Il processo di digitalizzazione del settore automobilistico. Quando il progresso tecnologico deve sempre essere supportato da norme, regole di condotta e buone pratiche

The digitalisation process in the automotive sector. When technological progress must always be supported by standards, codes of conduct and best practices

Michela Morelli[1]

Sommario

Il saggio esamina la relazione tra vetture intelligenti e diritto alla privacy. Nella sezione iniziale, si analizza la digitalizzazione del veicolo, che include non solo l'automazione della guida ma anche altri aspetti informatici, spesso trascurati e vulnerabili agli attacchi esterni. L'importanza di questa vulnerabilità è stata riconosciuta nel 2022 con l'emissione di due regolamenti dell'UNECE che impongono agli sviluppatori di veicoli rigorose responsabilità per proteggere la privacy del conducente.

La seconda parte approfondisce la responsabilità civile legata all'uso dell'intelligenza artificiale nelle vetture, esplorando le argomentazioni più accreditate.

Nella sezione conclusiva, si invita il lettore a riflettere su quanti diritti fondamentali sia disposto a sacrificare per una vita completamente digitalizzata.

Parole chiave: vetture intelligenti, responsabilità civile, diritti fondamentali, privacy, vita digitalizzata.

Abstract

The essay examines the relationship between smart cars and the right to privacy. In the first section, it analyzes the digitalization of vehicles, which includes not only driving automation but also other IT aspects that are often overlooked and vulnerable to external attacks. The importance of this vulnerability was recognized in 2022 with the issuance of two UNECE regulations that impose strict responsibilities on vehicle developers to protect the driver's privacy.

1 Dipartimento di Bioscienze e Territorio, Università degli Studi del Molise. michelamorelli90@gmail.com

Data invio: 30 agosto 2023. Data accettazione: 27 aprile 2024.
DOI: https://doi.org/10.54103/1972-5760/27558

The second part delves into civil liability related to the use of artificial intelligence in vehicles, exploring the most credible arguments.
In the concluding section, the reader is invited to reflect on how many fundamental rights they are willing to sacrifice for a fully digitalized life.

Keywords: smart vehicle, civil liability, fundamental rights, privacy, digitalized life.

1. Introduzione

Nell'attuale Era Digitale la tecnologia e il diritto esercitano un'influenza pervasiva sulla vita quotidiana dei cittadini. In questo incontro tra diritto e tecnologia, emerge la necessità di una nuova figura giuridica: il giurista interdisciplinare; tale figura è imprescindibile, poiché il giurista deve essere capace di accogliere il progresso tecnologico e integrarlo armoniosamente nel sistema normativo. Il ruolo di questa figura è di mediatore tra diritto e tecnologia, per promuovere la comprensione reciproca e facilitare la collaborazione tra esperti di entrambi i settori; a tal proposito, è emblematica la seguente riflessione: "per i giuristi si pone il problema di stabilire regole che non soffochino i progressi scientifici, ma che al contempo non ledano i diritti degli individui" (Faralli 2019, pp. 44-55).

Già con l'avvento dei primi computer, ai giuristi è stato imposto di esaminare gli effetti giuridici che queste nuove tecnologie producevano sull'uomo.

A livello nazionale l'impulso a regolamentare l'evoluzione tecnologica si è manifestato all'inizio degli anni Novanta, con l'istituzione dell'AIPA, l'Autorità per l'informatica nella pubblica amministrazione[2] ed è poi proseguito con l'istituzione del Garante per la protezione dei dati personali[3].

Contemporaneamente, l'Unione europea, ritenendo necessario disciplinare l'uso della tecnologia e, da ultimo dell'intelligenza artificiale, si è adoperata per instaurare una proficua collaborazione sia con gli Stati membri che con gli Organismi internazionali, per predisporre standard globali nell'ambito dell'intelligenza artificiale e per fronteggiare congiuntamente le sfide che essa presenta.

