cui lo ha in uso[163], è responsabile dei danni cagionati dall'animale, sia che fosse sotto la sua custodia, sia che fosse smarrito o fuggito, salvo che provi il caso fortuito". In merito alla prova liberatoria del "caso fortuito", ancora una volta la giurisprudenza italiana non si accontenta della prova dell'utilizzo della normale diligenza nella custodia dell'animale, ma richiede che la causa esterna sia assolutamente non prevedibile e non evitabile[164]. Come avviene per la responsabilità in "attività pericolose", dunque, anche in questo caso la prassi giurisprudenziale pare trattare questa tipologia di responsabilità "aggravata" come sostanzialmente oggettiva.

Proprio la soluzione della responsabilità oggettiva appare suscettibile di estensione anche ai danni causati dalle IA autonome della c.d. "seconda fascia", in quanto la norma "si rivela idonea a disciplinare il "fatto" di "cose" dotate di intelligenza artificiale, così come l'art. 2052 c.c. detta una disciplina identica alla responsabilità per fatto dell'intelligenza (naturale) animale (anch'essa self-learning)"[165]; potrebbe applicarsi anche la disciplina statunitense per i detentori di animali domestici, a patto che il proprietario dell'IA si consideri sempre a conoscenza dei tratti caratteristici (*rectius* delle caratteristiche tecniche) del prodotto che acquista.

Alcuni autori ritengono applicabile ai sistemi autonomi anche il disposto dell'art. 2051 del codice civile italiano, secondo cui "ciascuno è responsabile del danno cagionato dalle cose che ha in custodia". La disciplina dell'art. 2051 e dell'art. 2052 c.c.it. non presenta sostanziali differenze, ma quello che in questa sede preme rilevare è come nell'art. 2051 si faccia riferimento alle "cose": una assimilazione a queste ultime

---

[163] Comparando la la disciplina statunitense con quella appena esposta, è bene notare come in America si faccia riferimento al "detentore" dell'animale, mentre nell'ordinamento italiano la relativa responsabilità ricade su chi utilizza l'animale (che di regola è il proprietario, ma può anche essere un soggetto terzo che esercita un c.d. "potere di governo" su di esso).

[164] Cfr. Cass. civ., Sez. III, 22 marzo 2015, n. 7260.

[165] Ugo Ruffolo, Guido Alpa, Augusto Barbera, "Intelligenza artificiale: il diritto, i diritti, l'etica" (Milano: Giuffrè, 2020), p. 115.

degraderebbe le IA a meri oggetti, eliminando totalmente il loro connotato di "esseri" attivi.

4.5.2. (*Segue*): la responsabilità per fatto altrui.

Altra parte della dottrina, basandosi "sulla sostanziale differenza tra animali […] e sistemi di IA, per cui, nei primi, autodeterminazione e istinto li porterebbero ad azioni diverse da quelle per le quali sono addomesticati"[166], ritiene preferibile l'estensione delle norme sulla responsabilità per fatto altrui (anche nota come responsabilità vicaria) ai sistemi intelligenti.

Nella *common law* statunitense, la *vicarious liability* è la responsabilità attribuita ad un soggetto che assume una posizione di supervisione (come un datore di lavoro) per la condotta di un suo subordinato (come un dipendente), sulla base del rapporto intercorrente fra le due parti. Tale responsabilità si fonda sulla dottrina del "*respondeat superior*", in base alla quale un soggetto è legalmente responsabile per gli atti commessi da un proprio dipendente o agente, se tali atti si verificano nell'ambito del lavoro o dell'agenzia. La *vicarious liability* è un istituto assai flessibile, che racchiude al suo interno altre forme di responsabilità "*relating to wild and domestic animals, children, unpredictable actors under supervision such as prisoners and even slaves*".

Nei PETL la disciplina del fatto altrui è contenuta in due articoli, concernenti la responsabilità per fatto dei minori o incapaci psichici e per fatto degli ausiliari: l'art. 6:101 stabilisce che "chiunque sia tenuto alla sorveglianza di un minore o di un soggetto affetto da disabilità psichica è responsabile per il danno causato da questi, salvo che non provi di avere osservato lo standard di condotta richiesto nella sorveglianza"; l'art. 6:102 dispone che la "chiunque è responsabile per il danno causato dai propri ausiliari, che agiscono nell'ambito delle proprie funzioni, in violazione dello standard di condotta richiesto". Nel primo caso si è in presenza di responsabilità extracontrattuale classica (ove la prova liberatoria si sostanzi a nella dimostrazione dell'assenza di negligenza, imprudenza o imperizia), mentre nel secondo caso si tratta di responsabilità oggettiva.

---

[166] *op. cit.* Laura Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, p. 725.

Nell'ordinamento italiano molteplici sono le fattispecie ricondotte alla responsabilità per fatto altrui. Tuttavia, tale forma di responsabilità, anche nota come responsabilità c.d. indiretta, si caratterizza per il fatto che alla responsabilità dell'autore dell'illecito si aggiunge quella del terzo (ciò al fine di migliorare la posizione del danneggiato, che potrà rivolgersi per il risarcimento ad un ulteriore soggetto). Ai fini dell'analisi che si sta conducendo, ritengo che due siano gli articoli maggiormente rilevanti e cioè gli artt. 2048 e 2049 del codice civile.

L'art. 2048, al primo comma, disciplina il danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone sottoposte a tutela, di cui rispondono, rispettivamente, i genitori e/o il tutore; al secondo comma, si attribuisce la responsabilità per i danni cagionati a terzi dal fatto illecito commesso da allievi ed apprendisti nel tempo in cui sono sotto la loro vigilanza, ai precettori e coloro che insegnano un mestiere o un'arte[167]. L'art. 2049, invece, ritiene responsabili dei danni cagionati a terzi da fatto illecito commesso da domestici e commessi nell'esercizio le incombenze a cui sono adibiti, i padroni e i committenti[168]. Una sostanziale differenza fra i due istituti è meritevole di attenzione: quanto alla prova liberatoria, i soggetti obbligati a norma dell'art. 2048 possono liberarsi provando di non aver potuto impedire il fatto; i soggetti obbligati a norma dell'articolo 2049, invece, non possono sottrarsi a responsabilità, rispondendo a prescindere da qualsiasi colpa.

Orbene, dopo aver esposto i tratti essenziali di questa particolare tipologia di responsabilità, ritengo condivisibili le argomentazioni della dottrina contraria all'equiparazione fra responsabilità genitoriale (o del tutore) e responsabilità dell'utilizzatore di sistemi intelligenti; sebbene "tali norme appaiono suscettibili, in astratto, di interpretazione anche analogica (oltre che estensiva), […] esse sembrano, tuttavia, fuori causa, in quanto tarate sulla specificità della natura umana dell'essere […] del cui "illecito" si risponde, dettando così una disciplina molto settoriale,

---

[167] Si fa qui riferimento a tutti quei soggetti cui il minore è affidato per fini di istruzione.

[168] Perché possa trovare applicazione tale norma deve intercorrere il c.d. rapporto di preposizione, per cui "un soggetto (preponente) si appropria, a titolo oneroso ovvero gratuito, delle utilità derivanti dall'attività di altro soggetto (preposto), che opera sotto il potere di direzione e sorveglianza del preponente"; cfr. *op. cit.* Andrea Torrente, *Manuale di Diritto Privato*, pp. 938-939.

modulata sulla particolare tipologia di minorata capacità di intendere e volere di un soggetto"[169].

D'altra parte, è mia opinione che la fattispecie dettata dall'art. 2049 si presti maggiormente ad una applicazione estensiva: ciò in quanto essa non trova il suo fondamento in particolari tratti o caratteristiche del soggetto che determina il danno (come avviene per la responsabilità genitoriale), ma sul fatto che gli oneri debbono essere a carico di chi gode dei benefici di un bene (secondo il principio *cuius commoda eius et incommoda*). Tale norma risulta essere anche più efficace di una estensione della normativa sul danno provocato da animali, poiché l'imprevedibilità del comportamento di robot intelligenti, potrebbe portare ad un eccessivo utilizzo della prova liberatoria circa l'assoluta imprevedibilità e inevitabilità del comportamento del sistema, indebolendo indebitamente la posizione del soggetto danneggiato.

Un simile approccio sembra essere stato seguito in Germania, in relazione ai veicoli a guida autonoma (appartenenti alla seconda fascia): il proprietario di un veicolo a guida autonoma è responsabile oggettivamente per i danni causati dal suo veicolo, indipendentemente dal fatto che l'auto fosse in modalità "guida autonoma" o fosse governata manualmente. È opportuno notare che il guidatore, se diverso dal proprietario, "*in case of an accident due to an error of the automated system, […] is not liable, even if the accident could have been prevented by monitoring the system constantly*"[170]. La nuova disciplina del codice della strada tedesco (*Straßenverkehrsgesetz*) sembra alleggerire il dovere di prestare costante attenzione: al guidatore è infatti consentito di distogliere lo sguardo dal traffico, purché mantenga un livello di attenzione tale da poter riassumere il controllo del veicolo su richiesta

---

[169] *op. cit.* Ugo Ruffolo, "Intelligenza artificiale: il diritto, i diritti, l'etica", p. 115.

[170] Dr. Jan-Erik Schirmer, "*Germany's half-hearted draft law on automated vehicles*", disponibile presso https://www.jura.fu-berlin.de/fachbereich/einrichtungen/zivilrecht/lehrende/schweitzerh/informationen/Datenordner/Autonomous-Driving/002-SlidesAutomatedVehicles.pdf (ultimo accesso 25 settembre 2020).

dell'automazione o a seguito di evidenti malfunzionamenti tecnici; al di fuori di queste situazioni il conducente dovrebbe rimaner esente da responsabilità[171].

4.6. Considerazioni conclusive sulla responsabilità extracontrattuale dei robot-agenti della seconda fascia.

Una eventuale applicazione estensiva della norma dell'art. 2049 c.c.it. non risulta comunque del tutto efficace per affrontare le sfide giuridiche poste da robot-agenti della seconda fascia. È necessaria infatti una rimodulazione di tale disciplina, anche in considerazione di quanto proposto dal Parlamento Europeo.

La risoluzione rubricata "Norme di diritto civile sulla robotica" del 16 febbraio 2017 propone come possibili soluzioni normative due modelli alternativi: l'approccio della responsabilità oggettiva o quello della gestione dei rischi.

La responsabilità oggettiva "richiede una semplice prova del danno avvenuto e l'individuazione di un nesso di causalità tra il funzionamento lesivo del robot e il danno subito dalla parte lesa", mentre l'approccio di gestione dei rischi si concentra "sulla persona che, in determinate circostanze, è in grado di minimizzare i rischi e affrontare l'impatto negativo".

La responsabilità oggettiva, così come definita dal Parlamento Europeo, potrebbe essere modellata sulla falsariga della responsabilità prevista dall'2049 c.c.it.

D'altra parte, un miglior risultato potrebbe essere raggiunto considerando i due approcci come complementari: "la responsabilità oggettiva prescinde dall'elemento soggettivo della colpevolezza; l'approccio di gestione dei rischi serve per individuare il responsabile, tra più soggetti potenzialmente coinvolti nel verificarsi del danno, nel soggetto causalmente «più vicino al prodotto»"[172]. Così modulata, la fattispecie consentirebbe alla parte lesa di agire sia nei confronti del "datore di lavoro" (*rectius*

---

[171] La differenza è sostanziale con, ad esempio, il disposto dell'art. 2054 del codice civile italiano, che, in tema di danni prodotti dalla circolazione del veicolo, prevede che il conducente possa liberarsi da responsabilità dando la "prova di aver fatto tutto il possibile per evitare il danno".

[172] *op. cit.* Laura Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, p. 727.

dell'utilizzatore) del sistema intelligente, sia nei confronti del soggetto che, intervenendo, avrebbe potuto impedire o minimizzare il danno. Ancora, la normativa in tal modo perfezionata, non escluderebbe a priori una responsabilità del produttore e/o sviluppatore, qualora il danno sia provocato da un difetto del prodotto (*v. supra*). In altre parole, il danneggiato avrà una pluralità di soggetti contro cui far valere l'azione risarcitoria; se poi si concluderà che il danno è stato determinato da un difetto di fabbricazione e/o da un bug presente nel software (e non tempestivamente eliminato), allora l'utilizzatore potrà esercitare l'azione di rivalsa nei confronti di questi ultimi soggetti.

4.7. La responsabilità extracontrattuale dei robot-agenti della terza fascia.

Passiamo ora ad analizzare i sistemi intelligenti del terzo tipo, i quali sono caratterizzati da una preminente assenza di controllo umano: la macchina è in grado di svolgere il compito per cui è stata realizzata con le medesime capacità di un essere umano esperto ed è in grado di reagire a situazioni particolarmente difficili, anche qualora tale risposta non sia stata programmata dallo sviluppatore; nessuna supervisione è richiesta all'utilizzatore considerato l'elevato grado di affidabilità del sistema stesso (così, appunto, nei veicoli a guida autonoma di livello 6 sono assenti il volante e i pedali). Sebbene le capacità delle intelligenze artificiali possano aiutare a prevenire la maggior parte degli incidenti dovuti a disattenzione o errore umano (si pensi, ad esempio, a come l'errore umano contribuisca a circa il 90% degli incidenti stradali[173]), ciò non significa che questi stessi incidenti non si verificheranno più. Orbene, la domanda da porsi è chi sarà responsabile (il "chi paga?" di Ugo Pagallo) per questi sinistri e, a tal fine, vengono nuovamente a rilevare le figure dell'utilizzatore, del proprietario, del produttore e dello sviluppatore.

---

[173] Paul Gao, Russell Hensley, Andreas Zielke (14 febbraio 2018), "*A road map to the future for the auto industry*". Disponibile presso https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/a-road-map-to-the-future-for-the-auto-industry (ultimo accesso 25 settembre 2020).

Consideriamo, in prima istanza, la posizione dell'utilizzatore, ad esempio, di un'auto a guida autonoma. Il livello di attenzione richiestogli non è particolarmente differente da quello di una persona che scelga di prendere l'autobus per dirigersi a lavoro: in entrambi i casi al soggetto non sarà richiesto di prestare attenzione all'ambiente circostante in quanto v'è qualcun altro che svolgerà tale compito per lui (il sistema intelligente o l'autista). Se già il regime della colpa e degli oneri di diligenza, prudenza e perizia sono stati alleggeriti per robot-agenti della seconda fascia (*v. supra* la normativa tedesca), è lecito attendersi che tali oneri cesseranno di esistere per i sistemi intelligenti della terza fascia.

In assenza del requisito della colpa, l'unica via praticabile sembra essere quella della responsabilità oggettiva. Tuttavia, è necessario considerare l'impossibilità per l'utilizzatore di esercitare un pieno controllo sul sistema: sebbene la creazione di sistemi autonomi del terzo tipo (in particolare di livello 5) debba attuarsi in ossequio alla dottrina del c.d. *human-governing-the-loop* (che comporterebbe la presenza di un *master switch*, che, continuando con l'esempio delle *self-driving cars*, potrebbe realizzarsi mediante sofisticati sistemi di freno "a mano"), ciò non significa che l'utilizzatore possa prendere pienamente il comando della macchina; se quanto appena detto fosse comunque possibile, non si potrebbe richiedere una costante attenzione dell'utilizzatore in modo tale da poter prendere il comando quando se ne presenti la necessità poiché il fine ultimo della realizzazioni di veicoli a guida autonoma è proprio sollevare l'essere umano da queste "fatiche". Ancora, applicando una responsabilità oggettiva in ossequio alla dottrina *cuius commoda eius et incommoda*, si aggraverebbe eccessivamente, ed ingiustamente, la posizione dell'utilizzatore; ad analoga conclusione può giungersi per il proprietario diverso dall'utilizzatore.

In definitiva, il solo fatto di possedere un sistema autonomo di terza fascia non può essere fonte di responsabilità.

4.7.1. (*Segue*): la posizione del produttore e dello sviluppatore e i c.d. *social dilemmas*.

Premesso che se il sinistro è provocato da un difetto del robot-agente potrà sempre essere invocata la responsabilità del produttore e/o dello sviluppatore, è opportuno domandarsi se questa stessa responsabilità possa sorgere quando il danno derivi non da un da un difetto del robot, ma da un suo comportamento: in via del tutto generale "se il comportamento è stato impostato come standard dal produttore, certamente sì. La situazione cambia notevolmente se, invece, si considera un robot con capacità di apprendimento, che è capace di «imparare» nuovi comportamenti e reazioni per effetto della propria esperienza e interazione con l'ambiente"[174]. La capacità di apprendimento è stata da alcuni autori ricondotta ad una certa "imprevedibilità" del robot, che impedirebbe il sorgere di una responsabilità da prodotto difettoso. Tale responsabilità, infatti, si basa su una premessa e cioè che "*the manufacturer is able to predict, in a way that the consumer is not, the effects of the product at issue. But where the product is by definition acting in an unpredictable way, the application of this theory of liability may be impossible*"[175]. L'imprevedibilità in questione diventa quindi "*a feature and not a bug. […] Unpredictability derives in part from the fact that its inputs are, in principle, the complete set of information "out there" […] When sets of algorithms act on such a vast set of ever-shifting inputs, the outputs become unpredictable*"[176].

Fra i comportamenti che il sistema intelligente può assumere, si rivela particolarmente problematica la c.d. *dilemma situation*, analizzata con particolare riferimento ai veicoli a guida autonoma, ma estensibile anche ad altri sistemi intelligenti, e cioè come dovrebbe agire una macchina qualora debba scegliere se salvare la vita di uno o più pedoni o quella dell'utilizzatore. La scelta potrebbe essere o predeterminata dal

---

[174] *op. cit.* Amedeo Santosuosso, Chiara Boscarato, Franco Caroleo, *Robot e diritto: una prima ricognizione*, p. 18.

[175] Curtis E.A. Karnow, "*The application of traditional tort theory to embodied machine intelligence*" (The Robotics and the Law Conference, Center for Internet and Society, Stanford Law School, Aprile 2013), p. 14.

[176] Jason Millarand, Ian R. Kerr, "*Delegation, Relinquishment and Responsibility: The Prospect of Expert Robots*" (2013), p. 107.

produttore e/o sviluppatore ovvero lasciata al sistema intelligente. Quest'ultimo potrà basare la sua decisione o sui sensori di cui dispone (ad es. i sensori individuano un pedone e la macchina dovrà evitarlo, anche se ciò comporti un danno per i passeggeri) o su calcoli puramente statistici (se evitare il pedone potrebbe determinare la morte di una pluralità di passeggeri, la macchina non lo eviterà; viceversa, se la macchina dovesse scegliere fra evitare una pluralità di pedoni e rischiare la vita dell'unico passeggero, opterà per la prima soluzione). Il produttore e/o sviluppatore potrà invece determinare, non importa la situazione, se salvare il pedone o il passeggero.

Per rispondere alla domanda su quali canoni tali soggetti debbano basare la decisione, è utile riportare una serie di studi, aventi a riguardo questi *social dilemmas*, condotti nel 2015: nel primo studio, la maggioranza dei partecipanti ha espresso una preferenza per sistemi "morali", programmati per ridurre al minimo il numero di vittime; in un secondo studio, dovendo risolvere dilemmi in cui variavano il numero di vite che potevano essere salvate, i partecipanti non pensavano che si dovesse sacrificare il passeggero quando solo un pedone poteva essere salvato, ma tale sacrificio era ritenuto necessario qualora più pedoni potessero esse salvati; nel terzo studio agli intervistati è stato chiesto di indicare se avrebbero privilegiato l'acquisto un veicolo programmato per ridurre al minimo le vittime, ovvero di un veicolo programmato per dare la priorità alla protezione dei suoi passeggeri, anche a costo di uccidere più pedoni. Sebbene una parte degli intervistati non abbia optato per l'acquisto di un'auto con sistema "morale", è opportuno notare come, comunque, "*the reported likelihood of buying an AV was low even for the self-protective option*"[177].

Sulla base di questi studi, quindi, si può dedurre che la soluzione preferibile è quella di un sistema tarato su basi morali, che opti sempre per il minor sacrifico di vite.

---

[177] Jean-François Bonnefon, Azim Shariff, Iyad Rahwan, "*The Social Dilemma of Autonomous Vehicles*" (Science, Vol. 352, issue 6293, 24 giugno 2016), p. 1574.

D’altra parte, e ai fini di un attribuzione di responsabilità, appare poco conveniente per le case produttrici effettuare a priori la scelta fra passeggero[178] e pedone, in quanto, così facendo si accetterebbe aprioristicamente sacrificio di una delle due “parti”. In considerazione di ciò potrebbe essere fatta valere una azione risarcitoria nei confronti della casa produttrice per i danni, ad esempio, subiti dal pedone, sulla base dell’assenza della dovuta diligenze, prudenza o perizia nella fase di realizzazione del sistema.

4.8. Considerazioni conclusive sulla responsabilità extracontrattuale dei robot-agenti della terza fascia.

L’elevata autonomia di cui sono dotati i sistemi intelligenti del terzo tipo e la conseguente imprevedibilità delle loro azioni, comporta molteplici difficoltà nell’estensione della responsabilità extracontrattuale nei confronti dell’utilizzatore del sistema. Analoghe difficoltà, con i dovuti adattamenti, si presentano nella ricerca del responsabile fra il produttore e lo sviluppatore, i quali, sempre a causa dell’imprevedibilità delle azioni della macchina, non potrebbero essere chiamati a risarcire il danno. D’altra parte non è concepibile che il danneggiato non trovi ristoro per il danno subito; si pone, dunque, il problema di stabilire come detto danno possa essere risarcito.

A tal proposito è condivisibile l’impostazione proposta dal Parlamento Europeo nella Risoluzione del 2017: in tale documento, infatti, si “sottolinea che una possibile soluzione al problema della complessità dell'attribuzione della responsabilità per il danno causato da robot sempre più autonomi potrebbe essere un regime di assicurazione obbligatorio”. Invero, questo sistema di tutela è già stato da tempo adottato per le automobili a guida umana e recentemente è stato imposto in Italia per l’utilizzo di droni (art. 32 del regolamento ENAC per i mezzi aerei a pilotaggio remoto) e si ritiene debba

---

[178] Sembra essere questa la soluzione scelta da Mercedes, le cui macchine saranno programmate per salvare il passeggero piuttosto che il pedone, qualora queste fossero le uniche due soluzioni praticabili. Cfr. David Morris, “*Mercedes' Self-Driving Cars Would Save Passengers, Not Bystanders*” (Fortune, 15 ottobre 2016), disponibile presso https://fortune.com/2016/10/15/mercedes-self-driving-car-ethics/ (ultimo accesso 25 settembre 2020).

essere applicato anche alle intelligenze artificiali che operino nel campo sanitario[179]; ciò considerato la previsione di una assicurazione obbligatoria sarebbe la risposta all'esigenza di tutela del danneggiato.

Più nello specifico, colui che intenda acquistare un robot-agente del terzo tipo dovrebbe sottoscrivere una assicurazione obbligatoria che copra i danni eventualmente causati dal sistema intelligente. Dal canto loro, ai produttori e sviluppatori, consci dell'imprevedibilità che accompagna il prodotto che concorrono a realizzare, dovrebbe essere richiesto di partecipare ad un fondo di garanzia per i danni subiti da persone o cose a causa del comportamento di sistemi intelligenti, di modo che, quandanche il proprietario si sprovvisto di assicurazione, il danneggiato possa trovare ristoro economico.

5. La responsabilità penale nelle controversie che coinvolgono robot e IA.

Nel 1981, un operaio giapponese di 37 anni di nome Kenji Urada entrò in una zona di sicurezza ad accesso limitato in uno stabilimento di produzione Kawasaki, per eseguire alcuni lavori di manutenzione su un robot. Nella fretta, però, non riuscì a spegnerlo completamente. Il potente braccio idraulico del robot spinse l'ingegnere verso alcuni macchinari adiacenti, "*thus making Urada the first recorded victim to die at the hands of a robot*"[180].

Chi è il responsabile per la morte di Urada? Più in generale, occorre chiedersi se sia possibile attribuire ai robot-agenti la responsabilità di reati da essi stessi compiuti. Naturalmente, la questione non potrà porsi per i robot-oggetti: in quanto, appunto, oggetti, cose, essi non potranno mai determinare autonomamente il verificarsi di fatto a

---

[179] Giulia Cavalcanti, "Che succede se sbaglia il robot chirurgo? L'esperto: «Presto assicurazioni obbligatorie anche per IA»" (Sanità Informazione, 7 Agosto 2019), disponibile presso https://www.sanitainformazione.it/lavoro/errore-robot-assicurazioni/ (ultimo accesso 25 settembre 2020).

[180] Yueh-Hsuan Weng, Chien-Hsun Chen & Chuen-Tsai Sun, "*Toward the Human–Robot Co-Existence Society: On Safety Intelligence for Next Generation Robots*" (*Int J of Soc Robotics* 1, 267, 2009"). Disponibile in: https://doi.org/10.1007/s12369-009-0019-1.

rilevanza penale; tuttalpiù essi potranno essere utilizzati come strumento per la commissione di un reato, ma in tal caso si applicheranno le normali regole penalistiche.

Per poter stabilire se un sistema intelligente ed autonomo possa assumersi la responsabilità penale delle proprie azioni, si deve in primo luogo stabilire quando un'azione sia penalmente rilevante. A tal proposito, la scienza criminale distingue una teoria "causalista" e una "finalistica": la teoria "causalista", dai più considerata obsoleta, ritiene che non siano necessari particolari requisiti di volontà perché un'azione abbia rilevanza penale, ponendo l'accento sul comportamento; "ogni movimento del corpo "volontario" è un atto penalmente rilevante salvo che per le azioni automatiche (come i riflessi incontrollabili)[181]". Secondo la più moderna teoria "finalistica" è richiesto un qualcosa in più, un "significato sociale" del comportamento, per cui l'atto umano è diverso dagli altri eventi naturali in quanto esprime una particolare volontà intenzionale e cosciente dell'attore[182].

Applicando queste due teorie alle intelligenze artificiali, per la teoria causalista, i robot-agenti "sarebbero imputabili in sede penale, in quanto loro "agiscono", nel senso che pongono in essere un movimento corporeo voluto (perché frutto dell'esecuzione delle specifiche di programmazione e quindi pienamente previsto)"[183]. Per la teoria finalistica, invece, l'evento non potrebbe essere imputato all'IA in quanto essa manca di quei requisiti di intenzionalità e coscienza nell'agire.

Sicuramente risulta preferibile questa seconda teoria, anche alla luce del fatto che per attribuire una responsabilità penale devono sussistere due elementi: un elemento esterno o fattuale, cioè la condotta criminale (*actus reus*); un elemento interno o mentale, cioè la conoscenza o l'intento generale di determinare l'elemento condotta (*mens rea*); "*if one element is missing, no criminal liability can be imposed*"[184].

---

[181] Maria Beatrice Magro, "*Robot, cyborg* e intelligenze artificiali", in A. Cadoppi "Trattato di Diritto penale - Cybercrime" (Utet Giuridica, 2019), p. 1203.

[182] *ibid*.

[183] Vittorio Guarriello, "L'intelligenza artificiale tra profili giuridici ed alcune delle più attuali applicazioni al servizio della società" (Associazione Romana di Studi Giuridici), disponibile presso https://arsg.it/?p=1781#_ftnref9 (ultimo accesso 25 settembre 2020).

[184] Gabriel Hallevy, "*The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*", (Akron Intellectual Property Journal: Vol. 4, Iss. 2 , Article 1, 2010).

5.1. La responsabilità penale degli enti.

Non sempre l'attribuzione della responsabilità penale si è basata sull'intenzionalità dell'agire dell'uomo, ma, anzi, una simile responsabilità è stata, in taluni casi, attribuita a soggetti diversi dall'essere umano. A tal proposito particolarmente utile si rivela l'*excursus* storico fornito da William Ewald in "*What Was it Like to Try a Rat?*":

"*From the ninth century to the nineteenth, in Western Europe, there are over two hundred well- recorded cases of trials of animals. […] An example is the decision of the Law Faculty of Leipzig condemning a milk cow to death for killing a pregnant woman. […] Among criminal cases of this sort, there are many instances of pigs being condemned to death for infanticide. […] A dog in Austria was placed in prison for a year; at the end of the seventeenth century a he-goat in Russia was banished to Siberia. Pigs convicted of murder were frequently imprisoned before being executed; they were held in the same prison, and under substantially the same conditions, as human criminals*"[185].