L'Unione Europea, poi, sta promuovendo fortemente l'utilizzo etico dell'intelligenza artificiale, attraverso finanziamenti mirati per la formazione e l'istruzione in questo settore. Tale impegno ha, anche, l'obiettivo di impiegare l'intelligenza artificiale per promuovere il progresso sociale, mantenendo saldi i valori fondamentali dell'identità europea e prevenendo potenziali

2 Istituita con il Decreto Legislativo n. 39 del 12 febbraio1993.
3 Previsto nella Legge 31 dicembre 1996, n. 675.

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

conflitti con tali valori che questa potente tecnologia potrebbe provocare; in quest'ottica, ha predisposto un quadro normativo di settore basato su principi di trasparenza, equità, responsabilità, sicurezza, partecipazione umana e protezione della privacy.

Tali norme sono progettate per rendere trasparente l'utilizzo dell'IA, garantire l'imparzialità, definire responsabilità per eventuali danni, assicurare la sicurezza, mantenere il controllo umano nelle decisioni critiche e proteggere i dati personali; attualmente, però, la responsabilità è il principio meno soggetto a regolamentazione.

Nel dicembre 2023, Consiglio dell'UE e Parlamento europeo hanno raggiunto un accordo sugli emendamenti al Regolamento sull'intelligenza artificiale, noto come IA Act. Questo regolamento, approvato dal Parlamento europeo il 13 marzo 2024, disciplina l'uso dell'intelligenza artificiale nell'UE ed ha l'obiettivo di promuovere l'innovazione tecnologica garantendo il rispetto dei diritti fondamentali imponendo dei requisiti rigorosi per i sistemi di IA ad alto rischio e prevedendo delle norme trasparenti. L'IA Act stabilisce dei meccanismi di sorveglianza e prevedere delle sanzioni per assicurare uno sviluppo ed un utilizzo etico e legale dei sistemi di IA.

L'IA Act, inoltre, ha il compito di preservare i principi etici e i diritti umani fondamentali, incentivando, contemporaneamente, l'applicazione dell'intelligenza artificiale. La norma prevede, altresì, restrizioni su pratiche di liceità dubbia, quali manipolazione comportamentale, riconoscimento facciale, punteggio sociale e polizia predittiva, consentendo l'uso dell'identificazione biometrica remota in spazi pubblici solo alle autorità di polizia con adeguate tutele per la protezione e il controllo contro i crimini terroristici.

In definitiva, il quadro normativo dell'Unione Europea è volto a

> migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale nell'Unione, in conformità con i valori dell'Unione. Promuove la diffusione di un'intelligenza artificiale antropocentrica e affidabile, garantendo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione (Parlamento europeo 2024, p. 3).

2. La digitalizzazione dell'automobile. Innovazione normativa

Nel settore automotive, il processo di informatizzazione è iniziato solo negli ultimi vent'anni e, come in altri settori, il boom digitale ha colto impreparato il mondo del diritto. Recentemente, le Istituzioni europee, riconoscendo il ritardo legislativo rispetto al rapido progresso, hanno sollecitato gli Stati

membri a intervenire nei settori dell'industria automobilistica e della cybersicurezza, emanando Direttive e Regolamenti volti a implementare una politica di digitalizzazione nel settore automobilistico. Un esempio significativo è il Regolamento 2019/2144, che ha introdotto, a partire dal 2022, l'obbligo di installare su tutti i veicoli di nuova immatricolazione undici dispositivi tecnologici avanzati (Advanced driver assistance systems - ADAS), tra cui il registratore dati di evento, noto come scatola nera, che registra informazioni che, in caso di incidenti stradali, facilitano una dettagliata ricostruzione dell'evento.

Tale obbligo si inserisce nella strategia europea per la sicurezza stradale denominata "Zero morti sulle strade entro il 2050" che promuove l'impiego dell'intelligenza artificiale nelle autovetture per prevenire incidenti e tutelare la sicurezza dei conducenti e degli utenti della strada.

Si deve, inoltre, affermare che la digitalizzazione dei veicoli e il concetto di cybersecurity solo in una piccolissima percentuale afferiscono all'automazione della guida mentre, nella maggior parte dei casi, riguarda tutti gli altri dispositivi di assistenza alla guida presenti nel veicolo stesso, emblematica è, infatti, la seguente affermazione: "partendo dall'assunto che tra qualche anno, secondo gli operatori del settore, si parlerà sempre più di auto hackerata, invece che rubata, il concetto di cybersecurity all'interno del mondo delle auto connesse è ormai un must" (Carrà 2021, p. 1).