Sebbene al giurista moderno tali esempi risultino bizzarri, fuori luogo, ciononostante chiariscono come sia possibile ritenere responsabile, anche in sede penale, qualcuno o qualcosa di diverso dall'uomo.

A riprova di ciò si può considerare la recente introduzione della disciplina della responsabilità amministrativa degli enti dipendente da reato commesso da un soggetto appartenente ad essi.

Fino, infatti, a qualche decennio fa vigeva in europa il principio secondo cui *societas delinquere non potest*[186]. Secondo tale dottrina gli enti non potevano rispondere in sede penale delle proprie azioni, poiché mancavano dell'elemento soggettivo (la *mens rea*) necessario per l'imputazione di un fatto penale. Questa impostazione è rimasta in vigore fino a quando, nel 1988, il Comitato dei Ministri del Consiglio d'Europa non esortò una introduzione (*rectius* reintroduzione, considerato che già nel diritto romano è

---

[185] William B. Ewald, "*Comparative Jurisprudence (I): What Was it Like to Try a Rat?*" (Faculty Scholarship, Paper 1405, 1995), pp. 1903-1905.

[186] Brocardo latino erroneamente attribuito al diritto romano, ma di elaborazione della dottrina tedesca del XIX sec.

ravvisabile una sorta di responsabilità degli enti) di questa tipologia di responsabilità. Nonostante i diversi tempi di adeguamento a questa raccomandazione (in Italia avvenuto con il d.lgs. del 8 giugno 2001, mentre in Spagna si è dovuto attendere fino al 2010), si tratta comunque di una disciplina recente che individua in quelle che sono, fondamentalmente, cose, centri di imputazione di responsabilità penale.

Questa disciplina potrebbe sembrare adeguata per una estensione analogica ad una responsabilità penale dell'intelligenza artificiale.

D'altra parte, "è inevitabile ammettere che, quando le sanzioni colpiscono l'astratta persona giuridica, esse vanno ad incidere, sia pur indirettamente, su quelle persone fisiche che sono […] dietro la persona giuridica"[187]. Ciò considerato, l'estensione analogica ora proposta sembra alquanto vacillare.

Oltretutto, seppure si volesse procedere con questa analogia, v'è da considerare il ruolo svolto dalla pena: nella sua forma embrionale la pena è uno strumento attraverso il quale l'autore del reato paga il suo debito con la società; negli ordinamenti più evoluti la pena deve essere diretta a rieducare l'autore del reato, nel senso che "il tipo e la misura della pena minacciata dal legislatore devono essere tali da rendere possibile che successivamente, nello stadio dell'inflazione soprattutto in quello dell'esecuzione, si realizzi un'opera di rieducazione del condannato"[188]. Sebbene, infatti sia vero che le discipline in tema responsabilità degli enti prevedano delle sanzioni dirette a questi ultimi, è altrettanto vero che gli effetti di questa sanzione e la correlativa funzione rieducativa saranno avvertiti dalle persone fisiche dietro la persona giuridica.

Se si considera, poi, che gli scienziati del settore ritengono non appartenere alle IA del futuro prossimo né un libero arbitrio tale da poterle considerare centri di imputazione diretta di responsabilità penale né una "coscienza" che sia in grado di fargli comprendere la differenza fra "giusto e sbagliato" e, in quest'ultimo caso, di essere rieducate, allora sarà necessario individuare anche per queste tecnologie le persone

---

[187] *op. cit.* Maria Beatrice Magro, "*Robot, cyborg* e intelligenze artificiali", p. 1205.

[188] Giorgio Marinucci, Emilio Dolcini, "Manuale di Diritto Penale - Parte Generale" (sesta ed., Giuffrè editore, 2017).

fisiche che vi sono dietro e prendere in esame una loro possibile responsabilità anche in sede penale.

5.2. Le persone fisiche dietro l'intelligenza artificiale.

Se si vuole continuare l'analogia con la responsabilità delle persone giuridiche, è necessario individuare le persone fisiche che si trovano dietro l'intelligenza artificiale; come per la responsabilità civile, tali soggetti possono essere individuati nell'utilizzatore e nel produttore/sviluppatore. Ciò posto, occorre chiedersi a chi attribuire la responsabilità del reato e, da ultimo, considerare le "sanzioni" che possono ricadere sul sistema intelligente. Quanto al primo problema, è, infine, necessario riprendere la distinzione fra sistemi intelligenti di terza e seconda fascia, cominciando l'analisi proprio da questi ultimi (che, si ricorderà, si caratterizzano per la possibilità che l'essere umano riprenda il controllo del robot).

Si consideri, dunque, la situazione di un'auto che procede in modalità "guida autonoma" a bassa velocità e che il soggetto sul posto del guidatore stia dormendo; si consideri, poi, che in quel momento, a qualche centinaia di metri di distanza, un pedone attraversi la strada e che i sensori dell'auto non percepiscano tempestivamente il pedone; l'auto, avendo notato il pedone troppo tardi, non riesce a frenare in tempo, investendo il pedone e determinandone la morte all'impatto. Esaminata questa situazione, e tenuto conto che si tratta di una autonomia di livello 3, il passeggero sarà responsabile per omicidio colposo, in quanto ha agito con negligenza, imprudenza o imperizia.

Analizziamo invece l'esempio proposto con Ro-Dog nel par. 4.5.1: i sensori di Ro-Dog confondono un semplice pezzo di carta con un giornale e si dirigono a raccoglierlo, ma in quello momento sta passando un ragazzo in bici; consideriamo, poi, che il proprietario di Ro-Dog sia a conoscenza di questi errori di calcolo nei sensori e che nonostante ciò non abbia preso adeguate precauzioni; non potendo evitarlo, il ragazzo si scontra con Ro-Dog e, sbattendo la testa nella caduta, decede sul colpo. In questa

diversa situazione, il proprietario di Ro-Dog risponderà comunque di omicidio colposo, in quanto ha agito con negligenza.

In entrambi i casi alla responsabilità dell'utilizzatore si potrà accompagnare quella del produttore/sviluppatore: nel secondo caso, la responsabilità del produttore per gli errori nei sensori di Ro-Dog si aggiungerà a quella del proprietario, che comunque era a conoscenza dell'errore; nella prima situazione, invece, l'estensione di responsabilità si avrà solo se emergerà un vero e proprio difetto dei sensori.

La questione dell'attribuzione di responsabilità cambia quando si tratti di agenti intelligenti della terza fascia. L'assenza di controllo incisivo da parte dell'essere umano e una certa imprevedibilità nel comportamento dell'IA impongono di giungere alle medesime conclusione tratte per la responsabilità extracontrattuale, quantomeno per l'utilizzatore, in quanto egli non potrà mai essere considerato in colpa, perché è verosimile attendersi una eliminazione della diligenza richiesta.

Quanto al produttore/sviluppatore, premesso sempre che un difetto del prodotto potrà in ogni caso dare adito ad una sua responsabilità, alcuni autori ritengono che su di loro dovrebbe ricadere l'imputazione soggettiva del reato, sulla base di un concetto molto esteso di prevedibilità del difetto: il reato materialmente commesso dal sistema intelligente è un difetto che comunque doveva essere previsto dal produttore/ sviluppatore e, in quanto questa previsione è mancata, sarà quest'ultimo a risponderne; "la prevedibilità opera come componente della colpa, anche sulla base di leggi scientifiche non corroborate da studi e non consolidate, o nella totale ignoranza di leggi scientifiche di spiegazione causale"[189].

Ritengo, tuttavia, che tale impostazione sia eccessivamente rigorosa nei confronti del produttore/sviluppatore e che, in ultima istanza, ostacolerebbe ingiustificatamente lo sviluppo dell'industria di settore. Non si possono, infatti, trascurare i numerosi benefici che i sistemi autonomi porterebbero con loro: a titolo esemplificativo, si considerino le rilevazioni del 2019 dell'Istituto Nazionale di Statistica (ISTAT) italiano sugli incidenti stradali, che individuano nelle prime 3 circostanze di incidente la distrazione alla guida, il mancato rispetto della precedenza e la velocità troppo elevata; si tratta di situazioni

[189] Maria Beatrice Magro, "Biorobotica, robotica e diritto penale", p. 15.

che un'auto a guida autonoma eviterebbe nella stragrande maggioranza dei casi, di fatto riducendo il numero di incidenti (e morti) stradali. È per questo quindi che i vari legislatori dovrebbero introdurre un "divieto di produzione di agenti artificiali i cui rischi associati possano essere di gran lunga superiori ai benefici, in tal modo limitando l'accesso nell'ambiente solo a quella tecnologia […] i cui rischi sono accettati"[190]. In tal senso, una volta accettato il rischio a livello normativo, la responsabilità non potrà ricadere sul produttore/sviluppatore, restando ferma la responsabilità penale per "inattività", cioè una responsabilità "per aver immesso nell'ambiente una tecnologia innovativa che aumenta il rischio per la salute umana violando il dovere di continuo e costante monitoraggio del prodotto e dei suoi possibili effetti dannosi, anche se non identificati durante la programmazione e produzione, ma evidenziati una volta che il prodotto viene immesso in un ambiente aperto, con l'uso"[191].

5.3. Considerazioni conclusive sulla responsabilità penale dei robot-agenti.

Le medesime difficoltà prospettate in tema di responsabilità extracontrattuale potrebbero emergere in sede penale: se da una parte, infatti, non appare particolarmente difficile individuare il responsabile di un reato quando si ha a che fare con IA di seconda fascia, dall'altra, non può dirsi lo stesso per le IA di terza fascia.

Accettare le possibili conseguenze dannose di questi sistemi, considerati i tanti maggiori benefici, non può comunque voler dire che il danneggiato, o chi ne fa le veci, rimanga senza ristoro. Ancora una volta un sistema assicurativo e di fondi di garanzia, consentirebbe alla vittima di vedere il suo danno risarcito, quanto meno sul piano economico.

Per limitare le possibili conseguenze dannose, appare opportuno introdurre anche una *black list* di sistemi autonomi, o comunque una lista di IA qualificate come "*high-risk*", i cui benefici non superano le conseguenze dannose. L'introduzione di simili robot-agenti darà adito a responsabilità, anche in sede penale, per i danni da essi causati.

---

[190] *op. cit.* Maria Beatrice Magro, "*Robot, cyborg* e intelligenze artificiali", p. 1210.

[191] *ibid.*

Capitolo Quinto
Attività Ad Alto Rischio. Un Caso Particolare.

1. Le attività ad alto rischio.

Nel precedente capitolo si è focalizzata l'attenzione sulle attività materiali svolte dall'intelligenza artificiale (quali, ad esempio, l'attività medica o la circolazione stradale); si sono poi considerati gli effetti (negativi) materiali che tali sistemi potrebbero comportare, quali danni a proprietà ovvero alla salute o alla vita delle persone.

È necessario, ora, considerare le attività e i possibili effetti negativi "immateriali" che correlati all'uso di IA: ci si riferisce, in particolar modo, alle attività decisionali che possono impattare significativamente sulla vita delle persone ed implicare un'ampia varietà di rischi. Appare, dunque, necessaria l'introduzione di un quadro normativo che si concentri su come ridurre al minimo i rischi "immateriali" più significativi.

A questo punto, occorre stabilire quando un rischio sia significativo, o, per meglio dire, quando si debba qualificare una applicazione dell'IA come "*high-risk*".

A tale fine, si condivide l'impostazione proposta dalla Commissione Europea nel *White Paper on Artificial Intelligence*, secondo cui una IA dovrebbe essere considerata ad alto rischio se soddisfa due criteri cumulativi:

- in primo luogo, il sistema intelligente deve essere impiegato in un settore in cui, date le caratteristiche delle attività tipicamente svolte, si possono prevedere rischi significativi, cioè si ritiene che i rischi si verifichino con maggiore probabilità. Viene fornito, poi, qualche esempio di settore a rischio, quale l'assistenza sanitaria, il trasporto e parti del settore pubblico, fra i quali rientra il giudiziario;
- in secondo luogo, l'IA deve essere utilizzata nel settore in questione in modo tale che sia probabile che sorgano rischi significativi. Posto che non tutti gli usi dell'IA nei settori selezionati comportano necessariamente rischi significativi. Ad esempio, l'utilizzo di sistemi intelligenti nella cancelleria dei tribunali difficilmente creerà

danni “immateriali”, mentre tale rischio sarà molto più elevato se l’IA si sostituirà al giudice nella decisione di uno o più aspetti della controversia.

2. Applicazioni di IA in ambito giudiziario.

L’analisi delle attività ad “alto rischio” si concentrerà sul sistema giudiziario, poiché si tratta di un settore in cui è maggiormente probabile il verificarsi di danni “immateriali”, diversamente, ad esempio, dal settore medico e dei trasporti (in parte, comunque, già esaminato nel precedente capitolo) in cui è maggiore la possibilità che si verifichino danni “materiali”.

2.1. La polizia predittiva.

L’utilizzo di intelligenze artificiali in funzione ausiliaria dell’attività di polizia è fenomeno diffuso in diverse nazioni. Si legge infatti nel *Concept Paper* del Convegno annuale di esperti di Polizia del 2019 che “*in their efforts to increase efficiency and effectiveness, and to keep up with technological innovations, law enforcement authorities and agencies across the world are increasingly exploring potentials of AI for their work. […] Even though the use of AI in the work of law enforcement is a relatively new topic, some AI-based tools have been already trialed and are even actively in use by police services of several countries around the world. These include video and image analysis software, facial recognition systems, biometric identification, autonomous drones and other robots, and predictive analysis tools to forecast crime “hot spots" or even to identify potential future criminals, in particular high-risk offenders*”[192].

Tali sistemi consentono di realizzare la c.d. polizia predittiva (*predictive policing*), che consiste nel prevedere, sulla base di modelli statistici, la possibilità che in un determinato tempo e luogo verrà commesso un reato, al fine di prevenire la commissione di detto reato. Sebbene il concetto di polizia predittiva non sia nato grazie

[192] OSCE Annual Police Experts Meeting, Concept Paper, “*Artificial Intelligence and Law Enforcement: an Ally or an Adversary?*” (23-24 settembre 2019, Vienna Hofburg), disponibile presso https://dirittopenaleuomo.org/wp-content/uploads/2019/07/19.pdf (ultimo accesso 25 settembre 2020).

ai sistemi intelligenti, tuttavia questi ultimi hanno consentito una attuazione efficace di questo modello, sia grazie alle numerose informazioni in più di cui dispone la polizia, sia grazie alla capacità di elaborare grandi quantità di dati in poco tempo.

I sistemi di polizia predittiva possono essere suddivisi in due categorie.

Da una parte quelli che individuano degli "*hot spots*", ossia zone "calde" dove la possibilità di commissione di reati è maggiore rispetto ad altri luoghi. La determinazione degli "*hot spots*" avviene sulla scorta delle teorie elaborate dalla criminologia ambientale, secondo le quali, "gli atti criminali possono essere previsti considerando come un individuo tenderà a commettere un delitto ogni qual volta che i benefici derivanti dal crimine siano altamente desiderabili e vi sia l'opportunità di commetterlo"[193]. In particolare, in base alla "teoria delle attività di routine", affinché si presenti l'opportunità di un reato, e che quindi si verifichi un evento criminale c.d. predatorio, sono necessari tre elementi: un "aggressore motivato"; una vittima designata, cioè qualcosa che valga la pena essere rubato o preso e che motivi l'aggressore a ciò; l'assenza di un guardiano capace, cioè qualcuno o qualcosa che disincentivi la commissione del fatto[194].

La seconda categoria, invece, segue "le serialità criminali di determinati soggetti (individuati o ancora da individuare), per prevedere dove e quando costoro commetteranno il prossimo reato"[195]; tali sistemi si basano sul c.d. *crime linking*, in base al quale, grazie allo studio analitico di due o più casi, si determinano il comportamento e le abitudini del soggetto[196].

---

[193] Roberto Pelliccia, "Polizia Predittiva: il futuro della prevenzione criminale?" (9 Maggio, 2019). Disponibile inhttps://www.cyberlaws.it/2019/polizia-predittiva-il-futuro-della-prevenzione-criminale/ (ultimo accesso 25 settembre 2020).

[194] Frank P. Williams, Marylin D. McShane, "*Devianza e Criminalità*" (Il Mulino, 2002).

[195] Fabio Basile, "Intelligenza Artificiale E Diritto Penale: Quattro Possibili Percorsi Di Indagine" (Diritto Penale e Uomo, Milano, 29 settembre 2019).

[196] Cfr. "*The Practice of Crime Linkage: A Review of the Literature*" (*Journal of investigative psychology and offender profiling.* 16, no. 3 (2019): 169–200); "*The Psychology of Linking Crimes: A Review of the Evidence*" (*Legal and criminological psychology.* 12, no. 2 (2007): 233–249); Roberto Tuninetti, "Sistemi di investigazione predittiva: cosa sono, come funzionano e i dubbi privacy" (Agenda Digitale, 19 Mar 2020), disponibile presso https://www.agendadigitale.eu/sicurezza/privacy/sistemi-di-investigazione-predittiva-cosa-sono-come-funzionano-e-i-dubbi-privacy/ (ultimo accesso 25 settembre 2020).

Consideriamo, ora, alcuni esempi di sistemi del primo e del secondo tipo, precisando, comunque, che le previsioni fornite da entrambi i sistemi non riguardano la totalità dei reati, ma solo di quelli che maggiormente si prestano ad analisi statistiche (quali, ad esempio, i reati c.d. di strada).

Al primo gruppo appartiene il *Risk Terrain Modeling* (RTM), uno strumento di analisi geospaziale del crimine progettato per diagnosticare i fattori di rischio ambientale che favoriscono la criminalità nonché per identificare i luoghi in cui tali rischi sono maggiori e vi sia un'alta possibilità che venga commesso un crimine[197]. Prendendo ad esempio, il cliché del "vicolo buio", in questo caso vengono in rilievo almeno due attributi di quello spazio: il vicolo e la scarsa illuminazione; si può ritenere, dunque, che il rischio di criminalità sia eccezionalmente alto nei luoghi in cui questi attributi coesistono. Sulla base di un enorme mole di attributi che definiscono il rischio di criminalità, RTM suddivide il territorio in una griglia, determinando i riquadri con maggiori probabilità di commissione di crimini.

Un simile approccio è seguito con il sistema *PredPol*, nato da un progetto di ricerca tra il dipartimento di polizia di Los Angeles (LAPD) e l'Università della California di Los Angeles (UCLA); si tratta di un sistema oggi diffuso negli Stati Uniti e in Gran Bretagna, che indica dove è possibile che un reato venga commesso (sembra, almeno da quanto riportato sul sito ufficiale, con maggiore precisione rispetto ad altri sistemi di *hot spots*).

Ancora, si può fare riferimento ad "X-Law", dispositivo di polizia predittiva originariamente sviluppato dalla Questura di Napoli, ma ad oggi diffuso in diverse zone dell'Italia. Il software opera basandosi su una serie di dati estrapolati dalle denunce inoltrate alla Polizia di Stato; qualora si individuino fattori ricorrenti o coincidenti, il sistema effettua "previsioni che diventano estremamente attendibili: rapine commesse sempre negli stessi luoghi, da persone con lo stesso tipo di casco o di moto, con modalità analoghe consentono al sistema di tracciare una mappa sul territorio dove

---

[197] Joel M. Caplan, Leslie W. Kennedy, Jeremy D. Barnum, Eric L. Piza, "*Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis of Case Configurations to Explore the Dynamics of Criminogenic Behavior Settings*", (*Journal of Contemporary Criminal Justice* 33, no. 2, maggio 2017: 133–51).

vengono evidenziate le zone a più alto rischio fino a raggiungere il livello massimo in determinati orari, tale da far scattare l'alert che mette in moto le volanti della polizia"[198].

Appartengono, invece, alla seconda categoria le ben note "*no-fly lists*" che, raccogliendo e analizzando dati su potenziali terroristi con l'obiettivo di prevenire la commissione di atti criminali, stilano una lista di persone a cui è proibito viaggiare con aerei commerciali.

Assume la fisionomia di *crime linking* anche il progetto pilota condotto nel 2013 dal dipartimento di polizia di Chicago, in collaborazione con l'*Illinois Institute of Technology* (IIT), il cui scopo era quello di individuare i soggetti in una comunità a rischio di partecipazione alla violenza armata, sia come vittime che come autori. Il programma includeva lo sviluppo di un lista strategica di soggetti (SSL), cioè di persone che si stimava fossero a più alto rischio di violenza armata, comunicata ai comandanti della polizia locale per un intervento preventivo[199].

Ancora si può fare riferimento a Keycrime, software ideato dall'ex assistente capo della Questura di Milano Mario Venturi. Tale programma, spiega il suo ideatore, "è in grado di immagazzinare e analizzare fino a 12.000 informazioni per ciascun atto criminoso: da quelle più generiche quali data, ora, luogo dell'evento, a quelle più specifiche e dettagliate che prendono in considerazione l'autore/i del reato. Esattamente come un cervello umano, il software mira a svolgere un'attività computazionale dei dati archiviati attraverso principi di osservazione, analisi e logica, che prendono spunti da diverse discipline quali la matematica, la statistica la psicologia comportamentale e l'analisi geo spaziale"[200]; analizzando ed elaborando migliaia di dati, Keycrime è in

---

[198] Michele Iaselli, "X-LAW: la polizia predittiva è realtà" (Altalex, 28/11/2018), disponibile presso https://www.altalex.com/documents/news/2018/11/28/x-law-la-polizia-predittiva (ultimo accesso 25 settembre 2020).

[199] Per approfondimenti sul progetto vedi Jessica Saunders, Priscillia Hunt & John S. Hollywood, "*Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot*" (*J Exp Criminol* 12**,** 347–371, 2016).

[200] Mario Venturi, "Key Crime. La chiave del crimine" (Profiling. I profili dell'abuso, 5 (4), 2014).

grado di “mettere in correlazione diversi crimini e determinare quali sono stati compiuti dalla stessa persona o gruppo di persone”[201].

2.1.1. Criticità dei sistemi di polizia predittiva.

Indubbi sono i vantaggi apportati dai sistemi di polizia predittiva in tema di riduzione di commissione di crimini. Basti pensare che dall’introduzione di PredPol la Foothill Division del dipartimento di polizia di Los Angeles (LAPD) ha registrato un calo del 20% dei crimini fra il 2013 e il 2014 o che gli agenti di polizia di Venezia, grazie all’alert di X-Law che indicava la possibilità di un furto nel quartiere di Mestre fra le 3 e le 4 del mattino in un esercizio commerciale, sono riusciti ad arrestare il ladro prima che potesse fuggire[202] o che, ancora, grazie a Keycrime “la Questura di Milano è riuscita a contenere e a ridurre in modo significativo i fenomeni di rapina perpetrati in ambito bancario e commerciale, producendo un effetto di deterrenza”[203].

L’utilizzo di tali sistemi, oltre a permettere il conseguimento di migliori risultati sul piano investigativo ed in termini di prevenzione del crimine, consente di realizzare anche un ingente risparmio economico (si stima che mediante PredPol, il LAPD possa risparmiare fino nove milioni di dollari annui).

Se, dunque, è incontrovertibile la presenza di una molteplicità di benefici, occorre verificare quale sia il costo da pagare, in particolare chiedendosi se i soggetti che subiscono l’identificazione mediante questi sistemi vedano compromessi i propri diritti. Ciò, peró, è tanto più vero per i sistemi di *hot spots* e ciò per due ordini di considerazioni: da una parte essi si basano su dati che vanno oltre "la quantità degli episodi commessi da un soggetto o dalla sua cerchia di amici o da persone appartenenti

---

[201] Andrea Daniele Signorelli, “Il software italiano che ha cambiato il mondo della polizia predittiva” (Wired, 18 maggio 2019), disponibile presso https://www.wired.it/attualita/tech/2019/05/18/polizia-predittiva-software-italiano-keycrime/?refresh_ce= (ultimo accesso 25 settembre 2020).

[202] Cfr. Eleonora Biral, “«Ecco dove e quando colpirà» Ladro arrestato dall’algoritmo” (Corriere del Veneto, 17 novembre 2018).

[203] *op. cit.* Mario Venturi, “Key Crime. La chiave del crimine”

ad un quartiere"[204]; inoltre si aumenta il rischio che si verifichi "l'effetto valanga secondo cui più previsioni di crimini ci sono in un certo quartiere o su determinati soggetti più crimini realmente rilevati ci saranno in quel quartiere o per quei soggetti (in dipendenza dell'aumento di controlli) e dunque la previsione per quello stesso quartiere e per quei soggetti aumenterà esponenzialmente". Infine, è necessario considerare come le minoranze etniche possano venire colpite da tali sistemi a causa della loro fragilità sociale ed economica: tali fattori, corroborati da una maggiore incidenza di crimini in aree periferiche, determinerebbe una eccessiva presenza delle forze dell'ordine. A riprova di ciò, nel 2016 lo *Human Rights Data Analysis Group* (HRDAG) statunitense ha dimostrato che, utilizzando PredPol per prevenire crimini aventi ad oggetto sostanze stupefacenti nella città di Oakland, il sistema avrebbe inviato pattuglie quasi esclusivamente nei quartieri di minoranza a basso reddito. Questo perché, nei registri del periodo precedente all'esecuzione dell'algoritmo, la maggior parte dei crimini di droga si erano stati verificati in quegli stessi quartieri; tuttavia i dati del dipartimento *Health and Human Services* dimostrano che l'uso illecito di sostanze è diffuso uniformemente in tutta la città[205].

I sistemi che si basano sul *crime linking*, invece, consentono di ridurre questo tipo di rischi, perché basano la loro attività principalmente su soggetti già individuati come "criminali" e sulla base di dati di cui la polizia è già in possesso. Tuttavia è bene evidenziare come alcuni principi fondamentali degli odierni Stati di diritto, quali la presunzione di innocenza[206], potrebbero essere minati se fosse consentito a tali sistemi di accedere ad informazioni ulteriori, come quelle presenti sui social network, o di effettuare una definizione del profilo criminale di soggetti mai ancora rilevati come "criminali", ma suscettibili di diventarlo.

---

[204] Cesare Parodi, Valentina Sellaroli, "Sistema Penale E Intelligenza Artificiale: Molte Speranze E Qualche Equivoco" (in Diritto Penale Contemporaneo, Fasciolo 6/2019).

[205] Kristian Lum, "*Predictive Policing Reinforces Police Bias*" (*Human Rights Data Analysis Group*, 10 ottobre 2016), disponibile presso https://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/ (ultimo accesso 25 settembre 2020).

[206] Sul punto cfr. Giuseppe Vaciago, "KEY CRIME: un futuro costituzionalmente ammissibile?" (30 luglio 2014), disponibile presso http://www.replegal.it/it/tmt-telecomunication-media-technology/item/413-key-crime-un-futuro-costituzionalmente-ammissibile (ultimo accesso 25 settembre 2020).

2.2. La giustizia predittiva.

Le intelligenze artificiali sono, poi, da qualche tempo utilizzate anche per coadiuvare l'attività dei giudici e, più in generale, delle corti di giustizia.

La funzione di ausilio di questi sistemi può assumere, in primo luogo, la forma di banche dati "smart". È questa, ad esempio, la via percorsa dalla Corte d'appello di Brescia, che fra il 2018 e il 2019 ha iniziato un progetto per la creazione di una banca dati il più possibile smart, tramite "la raccolta – al momento- di tutti i provvedimenti emessi dal 2018 in poi in determinati settori che sono le materie assegnata alla competenza del tribunale delle imprese, gli appalti, i contratti bancari, e il lavoro con specifico riferimento al rapporto di lavoro, infortunistica, licenziamenti, di primo e secondo grado" al fine di "mettere a disposizione di tutti gli stakeholder una banca dati ragionata e trasparente, da cui possano emergere orientamenti giurisprudenziali, di casistica, di tempistica e tutti quegli elementi che possano essere valutati dagli operatori (giudici, avvocati, imprese, lavoratori) per adottare le opportune precipue decisioni. Inoltre favorirà la circolarità della giurisprudenza di merito tra primo e secondo grado"[207].