Ebbene, l'automazione alla guida è solo uno dei processi di informatizzazione, infatti, le case automobilistiche, sia per rispondere alle normative sia per soddisfare la domanda di mercato, hanno progettato modelli con sempre più sistemi digitali, un esempio è il "*virtual cockpit*" o cruscotto digitale, sviluppato da alcune importanti case automobilistiche, che offre al conducente un navigatore satellitare e un assistente vocale sempre attivi.

2.1. La vulnerabilità delle autovetture smart

La rapida diffusione dell'intelligenza artificiale nel settore automobilistico ha sollevato interrogativi significativi tra i giuristi: emergono nuove forme di responsabilità legate all'uso dell'IA nei veicoli? Le normative attuali sono adeguate a regolamentare queste nuove dinamiche? È necessaria un'armonizzazione normativa a livello europeo per affrontare le sfide poste da queste tecnologie? Questi quesiti, sorti in ritardo rispetto al progresso tecnologico, sono cruciali anche perché, solo negli ultimi cinque anni, è stata acquisita la consapevolezza che i veicoli possono essere oggetto di attacchi cyber; infatti, in un'intervista pubblicata su Forbes nel 2021, Massimiliano Carrà discute la cybersecurity automobilistica con Fausto Mozzarella, evidenziando tre aree critiche di accesso o superficie di attacco: accesso fisico all'auto tramite l'interfaccia OBD, accesso a breve distanza tramite sistemi come il *keyless*

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

entry, e accesso a lunga distanza tramite sistemi di comunicazione wireless come Wi-Fi o 4/5G.

A partire dal 2018, le Istituzioni europee hanno analizzato approfonditamente il fenomeno delle smart cars e, in generale, analizzando l'ingerenza dell'intelligenza artificiale nella vita quotidiana degli individui. In quest'ottica, il 19 febbraio 2020, la Commissione europea ha redatto il "Libro Bianco sull'Intelligenza Artificiale - Un approccio europeo all'eccellenza e alla fiducia", sottolineando la necessità che l'IA europea si basi sui valori e diritti fondamentali come la dignità umana e la privacy. Il Libro Bianco si interroga sui rischi legati all'hackeraggio dei sistemi tecnologici delle automobili, evidenziando che ogni comando implementato dall'auto in modo non meccanico può essere compromesso, con conseguenze che vanno dal furto di informazioni alla compromissione della sicurezza fisica dei passeggeri e degli utenti della strada.

Ebbene, queste considerazioni iniziali hanno guidato la formulazione delle norme di dettaglio pubblicate successivamente.

2.2. Tutela giuridica e Regolamenti UNECE

Nel settore automobilistico, un'attenzione particolare alla protezione degli utenti nell'uso dell'intelligenza artificiale è emersa negli ultimi due anni quando le Istituzioni internazionali, passando da un periodo di stasi normativa a uno caratterizzato da un attivismo legislativo, hanno pubblicato, i Regolamenti UNECE 155 ed UNECE 156, che impongono stringenti vincoli ai produttori per garantire una maggiore protezione in termini di sicurezza informatica dei veicoli.

Prima di esaminare questi regolamenti, è necessario comprendere il contesto storico in cui sono stati pubblicati: nel corso dell'ultimo decennio, le case automobilistiche hanno gradualmente integrato componenti informatiche. Tuttavia, si ripete, la sicurezza informatica nel settore automobilistico è diventata oggetto di discussione solo a partire dal 2020, quando il Parlamento europeo e le organizzazioni internazionali hanno avviato il processo di creazione di una normativa specifica per armonizzare le legislazioni degli Stati membri.

A partire da questo momento, lo studio del ruolo dell'intelligenza artificiale nel settore automobilistico non si è limitato più solo all'analisi e alla regolamentazione delle auto a guida autonoma, ma si è esteso anche al resto della componentistica informatica, soggetta a possibili attacchi esterni.

Prima del 2020, gli studi nel settore si concentravano principalmente sulla diffusione delle auto automatiche e sulle relative questioni di responsabilità e i Regolamenti UNECE 155 e 156 rappresentano, invece, un'importante innovazione nel settore automobilistico. Questi Regolamenti, entrati in vi-

gore il 4 luglio 2022, prevedono un periodo di transizione; infatti, diverranno obbligatorie per tutti i veicoli, anche quelli già immessi sul mercato, solo dal quattro luglio 2024, mentre, attualmente sono obbligatorie solo per i veicoli di nuova immatricolazione. Tale approccio graduale è stato concepito proprio per consentire, alle società automobilistiche, di adeguarsi, anche a livello di assetto societario, a questo nuovo scenario legislativo, riconoscendo l'impatto considerevole che tali imposizioni avranno sul panorama automobilistico.