Ancora, una importante risultato è stato raggiunto negli Stati Uniti da Ross Intelligence con la sua IA "Ross", definita dalla *American Bar Association* come "*an example of how artificial intelligence can be used to improve the delivery of legal services*"[208]. Si tratta di uno strumento che si è dimostrato particolarmente utile per gli avvocati, essendo capace di ricercare una pluralità di casi giurisprudenziali sulla medesima materia partendo da alcune parole chiavi.

D'altra parte, sembra che tali sistemi intelligenti siano più d'aiuto per il lavoro svolto dagli avvocati (in particolare modo quelli di *common law*) che per quello dei giudici. A dimostrazione di ciò si può richiamare l'esperimento svolto in Francia nel 2017: su

---

[207] Claudia Morelli, "Giustizia predittiva: il progetto (concreto) della Corte d'appello di Brescia" (Altalex, 08 aprile 2019), disponibile presso https://www.altalex.com/documents/news/2019/04/08/giustizia-predittiva#uno (ultimo accesso 25 settembre 2020).

[208] La citazione si torva in prima pagina nel sito ufficiale di Ross Intelligence, accessibile presso https://www.rossintelligence.com.

iniziativa del Ministro della Giustizia, le Corti di Appello di Rennes e di Douai hanno accettato di testare un software di ausilio decisione, il cui obiettivo era "creare uno strumento di ausilio alla decisione in modo da ridurre, se necessario, l'eccessiva variabilità delle decisioni giudiziarie, in nome del principio di uguaglianza dei cittadini di fronte alla legge"[209]. Tuttavia, dopo qualche mese dalla sua introduzione, l'esperimento è risultato fallimentare, come esposto dal primo presidente della Corte d'Appello di Rennes: "Le nostre due Corti d'appello e il Ministero della giustizia hanno concluso che l'esperimento non è riuscito. Abbiamo ritenuto l'assenza di un valore aggiunto per il lavoro dei magistrati, poiché eravamo già in possesso di banche dati e quindi in grado, in ambito civile, di accedere a tutte le decisioni. Inoltre, disponiamo di strumenti di ricerca per rintracciare le decisioni partendo da parole chiave. Per quanto riguarda l'approccio quantitativo – che ci mancava – ci saremmo aspettati un approccio rinnovato, con una migliore leggibilità delle tabelle. Tuttavia, su un certo numero di *test*, abbiamo considerato come vi fossero effettive distorsioni di ragionamento, derivanti da una confusione interna all'analisi del testo non normato: si confondevano causalità – che informa il dispositivo – e circostanza. Ci siamo, quindi, ritrovati frustrati dal fatto di non poter disporre di una vera analisi quantitativa della giurisprudenza, e le nostre corti hanno deciso di non dar seguito al monitoraggio di questo *software*, aspettando i giorni felici di una migliore qualità analitica"[210].

Il software utilizzato in questo esperimento, d'altro canto, non sfrutta solo la funzione di banca dati (rispetto a cui ha mostrato la sua poca innovatività), ma anche quella di assistenza nella fase decisionale del giudizio. È proprio questa la seconda forma che le intelligenze artificiali possono assumere nelle corti di giustizia, forma che può poi essere suddivisa in due ulteriori categorie: sistemi alternativi di risoluzione delle controversie e *automated decision systems*.

---

[209] Commissione Europea Per l'Efficienza Della Giustizia (CEPEJ), "Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi".

[210] La citazione è riportata da Simone Gaboriau, "Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?", in "Una giustizia (im)prevedibile? Il dovere della comunicazione" (Questione Giustizia, Fascicolo 4/2018), disponibile presso https://www.questionegiustizia.it/rivista/2018-4.php (ultimo accesso 25 settembre 2020).

Lo sviluppo di sistemi alternativi di composizione delle controversie sembrano essere seguito da un certo entusiasmo, così come sostenuto dall'*Online Dispute Resolution Advisory Group* del *Civil Justice Council* inglese: "*we call for radical change in the way that the court system of England and Wales handles low value civil claims. We strongly advocate the introduction of online dispute resolution (ODR)*", poiché "*for low value claims, we are concerned that our current court system is too costly, too slow, and too complex, especially for litigants in person*"[211]. Sistemi di ODR sono già presenti in diversi paesi, sia europei che extra-europei.

É questo il caso di *Rechtwijzer* 2.0, servizio fornito dal Ministero della giustizia e della sicurezza olandese, progettato per aiutare le parti a risolvere le controversie (per lo più in ambito matrimoniale, anche se la piattaforma può essere configurata per rispondere ad altri problemi). Quale forma di assistenza nella negoziazione, il sistema offre una piattaforma per informazioni legali, consulenza e servizi, alcuni dei quali sono automatizzati. Consente alle persone di risolvere i problemi legali come meglio preferiscono ed insieme alla controparte. La fase ADR (che prende la forma di mediazione o arbitrato online) si apre in caso di mancato raggiungimento di un accordo stragiudiziale. Il processo si svolge online su una piattaforma sicura e riservata, progettata per il dialogo asincrono con un mediatore. Per assicurare la validità dell'operazione, l'accordo dovrà essere presentato ad un avvocato per la conferma.

Un altro esempio è offerto dal *Civil Resolution Tribunal* canadese, tribunale online alternativo ai tribunali tradizionali per la risoluzione di controversie di modesto valore (meno di 25.000 dollari canadesi per vicende relativi a debiti, danni, recupero di proprietà personali e alcune controversie condominiali). La piattaforma, in prima fase, cercherà sempre di aiutare le parti a trovare una soluzione condivisa, mostrando le possibili opzioni e utilizzando la piattaforma di negoziazione online del tribunale. Se non viene raggiunto un accordo, verrà nominato un responsabile del caso giudiziario per assistere le parti nella risoluzione della controversia attraverso un processo di mediazione che avrà luogo online o per telefono. Se le parti non si accontentano di

---

[211] Online Dispute Resolution Advisory Group, "*Online Dispute Resolution For Low Value Civil Claims*" (Civil Justice Council, febbraio 2015).

questo processo di mediazione, saranno quindi invitate ad accettare una terza e ultima fase di aggiudicazione. Il giudice contatterà le parti tramite la piattaforma online, per telefono o, se necessario, tramite videoconferenza, e poi prenderà una decisione che sarà definitiva e vincolante.

La forza (e la legalità) di questi sistemi risiede proprio nell'etere facoltativo: le parti della controversia potranno autonomamente scegliere se proseguire con le vie tradizionali o affidarsi alle modalità offerte online.

Il problema potrebbe porsi quando si passa da una soluzione alternativa, ad un vero e proprio giudice automatizzato. È questo l'obiettivo del ministero della Giustizia dell'Estonia, che ha affidato ad un team di esperti il non facile compito di sviluppare una intelligenza artificiale in grado di sostituirsi al giudice umano: più nello specifico, "si tratta di creare una sorta di macchina robotica con funzioni di giudice che possa prendere decisioni per dirimere dispute di minore valore, inferiori a 7000 euro. […] Le sentenze emesse dall'intelligenza artificiale saranno comunque appellabili potendo essere sottoposte anche al giudizio di un magistrato in carne ed ossa"[212].

2.2.1. Criticità dei sistemi di giustizia predittiva.

Come si è rilevato per i sistemi di polizia predittiva, anche in tema di giustizia predittiva non possono sottacersi i benefici apportati da tali tecnologie, sia in termini di miglioramento dell'accesso alla giustizia sia in termini di totale riduzione di costi e tempistiche dell'attività delle corti.

Anche in questo caso, tuttavia, occorre domandarsi quali rischi questi software celino. Se da una parte, infatti, le banche dati smart (come il sistema "Ross") appaiono prive di rischi, lo stesso non può dirsi per i sistemi di che si pongono come alternativi al giudice fisico.

---

[212] Carlo Lavalle, "In Estonia il giudice sarà un'intelligenza artificiale" (La Stampa, 04 Aprile 2019), disponibile presso https://www.lastampa.it/tecnologia/news/2019/04/04/news/in-estonia-il-giudice-sara-un-intelligenza-artificiale-1.33692863?refresh_ce (ultimo accesso 25 settembre 2020).

La sostituzione ad un giudice fisico potrà avvenire soltanto per quelle cause di modesto valore, sia perché particolarmente ripetitive (e che quindi si maggiormente prestano ad essere standardizzate) sia, soprattutto, perché le decisioni impatteranno su interessi di modesto valore dei cittadini. La sostituzione al giudice fisico, poi, non potrà essere assoluta, ma solo relativa, sia nel senso che le parti potranno autonomamente scegliere se ricorrere a tribunali online/automatizzati, sia nel senso che la questione possa essere rimessa ad un giudice fisico per una sua autonoma valutazione.

Da ultimo, la necessaria presenza di un giudice fisico impone di circoscrivere l'utilizzo di questi sistemi al solo ambito civilistico: secondo quanto sostenuto dalla CEPEJ "il ricorso alle statistiche e all'intelligenza artificiale nei procedimenti penali ha dimostrato che sussiste il rischio di incoraggiare la recrudescenza di dottrine deterministiche a scapito delle dottrine di individualizzazione della pena[213] che sono state ampiamente acquisite a partire dal 1945 nella maggior parte dei sistemi giudiziari europei"[214].

Ai fini di una esclusione delle IA in ambito penale, si condividono, inoltre, le ragioni esposte da Alessandro Traversi, avvocato in Firenze, nella rivista "Questione Giustizia": in primo luogo perché il mezzo di prova più frequentemente usato nel processo penale per l'accertamento di fatti materiali è la testimonianza ed un *computer* incontrerebbe serie difficoltà nel giudicare se un teste abbia detto la verità, sia stato reticente o abbia mentito. In secondo luogo perché plurimi e non predeterminati sono i criteri di valutazione della prova; in terzo luogo perché il *computer* è programmato per fornire risposte certe, non può avere dubbi, mentre nella maggior parte degli ordinamenti vige il principio secondo il quale il giudice pronuncia sentenza di condanna se l'imputato risulta colpevole al di là di ogni ragionevole dubbio (negli ordinamenti di *common law*

---

[213] L'individualizzazione della pena è una dottrina che richiede che si tenga conto delle specifiche esigenze dei singoli casi nell'attribuzione di pena. Si tratta, ovviamente, di valutazioni che il giudice dovrà operare caso per caso; le sempre mutevoli modalità di decisione difficilmente si prestano ad essere inserite nell'algoritmo o apprese dalle IA.

[214] *op. cit.* CEPEJ.

sussiste l'equivalente principio del *beyond reasonable doubt*) e deve invece assolvere qualora detto parametro non sia superato[215].

2.3. Il *risk assessment*.

La possibilità che un soggetto, dopo aver commesso un reato, possa commetterne un altro (c.d. rischio di recidiva) è stato in precedenza analizzato quale metodo per prevenire la (nuova) commissione di un reato. Tuttavia, una simile valutazione è effettuata dai giudici di vari ordinamenti quando si tratta di applicare una misura di sicurezza o una misura cautelare. I giudici più tradizionalisti valutano il rischio di recidiva per lo più intuitivamente, affidandosi alla loro esperienza personale e al loro buon senso ovvero alle valutazioni di periti[216]; tra le metodologie più moderne rileva invece la valutazione del rischio *evidence-based*[217]. Tale forma di *risk assessment* si basa su criteri oggettivi (i fattori di rischio) quali l'età, il sesso, l'origine etnica, la posizione sociale, i precedenti, i luoghi e le persone frequentati, ecc. L'utilizzo di criteri oggettivi permette di riprodurre la valutazione *evidence-based* su sistemi di IA in grado di sostituirsi, in questi compiti, al giudice.

Leader nell'attuazione di queste tecnologie sono gli Stati Uniti; si riporta, di seguito, qualche esempio.

Nello Stato del New Jersey, al fine di riformare il sistema del rilascio dal carcere su cauzione (*bail*), le udienze per la concessione della libertà su cauzione sono state sostituite con un algoritmo di *risk assessment*. In particolare, il *Public Safety Assessment* (PSA), sulla base di nove fattori (tra cui età e precedenti penali), stabilisce se il soggetto commetterà o meno un nuovo reato dopo essere stato rilasciato. È

---

[215] Alessandro Traversi, "Intelligenza artificiale applicata alla giustizia: ci sarà un giudice *robot*?" (Questione Giustizia, 10 aprile 2019), disponibile presso https://www.questionegiustizia.it/articolo/intelligenza-artificiale-applicata-alla-giustizia-ci-sara-un-giudice-robot-_10-04-2019.php (ultimo accesso 25 settembre 2020).

[216] *op. cit.* Fabio Basile, "Intelligenza Artificiale E Diritto Penale: Quattro Possibili Percorsi Di Indagine".

[217] Per approfondimenti sul tema cfr. Georgia Zara, "Tra Il Probabile E Il Certo" (Diritto Penale Contemporaneo, 20 maggio 2016).

opportuno notare come tale sistema non considera fattori come razza od origine geografica, in modo tale da risultare il più imparziale possibile[218].

Non è stata dello stesso avviso la NorthPointe, compagnia che ha prodotto il *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS), altro software capace di valutare il rischio di recidiva, quando tale dato sia utile al giudice nel determinare la pena da infliggere. Il sistema si basa sulle risposte fornite a 137 domande (sia direttamente dall'imputato sia estratte dal casellario giudiziale) relative all'imputato e formula una valutazione della persona da 1 (che corrisponde ad un rischio basso) a 10 (rischio massimo). Tale sistema costituisce un ausilio per il giudice, il quale ne tiene conto come uno dei fattori ai fini della determinazione la pena. Tuttavia, un'inchiesta della ONG ProPublica ha rivelato gli effetti discriminatori che sottostanno all'utilizzo di questo software. La ONG ha infatti rilevato come ai soggetti afro-americani sia stato attribuito un punteggio molto elevato di rischio di recidiva nei due anni successivi alla condanna rispetto ai soggetti caucasici. Occorre tener presente, però, che le intenzioni della NorthPointe non erano quelle di creare una IA razzista: si tratta infatti di un *data-driven bias* (*v. supra* capitolo 3).

D'altra parte, l'inchiesta di ProPublica ha rivelato un ulteriore problema nell'utilizzo di questi software e cioè la carenza di trasparenza nei processi di funzionamento degli algoritmi progettati da società private; si può leggere infatti nel documento della CEPEJ che "la cronaca ha dimostrato che il pubblico è informato delle operazioni relative ai megadati in maniera sporadica e accidentale, quando avvengono fughe di notizie o errori, come è accaduto quando ProPublica, a seguito del rifiuto della società proprietaria di condividere l'algoritmo COMPAS, ne ha rivelato le falle. La ONG ha dovuto fare appello alle autorità pubbliche per accedere ai dati e impiegare un suo scienziato per esaminare l'algoritmo"[219].

---

[218] Ephrat Livni, "Nei tribunali del New Jersey è un algoritmo a decidere chi esce su cauzione" (Internazionale, 2 marzo 2017), disponibile presso https://www.internazionale.it/notizie/ephrat-livni/2017/03/03/tribunali-algoritmo-cauzione (ultimo accesso 25 settembre 2020).

[219] *op. cit.* CEPEJ.

3. Considerazioni conclusive circa l'utilizzo di IA in settori ad alto rischio.

L'utilizzo di intelligenze artificiali in settori ad alto rischio di danni immateriali impone molte più cautele rispetto ai settori che presentano rischi di danni materiali. Alla luce dell'esposizione proposta nelle precedenti pagine, ritengo che i benefici apportati da sistemi intelligenti nel prendere decisioni delicate siano parziali e comunque presentino un elevato numero di rischi che, a mio avviso, non possono essere accettati, considerato anche l'impatto che questo tipo di IA può avere in diritti protetti dalle carte costituzionali di varie nazioni. Se infatti gli avvocati vedono la possibilità di utilizzare tali tecnologie per fornire ai loro clienti consigli più informati grazie a una valutazione delle probabilità di successo di una procedura, lo stesso non può dirsi per i giudici: gli esperimenti condotti nelle Corti di appello di Douai e di Rennes dimostrano chiaramente che l'impiego di intelligenze artificiali può portare ad inaccettabili conseguenze[220].

Ancora, sistemi di giustizia predittiva sembrano essere poco conformi agli ordinamenti di *civil law*: "il tema della giustizia predittiva viene oggi sviluppato, in misura prevalente, seguendo un'impostazione statistica-giurisprudenziale: si verificano i precedenti giurisprudenziali ed in base a questi si prevedono le decisioni future. Esemplificativamente: se dieci sentenze su cento precedenti dicono che nel caso x si applica y, allora ci sarà il 10% di possibilità che in futuro il giudice a parità di fatto x si orienterà su y"[221]. La previsione su base statistica-giurisprudenziale, cioè l'utilizzo di un modello induttivo (dal caso si giunge alla regola), si mal conforma con gli ordinamenti di *civil law*, dove si utilizza un modello deduttivo (la legge viene applicata al caso) e in cui il precedente non è, in assoluto, vincolante.

Tuttavia, un utilizzo di sistemi intelligenti, come meccanismi di risoluzione alternativa delle controversie, dovrebbe essere incoraggiato per quelle questioni civili di minor valore che, per le ragioni precedentemente esposte, tendono ad essere standardizzate.

---

[220] *op. cit.* CEPEJ.

[221] Luigi Viola, "Giustizia predittiva: è preferibile un modello deduttivo" (Altalex, 10 marzo 2020), disponibile presso https://www.altalex.com/documents/news/2020/03/10/giustizia-predittiva-preferibile-modello-deduttivo (ultimo accesso 25 settembre 2020).

Proprio le pratiche standardizzate si prestano ad essere trattate mediante sistemi automatizzati ed intelligenti. Sul punto, appare utile richiamare quanto esposto dal Consiglio di Stato italiano: "devono sottolinearsi gli indiscutibili vantaggi derivanti dalla automazione del processo decisionale dell'amministrazione mediante l'utilizzo di una procedura digitale ed attraverso un "algoritmo" […]. L'utilità di tale modalità operativa è particolarmente evidente con riferimento a procedure seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale. […] L'utilizzo di una procedura informatica che conduca direttamente alla decisione finale non deve essere stigmatizzata, ma anzi, in linea di massima, incoraggiata: essa comporta infatti numerosi vantaggi quali, ad esempio, la notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o peggio dolo) del funzionario (essere umano) e la conseguente maggior garanzia di imparzialità della decisione automatizzata. In altre parole, l'assenza di intervento umano in un'attività di mera classificazione automatica di istanze numerose, secondo regole predeterminate (che sono, queste sì, elaborate dall'uomo), e l'affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose"[222]. Nella medesima sentenza, d'altra parte, si pone l'accento su come l'attività svolta dalla IA debba essere "conoscibile", sia nel senso di poter verificare che il sistema abbia svolto i suoi compiti in maniera conforme alla legge, sia nel senso che la decisione debba poter essere sottoposta al sindacato di un giudice fisico. Sul punto il Consiglio di Stato è tornato in un'altra sentenza, affermando che "la fondamentale esigenza di tutela posta dall'utilizzazione dello strumento informatico c.d. algoritmico sia la trasparenza nei termini riconducibili al principio di motivazione e/o giustificazione della decisione"[223].
Alla luce delle considerazioni effettuate dal Consiglio di Stato, è possibile estrapolare alcuni principi cardine che debbono essere rispettati nell'utilizzo di IA in tutti settori ad alto rischio di danni immateriali: in primo luogo, l'utilizzo di queste tecnologie

[222] Cons. Stato, sez. VI, 08 aprile 2019 n. 2270.

[223] Cons. Stato, sez. VI, 13 dicembre 2019 n. 8472.

dovrebbe essere escluso in quei processi che possano comportare una limitazione o compressione dei diritti fondamentali dell'uomo, quale, ad esempio, la libertà (così quindi il processo penale, almeno allo stato attuale della tecnologia, non potrà essere automatizzato); seppur non vi sia ad oggetto un diritto fondamentale, qualora il processo richieda una valutazione fondata sull'esperienza e sul senso comune di una persona fisica, nuovamente l'utilizzo di IA è sconsigliabile; qualora questi primi due criteri siano rispettati, un sistema intelligente potrà essere utilizzato, ma la scelta rispetto ad una persona fisica dovrebbe essere libera e lasciata al soggetto su cui il danno immateriale possa ricadere.

In ossequio al principio di trasparenza (*v. supra* capitolo 3), le modalità decisionali della IA debbono poter essere conoscibili e comprensibili da una persona fisica, di modo da verificare se la procedura possa essere convalidata o ripetuta (se del caso, dinanzi ad una persona fisica).

Da ultimo, in conformità al principio *under user control*, la medesima decisione deve poter essere rimessa ad una persona fisica per una sua valutazione autonoma, nel senso che prescinda dai risultati raggiunti dall'intelligenza artificiale.

Conclusioni

Ci si aspetta che il mercato globale dell'intelligenza artificiale cresca con tasso medio annuo del 42.2% fra il 2020 e il 2027[224]. Considerati gli enormi risultati che la scienza e la tecnologia raggiungono di anno in anno, è ragionevole aspettarsi che le IA permeino in vari aspetti della società umana in tempi relativamente brevi. Agli albori di una nuova rivoluzione digitale, sorge la preoccupazione che le nuove tecnologie si presentino dinanzi all'essere umano prive di un quadro giuridico adeguato. È necessario, infatti, che i giuristi si attrezzino "per trovare soluzioni a problemi che, a dispetto del loro aspetto futuristico, possono concretizzarsi in un'aula di tribunale in modo improvviso"[225].

Nel corso dell'elaborato è, in effetti, emerso come i vari legislatori stiano guardano al problema con troppa enfasi, focalizzando l'attenzione sulla ricerca e sviluppo delle IA, distogliendola dalle questioni giuridiche da esse poste.

In primo luogo, appare inadeguato continuare a configurare i sistemi intelligenti e i robot-agenti come mere *res*, in considerazione delle peculiari caratteristiche di cui sono dotati. Risulta preferibile elaborare, quanto meno per i sistemi più avanzi ed autonomi, un nuovo *genus* di personalità, una personalità "elettronica" che consenta alle IA di godere di alcuni diritti ed obblighi; una personalità funzionale alle esigenze dell'uomo.

Ulteriormente, sebbene ammirevoli risultino i tentativi di alcuni Stati e Organizzazioni di ricercare principi utili nello sviluppo di queste tecnologie, si è evidenziato come la pervasività delle intelligenze artificiali impone di guardare al problema non in generale, ma nei singoli aspetti maggiormente colpiti dal loro impatto. Da una parte, infatti, il ricorso a strumenti normativi esistenti appare solo parzialmente idoneo a regolare i sistemi intelligenti; dall'altra la predisposizione di discipline onnicomprensive potrebbe determinare l'insorge di vuoti normativi.

---

[224] Grand View Research, "*Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution (Hardware, Software, Services), By Technology (Deep Learning, Machine Learning), By End Use, By Region, And Segment Forecasts, 2020 - 2027*" (luglio 2020).

[225] *op. cit.* Amedeo Santosuosso, Chiara Boscarato, Franco Caroleo, *Robot e diritto: una prima ricognizione*.

Nell'approntare una disciplina specifica, in ossequio ad un principio di precauzionalità, dovrà seguirsi un approccio costi-benefici, impedendo l'utilizzo di IA in quei settori dove i benefici siano pari od inferiori ai rischi dalle stesse presentati. Ove, invece, i benefici superino i rischi, dovrà comunque tenersi conto delle eventuali problematiche che possano insorgere: in tal senso i classici istituti della responsabilità civile e penale andrebbero rivisitati, in considerazione della possibilità che fra le parti della controversia vi possa essere una intelligenza artificiale.

Da ultimo, sempre secondo un approccio precauzionale, le varie nazioni dovranno essere chiamate ad istituire apposite agenzie statali o indipendenti che monitorino gli operatori delle IA, sia in fase di prima immissione nel mercato, sia nel successivo periodo di utilizzo.

In conclusione, l'auspicio è che i legislatori nazionali e le organizzazioni internazionali guardino al problema con lungimiranza, intervenendo in questa fase embrionale di sviluppo delle intelligenze artificiali, interrogandosi sulle future sfide legali da esse poste e sui necessari adattamenti alle normative vigenti, al fine di predisporre un framework giuridico solido e di lunga durata.

Bibliografia

- Alhelt K., "*The Applicability of the EU Product Liability Directive to Software*", Comparative and International Law Journal of Southern Africa 34, no. 2 (2001): 188-209.
- Arcelia E., Adriano Q., "*The Natural Person, Legal Entity or Juridical Person and Juridical Personality*", (4 PENN. ST. J.L. & INT'L AFF. 363, 2015).
- Asimov, I., "*Runaround*", in *I, Robot* (pp. 20-34), (NY, NY: The New American Library., 1956).
- Asimov, I., "*The Zeroth Law*", in *Robots and empire*. (Garden City, NY: Doubleday, 1985).
- Atabekov A., Yastrebov O., "*Legal status of artificial intelligence across countries: Legislation on the move*" (European Research Studies Journal. 21. 773-782, 2018).
- Basile F., "Intelligenza Artificiale E Diritto Penale: Quattro Possibili Percorsi Di Indagine" (Diritto Penale e Uomo, Milano, 29 settembre 2019).
- Biral E., "«Ecco dove e quando colpirà» Ladro arrestato dall'algoritmo" (Corriere del Veneto, 17 novembre 2018).
- Bonnefon J., Shariff A., Rahwan I., "*The Social Dilemma of Autonomous Vehicles*" (Science, Vol. 352, issue 6293, 24 giugno 2016).
- Bostrom, N., "*SUPERINTELLIGENCE - paths, dangers, strategies*" (ed. 1). (Oxford: Oxford University Press, 2014).
- Campobasso, G. F., & Campobasso, M. (2013). "Diritto Commerciale" (settima ed., Vol. 1. Diritto dell'impresa). Torino: UTET giuridica.
- Campobasso, G. F., & Campobasso, M. (2015). "Diritto Commerciale" (nona ed., Vol. 2. Diritto delle società). Torino: UTET giuridica.
- Cantú E. C., "*A Continuing Whimsical Search for the True Meaning of the Term "Product" in Products Liability Litigation*" (33 St. Mary's L.J. 455 (2004).
- Cantú E. C., "*The Illusive Meaning of the Term 'Product' Under Section 402A of the Restatement (Second) of Torts*", Vol. 44, 1991 (Oklahoma Law Review, 1991).
- Caplan, Joel M., Leslie W. Kennedy, Jeremy D. Barnum, and Eric L. Piza, "*Crime in Context: Utilizing Risk Terrain Modeling and Conjunctive Analysis of Case*

Configurations to Explore the Dynamics of Criminogenic Behavior Settings", (*Journal of Contemporary Criminal Justice* 33, no. 2, maggio 2017: 133–51).

- Consumer Affairs Australia and New Zealand, "*Australian Consumer Law Review*", (Marzo 2016).
- Coppini L., "*Robotica e intelligenza artificiale: questioni di responsabilità civile*", in "Politica del diritto, Rivista trimestrale di cultura giuridica fondata e diretta da Stefano Rodota'" 4/2018, pp. 713-740.
- Dobrev D., "*A Definition of Artificial Intelligence*" (Mathematica Balkanica, New Series, Vol. 19, 2005, Fasc. 1-2, pp.67-74), disponibile presso https://arxiv.org/pdf/1210.1568.pdf (ultimo accesso 25 settembre 2020).
- Dobrev, D., "*Formal Definition of Artificial Intelligence*", (*International Journal "Information Theories & Applications", 12*, 277-285, 2005), disponibile presso http://sci-gems.math.bas.bg/jspui/bitstream/10525/813/1/ijita12-3-p12.pdf (ultimo accesso 25 settembre 2020).
- European Group on Ethics in Science and New Technologies, "S*tatement on artificial intelligence, robotics and 'autonomous' systems: Brussels*" (Lussemburgo: Publications Office of the European Union, 9 marzo 2018).
- Ewald B. W., "*Comparative Jurisprudence (I): What Was it Like to Try a Rat?*" (Faculty Scholarship, Paper 1405, 1995).
- Expert meeting, "*Autonomous weapon systems: Technical, military, legal and humanitarian aspects*" (Geneva, Switzerland, 26-28 marzo 2014).
- Floridi L, Cowls J, Beltrametti M, et al., "*AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*" (Minds and Machines, 2018), DOI: 10.1007/s11023-018-9482-5.
- Fondazione Leonardo Civiltà delle Macchine, "*Statuto Etico e Giuridico dell'IA*" (2019).
- Fraser I., *"Guida all'applicazione della direttiva "macchine" 2006/42/CE*" (2ª ed., giugno 2010), Commissione Europea Impresa e Industria, disponibile presso https://ec.europa.eu/docsroom/documents/9202/attachments/1/translations/it/renditions/native (ultimo accesso 25 settembre 2020).