Nel dettaglio, il Regolamento 155 stabilisce che, per ottenere la certificazione UNECE, necessaria per l'immatricolazione del prototipo, i produttori di autoveicoli devono dimostrare all'Autorità UNECE che tutti i sistemi informatici del veicolo sono sicuri e conformi alle normative europee; devono dimostrare di conoscere i processi di creazione del sistema informatico installato nel veicolo e, se si affidano a fornitori terzi, devono possedere la documentazione attestante il processo di creazione del software o dell'hardware inserito nei veicolo. È richiesto, infatti, che i fornitori rispettino le norme UNECE, anche se non operano e non hanno sede nei Paesi firmatari. I produttori devono, poi, dichiarare di essere pronti a risolvere eventuali problemi di cybersecurity sui veicoli e dimostrare che gli ambienti in cui sono stati sviluppati i software installati sulle vetture sono sicuri e rispondono ai parametri della normativa.

Le disposizioni del Regolamento 155 impongono ai costruttori di identificare gli elementi critici del veicolo in termini di sicurezza informatica, valutare i rischi associati e implementare misure proporzionate per proteggere il veicolo da tali rischi. È, altresì, richiesta una verifica annuale, in cui si informa l'Autorità certificatrice sul monitoraggio dei sistemi informatici e le modifiche rilevanti alle prestazioni tecniche relative alla cybersicurezza.

Il Regolamento 156, invece, riguarda principalmente gli aggiornamenti software. Secondo questa norma, il costruttore deve sempre informare il consumatore finale dell'esecuzione di aggiornamenti, dimostrando e certificando la sicurezza durante l'esecuzione. Inoltre, in caso di aggiornamento via etere, il costruttore deve dimostrare all'Autorità di poter arrestare il singolo veicolo e renderlo non marciante per tutta la durata dell'installazione dell'aggiornamento. Questa disposizione ha sollevato preoccupazioni tra i produttori, che potrebbero dover gestire un grande numero di veicoli anche dopo la vendita, costringendoli a prediligere, quindi, l'aggiornamento manuale.

Queste nuove normative segnano una svolta nel settore automobilistico, in quanto per la prima volta le Istituzioni sono intervenute sulla regolamentazione del sistema informatico delle autovetture, al fine di tutelare la privacy degli utenti.

Anche in questo settore, emerge, però, una significativa contraddizione nella società contemporanea: da un lato, una quasi totale digitalizzazione

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

della vita quotidiana, dall'altro una maggiore vulnerabilità della sfera privata, soggetta a sempre più intrusioni attraverso dispositivi digitali e tecnologie smart. La crescente presenza di dispositivi e sistemi informatici nelle autovetture solleva legittime preoccupazioni sulla tutela della privacy individuale, con il rischio che conversazioni private tra gli occupanti del veicolo possano essere captate per scopi commerciali e non solo.

La responsabilità in caso di violazione del diritto alla privacy attraverso il sistema informatico dell'autovettura è una questione complessa e le nuove normative, come UNECE 155 e 156, non hanno affrontato esplicitamente il problema dell'intrusione malevola in detti sistemi.

Si confida, pertanto, che future leggi stabiliscano chiaramente le eventuali responsabilità delle case automobilistiche e degli sviluppatori di software nel garantire la sicurezza informatica e la protezione della privacy e che prevedano, in caso di violazioni, sanzioni o misure correttive. È possibile che la responsabilità venga estesa anche agli utenti stessi nel caso in cui la violazione derivi da comportamenti negligenti o dalla mancata adozione di misure di sicurezza consigliate.

In definitiva, la tutela della privacy in un contesto sempre più digitalizzato richiede un approccio interdisciplinare che coinvolga legislatori, aziende e utenti per garantire un equilibrio tra innovazione tecnologica e rispetto dei diritti fondamentali.