- Gadzhiyev, G. A., "*Whether the Robot-Agent is a Person? (Search of Legal Forms for the Regulation of Digital Economy)*" [Abstract]. (*Journal of Russian Law, 6*(1), 15-30, 2017), doi:10.12737/art_2018_1_2.
- Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale, "*Orientamenti Etici per un'IA Affidabile*", istituito dalla Commissione europea nel giugno 2018.
- Hallevy G., "*The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*", (Akron Intellectual Property Journal: Vol. 4, Iss. 2 , Article 1, 2010).
- House of Lords Artificial Intelligence Committee (2018), "*AI in the UK: ready, willing and able*".
- Jones, J. L. (2014). "*Autonomous Vehicle Report*" (pp. 1-7, Rep. No. #13-008), disponibile presso https://www.flhsmv.gov/html/HSMVAutonomousVehicleReport2014.pdf (ultimo accesso 25 settembre 2020).
- Karnow E.A. C., "*The application of traditional tort theory to embodied machine intelligence*" (The Robotics and the Law Conference, Center for Internet and Society, Stanford Law School, Aprile 2013).
- Kurki, A.J., V., *"Legal Personhood: Animals, Artificial Intelligence and the Unborn*" (Cham :: Springer International Publishing :, 2017, Vol. 119).
- Lehman-Wilzig, S. N., "*Frankenstein unbound*", (*Futures, 13*(6), 442-457, 1981) doi:10.1016/0016-3287(81)90100-2.
- Magro M.B., "Biorobotica, robotica e diritto penale".
- Magro M.B., "*Robot, cyborg* e intelligenze artificiali", in A. Cadoppi "Trattato di Diritto penale - Cybercrime" (Utet Giuridica, 2019).
- Mastrangelo L., "Il *peculium quasi castrense* - Privilegio dei *palatini* in età tardo antica" (luglio 2004).
- Mayer D., Warner D., Siedel G., Lieberman K. J., "*Business Law and the Legal Environment: Master of Accountancy Edition*" (Flatworld, 2012).
- Marinucci G., Dolcini E., "Manuale di Diritto Penale - Parte Generale" (sesta ed., Giuffrè editore, 2017).

- McCarthy, John, Marvin Minsky, Claude Elwood Shannon, and Nathaniel Rochester, "*A proposal for the Dartmouth Summer Research Project on Artificial Intelligence*" (1955), trad. it. di G. Paronitti, in https://web.archive.org/web/20150112124045/http://www.dif.unige.it/epi/hp/frixione/dartmouth_proposal_ital.pdf.
- Millarand J., Kerr R. I., "*Delegation, Relinquishment and Responsibility: The Prospect of Expert Robots*".
- Morandi E., "La rappresentanza di società inglesi", in *L'attività negoziale dello straniero comunitario: casi e materiali*, Atti del Seminario di studio Formanote tenutosi a Verona, 26 settembre 2009, disponibile presso https://elibrary.fondazionenotariato.it/articolo.asp?art=24/2405&mn=3 (ultimo accesso 25 settembre 2020).
- Newell A., Shaw J. C. and Simon H. A., "*Chess-Playing Programs and the Problem of Complexity*", (*IBM Journal of Research and Development*, vol. 2, no. 4, pp. 320-335, Ott. 1958), doi: 10.1147/rd.24.0320.
- OSCE Annual Police Experts Meeting, Concept Paper, "*Artificial Intelligence and Law Enforcement: an Ally or an Adversary?*" (23-24 settembre 2019, Vienna Hofburg), disponibile presso https://dirittopenaleuomo.org/wp-content/uploads/2019/07/19.pdf (ultimo accesso 25 settembre 2020).
- Pagallo U., "*The Laws of Robots Crimes, Contracts, and Torts*" 1st ed. 2013 (Dordrecht: Springer Netherlands, 2013).
- Parodi C., Valentina Sellaroli, "Sistema Penale E Intelligenza Artificiale: Molte Speranze E Qualche Equivoco" (in Diritto Penale Contemporaneo, Fasciolo 6/2019).
- Ricard M., "*Sei un animale!*" (Milano: Sperling & Kupfer, 2016).
- Ruffolo U., Alpa G., Barbera A., "Intelligenza artificiale: il diritto, i diritti, l'etica" (Milano: Giuffrè, 2020).
- Santosuosso A., Boscarato C., Caroleo F, "*Robot e diritto: una prima ricognizione*", in NGCC, luglio-agosto 2012, pp. 1-24.

- Saunders, J., Hunt, P. & Hollywood, J.S. "*Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot*" (*J Exp Criminol* 12**,** 347–371, 2016).
- Searle, John. R., "*Minds, brains, and programs*" (*Behavioral and Brain Sciences* 3 (3): 417-457, 1980).
- Sharkey N., "*Towards a principle for the human supervisory control of robot weapons*", Special Issue on "*Investigating the Relationship between Future Technologies, Self and Society*" (Politica & Società, No. 2, maggio-agosto 2014).
- Shaw G., "*The Future Computed Ai & Manufacturing*" (Microsoft Corporation Redmond, Washington U.S.A. 2019), disponibile online presso https://3er1viui9wo30pkxh1v2nh4w-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/393/2019/06/Microsoft_TheFutureComputed_AI_MFG_Final_Online.pdf (ultimo accesso 25 settembre 2020).
- Somalvico, M., Amigoni, F., & Schiaffonati, V. (n.d.). "INTELLIGENZA ARTIFICIALE".
- Stinnesbeck J., Research Division Legislative Counsel Bureau, "*Research Brief On Autonomous Vehicles*" (Novembre 2017), disponibile online presso https://www.leg.state.nv.us/Division/Research/Publications/ResearchBriefs/AutonomousVehicles.pdf (ultimo accesso 25 settembre 2020).
- "*The Practice of Crime Linkage: A Review of the Literature*" (*Journal of investigative psychology and offender profiling.* 16, no. 3 (2019): 169–200). Torrente A., Schlesinger P., Anelli F., Granelli C.. "Manuale di Diritto Privato" (Milano: Giuffrè, 2015).
- "*The Psychology of Linking Crimes: A Review of the Evidence*" (*Legal and criminological psychology.* 12, no. 2 (2007): 233–249).
- Turing, A. M., "I.—Computing Machinery And Intelligence", (*Mind, LIX*(236), 433-460, 1950), doi:10.1093/mind/lix.236.433.
- U.S. Executive Office of the President - National Science and Technology Council - Committee on Technology: "*Preparing for the Future of Artificial Intelligence*" (by the Office of Science and Technology Policy, Ottobre 2016), disponibile online

presso https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (ultimo accesso 25 settembre 2020).

- Vasilyev, A, Ibragimov Z., Gubernatorova E., "*The Russian draft bill of "the Grishin Law" in terms of improving the legal regulation of relations in the field of robotics: critical analysis*"(Journal of Physics: Conference Series. 1333. 052027. 10.1088/1742-6596/1333/5/052027, 2019).
- Venturi M., "Key Crime. La chiave del crimine" (Profiling. I profili dell'abuso, 5 (4), 2014).
- Villani C., "*For A Meaningful Artificial Intelligence*", missione parlamentare dal settembre 2017 al marzo 2018 assegnata dal primo ministro Édouard Philippe.
- Wagner G., "*Robot Liability*", Working Paper No. 2 dell'Istituto di ricerca per il diritto e la trasformazione digitale (2019).
- Wein E. L., "*The Responsibility Of Intelligent Artifacts: Toward An Automation Jurisprudence*", Harvard Journal of Law & Technology, Volume 6 (Autunno 2017).
- Weng, Y., Chen C., Sun C., "*Toward the Human–Robot Co-Existence Society: On Safety Intelligence for Next Generation Robots*" (*Int J of Soc Robotics* 1, 267, 2009"). Disponibile in: https://doi.org/10.1007/s12369-009-0019-1.
- Wiener N., "*The Human Use Of Human Beings Cybernetics And Society*" (Boston: Houghton Mifflin, 1950), p. 162.
- Williams F. P., McShane M.D., "*Devianza e Criminalità*" (Il Mulino, 2002).
- Zara G., "Tra Il Probabile E Il Certo" (Diritto Penale Contemporaneo, 20 maggio 2016).

Sitografia

- Ackerman E., "*Google and Johnson & Johnson Conjugate to Create Verb Surgical, Promise Fancy Medical Robots*" *IEEE Spectrum*, 17 dicembre 2015, disponibile presso https://spectrum.ieee.org/automaton/robotics/medical-robots/google-verily-johnson-johnson-verb-surgical-medical-robots (ultimo accesso 25 settembre 2020).
- Benfatto L., "Microsoft blocca il software Tay: Era diventato razzista e xenofobo" (ilSole24ore, 25 marzo 2016), disponibile presso https://st.ilsole24ore.com/art/tecnologie/2016-03-25/microsoft-blocca-software-tay-era-diventato-razzista-e-xenofobo--095134.shtml?refresh_ce=1 (ultimo accesso 25 settembre 2020).
- Bonomo, G., "Opere dell'ingegno e Intelligenza Artificiale" (17 settembre 2019), disponibile presso https://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2019-09-17/opere-ingegno-e-intelligenza-artificiale-095708.php (ultimo accesso 25 settembre 2020).
- Cavalcanti G., "Che succede se sbaglia il robot chirurgo? L'esperto: «Presto assicurazioni obbligatorie anche per IA»" (Sanità Informazione, 7 Agosto 2019), disponibile presso https://www.sanitainformazione.it/lavoro/errore-robot-assicurazioni/ (ultimo accesso 25 settembre 2020).
- Canalys (31 luglio 2020). "*Global smartphone market Q2 2020*", disponibile presso https://www.canalys.com/newsroom/canalys-global-smartphone-market-declines-q2-2020 (ultimo accesso 25 settembre 2020).
- Chiara P. G., "Software e responsabilità da prodotto: Il caso del Boeing 737 MAX 8", (Cyberlaws, 28 aprile 2018), disponibile presso https://www.cyberlaws.it/2019/software-responsabilita-prodotto-caso-boeing/ (ultimo accesso 25 settembre 2020).
- *Dictionary.cambridge.org/it/*, s.v., "artificial intelligence", disponibile presso https://dictionary.cambridge.org/it/dizionario/inglese/artificial-intelligence (ultimo accesso 25 settembre 2020).
- Edwards L., "*Edwards' Three Laws for Roboticists*" [Web log post, 01 ottobre 2010]. Disponibile presso http://blogscript.blogspot.com/2010/10/edwards-three-laws-for-roboticists.html (ultimo accesso 25 settembre 2020).

- Eliot, L., "*Human In-The-Loop Vs. Out-of-The-Loop in AI Systems: The Case of AI Self-Driving Cars*" (08 Aprile 2019), disponibile presso https://www.aitrends.com/ai-insider/human-in-the-loop-vs-out-of-the-loop-in-ai-systems-the-case-of-ai-self-driving-cars/ (ultimo accesso 25 settembre 2020).
- Gaboriau S., "Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?", in "Una giustizia (im)prevedibile? Il dovere della comunicazione" (Questione Giustizia, Fascicolo 4/2018), disponibile presso https://www.questionegiustizia.it/rivista/2018-4.php (ultimo accesso 25 settembre 2020).
- Gao P., Hensley R., Zielke A. (14 febbraio 2018), "*A road map to the future for the auto industry*", disponibile presso https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/a-road-map-to-the-future-for-the-auto-industry (ultimo accesso 25 settembre 2020).
- Grand View Research, "*Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution (Hardware, Software, Services), By Technology (Deep Learning, Machine Learning), By End Use, By Region, And Segment Forecasts, 2020 - 2027*" (luglio 2020), disponibile presso https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market (ultimo accesso 25 settembre 2020).
- Guarriello V., "L'intelligenza artificiale tra profili giuridici ed alcune delle più attuali applicazioni al servizio della società" (Associazione Romana di Studi Giuridici), disponibile presso https://arsg.it/?p=1781#_ftnref9 (ultimo accesso 25 settembre 2020).
- Hammond, K. "*5 unexpected sources of bias in artificial intelligence*" (10 dicembre 2016), disponibile presso https://techcrunch.com/2016/12/10/5-unexpected-sources-of-bias-in-artificial-intelligence/?guccounter=1 (ultimo accesso 25 settembre 2020).
- Hirsh J., "*The Policy Deficit Behind Canadian Artificial Intelligence*" (Centre for International Governance Innovation, 13 febbraio 2018) disponibile presso https://www.cigionline.org/articles/policy-deficit-behind-canadian-artificial-intelligence (ultimo accesso 25 settembre 2020).

- Iaselli M., “X-LAW: la polizia predittiva è realtà” (Altalex, 28/11/2018), disponibile presso https://www.altalex.com/documents/news/2018/11/28/x-law-la-polizia-predittiva (ultimo accesso 25 settembre 2020).
- International Data Corporation, “*IDC Forecasts Strong 12.3% Growth for AI Market in 2020 Amidst Challenging Circumstances*” (4 agosto 2020), disponibile presso https://www.idc.com/getdoc.jsp?containerId=prUS46757920 (ultimo accesso 25 settembre 2020).
- Judicial Education Center, University of New Mexico, disponibile presso http://jec.unm.edu (ultimo accesso 25 settembre 2020).
- Katznelson, G., “AI Citizen Sophia and Legal Status” (09 novembre 2017), disponibile presso https://blog.petrieflom.law.harvard.edu/2017/11/09/ai-citizen-sophia-and-legal-status/ (ultimo accesso 25 settembre 2020).
- Krausová, A., “*First Residency to AI Chatbot Shibuya Mirai*” (16 novembre 2017), disponibile presso http://www.biotechmerge.com/?p=116 (ultimo accesso 25 settembre 2020).
- Lahalle, M., “*L’Arabie saoudite accorde la citoyenneté à un robot… de sexe féminin*” (13 novembre 2017), disponibile presso https://madame.lefigaro.fr/societe/l-arabie-saoudite-accorde-la-citoyennete-a-sophia-robot-de-sexe-feminin-271017-135000 (ultimo accesso 25 settembre 2020).
- Lavalle C., “In Estonia il giudice sarà un’intelligenza artificiale” (La Stampa, 04 Aprile 2019), disponibile presso https://www.lastampa.it/tecnologia/news/2019/04/04/news/in-estonia-il-giudice-sara-un-intelligenza-artificiale-1.33692863?refresh_ce (ultimo accesso 25 settembre 2020).
- Law Library - American Law and Legal Information, “*Strict Liability*”, disponibile presso https://law.jrank.org/pages/10551/Strict-Liability.html (ultimo accesso 25 settembre 2020).
- *Lexico.com*, s.v., “artificial intelligence", disponibile presso https://www.lexico.com/definition/artificial_intelligence (ultimo accesso 25 settembre 2020).
- Livni E., “Nei tribunali del New Jersey è un algoritmo a decidere chi esce su cauzione” (Internazionale, 2 marzo 2017), disponibile presso https://

www.internazionale.it/notizie/ephrat-livni/2017/03/03/tribunali-algoritmo-cauzione (ultimo accesso 25 settembre 2020).

- Lum K., "*Predictive Policing Reinforces Police Bias*" (*Human Rights Data Analysis Group*, 10 ottobre 2016), disponibile presso https://hrdag.org/2016/10/10/predictive-policing-reinforces-police-bias/ (ultimo accesso 25 settembre 2020).
- MarketsandMarkets, "*Artificial Intelligence Market by Offering (Hardware, Software, Services), Technology (Machine Learning, Natural Language Processing, Context-Aware Computing, Computer Vision), End-User Industry, and Geography - Global Forecast to 2025*" (febbraio 2018), disponibile presso https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-market-74851580.html (ultimo accesso 25 settembre 2020).
- Morelli C., "Giustizia predittiva: il progetto (concreto) della Corte d'appello di Brescia" (Altalex, 08 aprile 2019), disponibile presso https://www.altalex.com/documents/news/2019/04/08/giustizia-predittiva#uno (ultimo accesso 25 settembre 2020).
- Morosi, D., "L'Arabia Saudita dà la cittadinanza a Sophia, una donna robot", (30 ottobre, 2017), disponibile presso https://www.corriere.it/tecnologia/17_ottobre_30/arabia-saudita-da-cittadinanza-sophia-donna-robot-ec459068-bd47-11e7-b457-66c72633d66c.shtml (ultimo accesso 25 settembre 2020).
- Morris D., "*Mercedes' Self-Driving Cars Would Save Passengers, Not Bystanders*" (Fortune, 15 ottobre 2016), disponibile presso https://fortune.com/2016/10/15/mercedes-self-driving-car-ethics/ (ultimo accesso 25 settembre 2020).
- Mozur P., "*Beijing Wants A.I. to Be Made in China by 2030*" (New York Times, 20 luglio 2017), disponibile presso https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html?_r=0 (ultimo accesso 25 settembre 2020).
- O'Carroll, B. (31 gennaio 2020). "*What Are The 3 Types Of AI? A Guide To Narrow, General, And Super Artificial Intelligence*", disponibile presso https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible (ultimo accesso 25 settembre 2020).

- Peirolo M, "*Le forniture di software in ambito intra-UE ed extra-UE*", Euroconference News Retrieved, edizione del 31 luglio 2017, https://www.ecnews.it/wp-content/uploads/pdf/2017-07-31_le-forniture-software-ambito-intra-ue-ed-extra-ue.pdf (ultimo accesso 25 settembre 2020).
- Pelliccia R., "Polizia Predittiva: il futuro della prevenzione criminale?" (9 Maggio, 2019). Disponibile inhttps://www.cyberlaws.it/2019/polizia-predittiva-il-futuro-della-prevenzione-criminale/ (ultimo accesso 25 settembre 2020).
- Pettine S., "Windows 10, gli aggiornamenti recenti impediscono ai programmi di funzionare a dovere" (13 giugno 2020), disponibile in https://multiplayer.it/notizie/windows-10-aggiornamenti-recenti-impediscono-programmi-funzionare-a-dovere.html (ultimo accesso 25 settembre 2020).
- Portale dedicato all'Intelligenza Artificiale. "Intelligenza Artificiale: Cos'è, Come Funziona E A Cosa Serve?" (N.D.), disponibile presso https://www.intelligenzaartificiale.it/ (ultimo accesso 25 settembre 2020).
- SAS Institute (n.d.). "Intelligenza Artificiale: Che cos'è e come funziona", disponibile presso https://www.sas.com/it_it/insights/analytics/what-is-artificial-intelligence.html (ultimo accesso 25 settembre 2020).
- Schirmer J., "*Germany's half-hearted draft law on automated vehicles*", disponibile presso https://www.jura.fu-berlin.de/fachbereich/einrichtungen/zivilrecht/lehrende/schweitzerh/informationen/Datenordner/Autonomous-Driving/002-SlidesAutomatedVehicles.pdf (ultimo accesso 25 settembre 2020).
- Sgarro, V., "*What Exactly Does It Mean to Call for "Ethics in Design"?*" (13 agosto 2018), disponibile presso https://slate.com/technology/2018/08/ethics-in-design-what-exactly-does-that-mean.ht (ultimo accesso 25 settembre 2020).
- Signorelli A.D., "Il software italiano che ha cambiato il mondo della polizia predittiva" (Wired, 18 maggio 2019), disponibile presso https://www.wired.it/attualita/tech/2019/05/18/polizia-predittiva-software-italiano-keycrime/?refresh_ce= (ultimo accesso 25 settembre 2020).
- Sophia and SingularityNET: Q&A [Intervista di C. Lawrence] (*Humanity+ Magazine,* 5 Novembre 2017). *Humanity+ Magazine*, disponibile presso https://

hplusmagazine.com/2017/11/05/sophia-singularitynet-qa/ (ultimo accesso 25 settembre 2020).

- Strategic Research Agenda (SRA) for Robotics in Europe, "*Glossario Tecnico*", disponibile presso https://www.eu-robotics.net/cms/front_content.php (ultimo accesso 25 settembre 2020).
- Tesla (n.d.), "Autopilot AI", disponibile presso https://www.tesla.com/it_IT/autopilotAI (ultimo accesso 25 settembre 2020).
- *The Great Soviet Encyclopedia, 3rd Edition*. S.v. "Civil Turnover", disponibile presso https://encyclopedia2.thefreedictionary.com/Civil+Turnover (ultimo accesso 25 settembre 2020).
- Tiffany K., "*Lil Miquela and the virtual influencer hype, explained*" (03 Giugno 2019), disponibile presso https://www.vox.com/the-goods/2019/6/3/18647626/instagram-virtual-influencers-lil-miquela-ai-startups (ultimo accesso 25 settembre 2020).
- Traversi A., "Intelligenza artificiale applicata alla giustizia: ci sarà un giudice *robot*?" (Questione Giustizia, 10 aprile 2019), disponibile presso https://www.questionegiustizia.it/articolo/intelligenza-artificiale-applicata-alla-giustizia-ci-sara-un-giudice-robot-_10-04-2019.php (ultimo accesso 25 settembre 2020).
- *Treccani.it, s.v., "PECULIO"* ultima consultazione il 25 settembre 2020, https://www.treccani.it/enciclopedia/peculio_%28Enciclopedia-Italiana%29/.
- *Treccani.it, s.v., "robòt"* ultima consultazione il 25 settembre 2020, https://www.treccani.it/vocabolario/robot.
- *Treccani.it, s.v., "senzienza"* ultima consultazione il 25 settembre 2020, http://www.treccani.it/vocabolario/senzienza_%28Neologismi%29/.
- Tuninetti R., "Sistemi di investigazione predittiva: cosa sono, come funzionano e i dubbi privacy" (Agenda Digitale, 19 Mar 2020), disponibile presso https://www.agendadigitale.eu/sicurezza/privacy/sistemi-di-investigazione-predittiva-cosa-sono-come-funzionano-e-i-dubbi-privacy/ (ultimo accesso 25 settembre 2020).
- Vaciago G., "KEY CRIME: un futuro costituzionalmente ammissibile?" (30 luglio 2014), disponibile presso http://www.replegal.it/it/tmt-telecomunication-media-

technology/item/413-key-crime-un-futuro-costituzionalmente-ammissibile (ultimo accesso 25 settembre 2020).

- Viola L., "Giustizia predittiva: è preferibile un modello deduttivo" (Altalex, 10 marzo 2020), disponibile presso https://www.altalex.com/documents/news/2020/03/10/giustizia-predittiva-preferibile-modello-deduttivo (ultimo accesso 25 settembre 2020).
- Vincent, C., "*Brussels parliament adopts crucial animal rights bill*" (23 novembre 2018), disponibile presso https://www.brusselstimes.com/brussels/52089/brussels-parliament-adopts-crucial-animal-rights-bill/ (ultimo accesso 25 settembre 2020).

Riferimenti Normativi

- *Asilomar AI Principles*. (2017). Principi sviluppati durante la conferenza di Asilomar del 2017. Disponibile presso https://futureoflife.org/ai-principles.
- Assemblée Nationale (France), Amendement n°59, 11 aprile 2014, disponibile presso http://www.assemblee-nationale.fr/14/amendements/1808/AN/59.asp (ultimo accesso 25 settembre 2020).
- Assemblea Parlamentare del Consiglio d'Europa, "T*echnological convergence, artificial intelligence and human rights*", Raccomandazione 2102/2017.
- Cass. civ., Sez. III, 20 gennaio 1999, n. 484.
- Cass. civ., Sez. III, 22 dicembre 2011, n. 28299.
- Cass. civ., sez. III, 29 maggio 2013, n. 13458.
- Cass. civ., sez. III, 14 novembre 2014, n. 23432.
- Cass. civ., Sez. III, 22 marzo 2015, n. 7260.
- Cass. Pen., sez. III, n. 46291 del 16/10/2003.
- Commissione Europea Per l'Efficienza Della Giustizia (CEPEJ), "Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi" CEPEJ(2018)14, adottata nel corso della 31ª Riunione plenaria a Strasburgo, 3-4 dicembre 2018.
- Cons. Stato, sez. VI, 08 aprile 2019 n. 2270.
- Cons. Stato, sez. VI, 13 dicembre 2019 n. 8472.
- Convenzione di Berna per la protezione delle opere letterarie e artistiche del 9 settembre 1886, completata a Parigi il 4 maggio 1896, riveduta a Berlino il 13 novembre 1908, completata a Berna il 20 marzo 1914 e riveduta a Roma il 2 giugno 1928, a Bruxelles il 26 giugno 1948, a Stoccolma il 14 luglio 1967 e a Parigi il 24 luglio 1971.
- Decisione N. 768/2008/Ce del Parlamento Europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE.
- Decreto Legislativo 6 settembre 2005, n. 206 "Codice del Consumo".

- Direttiva 1985/374/CEE del Consiglio, del 25 luglio 1985, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi.
- Direttiva 1999/44/CE del Parlamento europeo e del Consiglio, del 25 maggio 1999, su taluni aspetti della vendita e delle garanzie dei beni di consumo.
- Direttiva 2001/95/CE del Parlamento Europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti.
- Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione).
- *Elections in Kingdom of Saudi Arabia*, disponibile presso https://www.my.gov.sa/wps/portal/snp/aboutksa/electionsInTheKingdomOfSaudiArabia/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zivQIsTAwdDQz9LSw8XQ0CnT0s3JxDfA2AQD84NU-_INtREQAI12hE/ (ultimo accesso 25 settembre 2020).
- European Commission "*WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust"* (2020).
- Gaio, "*Institutiones*".
- Legge N. 8.078 dell'11 Settembre 1990, *Código De Defesa Do Consumidor*, disponibile presso https://presrepublica.jusbrasil.com.br/legislacao/91585/codigo-de-defesa-do-consumidor-lei-8078-90 (ultimo accesso 25 settembre 2020).
- *Montreal Declaration for a Responsible Development of Artificial Intelligence*. (2017). Da una iniziativa del 2017 dell'Université de Montréal, pubblicata nel 2018. Disponibile presso https://www.montrealdeclaration-responsibleai.com/the-declaration (ultimo accesso 25 settembre 2020).
- New Zealand Judicature Amendment Act 1972, pt 1, 3A, disponibile presso http://www.legislation.govt.nz/bill/government/2013/0107/latest/whole.html#DLM5174815 (ultimo accesso 25 settembre 2020).
- Mracek *v.* Bryn Mawr Hosp., 610 F. Supp. 2d 401 (E.D. Pa. 2009).
- Online Dispute Resolution Advisory Group, "*Online Dispute Resolution For Low Value Civil Claims*" (Civil Justice Council, febbraio 2015). People ex rel. Nonhuman Rights Project, Inc. v Lavery, 124 AD3d 148 (3rd Dep't 2014).

- Progetto di Relazione del Parlamento europeo del 31 maggio 2016 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)) (PR\1095387IT.doc).
- Quebec Animal Welfare and Safety Act (chapter B-3.1), disponibile presso http://legisquebec.gouv.qc.ca/en/ShowDoc/cs/B-3.1 (ultimo accesso 25 settembre 2020).
- *Restatement (Second) of Torts*, American Law Institute (1965).
- Regolamento (Ce) N. 765/2008 del Parlamento Europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93.
- Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (doc. P8_TA(2017)0051.
- Saudi Arabia - Constitution, adottata marzo 1992, disponibile presso https://www.legal-tools.org/doc/8942f2/pdf/ (ultimo accesso 25 settembre 2020).
- The Principles Of European Contract Law 2002 (Parts I, II, and III), EU.
- The Principles Of European Tort Law 2005, EU.
- U.S. Congress, Senate, "*Future of Artificial Intelligence Act of 2017*", S 2217, 115th Cong., 1st sess. (introduced in Senate December 12, 2017), disponibile presso https://www.congress.gov/bill/115th-congress/senate-bill/2217/text (ultimo accesso 25 settembre 2020).