3. Intelligenza artificiale e responsabilità giuridica

3.1. I contratti informatici

Prima di cercare di rispondere agli interrogativi sollevati in materia automotive, è opportuna una breve analisi dei contratti che interagiscono con l'intelligenza artificiale.

Nella letteratura giuridica, sono state elaborate varie classificazioni dei c.d. contratti informatici. Alcuni studiosi distinguono tra "contratti telematici" e "contratti cibernetici": l'appellativo "telematici" si riferisce a contratti in cui offerta e accettazione avvengono attraverso l'utilizzo di un computer, mentre quelli definiti "cibernetici" implicano che il computer stesso agisca come mezzo di formazione della volontà o integrazione della volontà dei contraenti fisici (Proietti 2020, p. 129). Altri distinguono, invece, tra contratti telematici e contratti digitali, mantenendo tra di loro una relazione di genere e specie.

È possibile definire il contratto cibernetico come quello in cui l'elemento informatico svolge un ruolo fondamentale nella conclusione e nell'esecuzione del contratto, considerato come un patto giuridico concretizzatosi attraverso l'interazione di entità computazionali avanzate. In questo con-

testo, l'attributo "cibernetico" enfatizza l'utilizzo e l'interazione di sistemi informatici nel processo contrattuale, superando il tradizionale modello di contrattazione tra i soli soggetti umani (Procida Mirabelli 2020).

All'interno del contratto cibernetico, poi, la dottrina ha elaborato una distinzione ulteriore tra *machine learning* e *data mining*: mentre il secondo presuppone sempre e comunque l'intervento dell'uomo, il machine learning, una volta stabilite pedissequamente le regole contrattuali, non necessita più dell'intervento umano ed è capace di elaborare testi e dati da solo. In entrambi i casi, però, sono stati riscontrati errori dovuti, nel primo caso, a un "addestramento insufficiente impartito alla macchina" e, nel secondo caso, "a una mole elevata di dati che potrebbe produrre relazioni prive di senso" (Proietti 2020, p. 136).

La classificazione della natura giuridica dei contratti informatici, tuttavia, non risolve il problema della responsabilità e, sul punto, alcuni studiosi hanno proposto di considerare l'agente software quale ente dotato di soggettività giuridica (Teubner 2019) attraverso la categorizzazione della *fictio iuris* e, in particolare, facendo ricorso alla rappresentanza ex art. 1387 c.c. e, infine, risolvendo il problema della capacità giuridica con l'utilizzo della firma digitale[4] (Limone 1995).

Secondo altra tesi (da preferire secondo chi scrive), non sarebbe necessario conferire una capacità giuridica al sistema informatico poiché vi sarebbe comunque una responsabilità da distribuire tra l'utilizzatore della macchina e l'altro contraente, secondo le normali disposizioni codicistiche previste in materia di inadempimento, responsabilità precontrattuale e responsabilità *in executivis* (Proietti 2020).

Un'altra teoria interessante, poi, riguarda l'equiparazione del sistema informatico al nuncio (Taddei Elmi, Romano 2016, pp. 115-137). Secondo tale elaborazione dottrinale, il sistema informatico non esprime una volontà propria, ma opera quale mero strumento per la trasmissione della volontà negoziale di un altro soggetto. In questa prospettiva, il sistema informatico assume una funzione analoga a quella del nuncius, il quale agisce in qualità di semplice veicolo di comunicazione senza autonomo potere decisionale (Bianca 2019, p. 71). Secondo questa impostazione, il sistema informatico, privo di autonoma capacità volitiva, si limita ad eseguire e trasmettere le istruzioni impartite dall'operatore umano, configurandosi quindi come un puro intermediario tecnico nella formazione e manifestazione della volontà contrattuale altrui. Questa interpretazione sottolinea l'importanza di considerare la responsabilità e il controllo umano nei processi automatizzati, ribadendo che la volontà negoziale, rilevante ai fini giuridici, risiede esclu-

4 La firma digitale può essere definita come la trasposizione informatica di una firma manoscritta convenzionale apposta su supporto cartaceo. La sua finalità consiste nell'attestare la legittimità, l'autenticità e l'origine di un documento digitale.

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

sivamente nel soggetto che utilizza il sistema informatico, che è ritenuto semplice strumento operativo.

Infine, quattro sono le categorie di contratti informatici elaborate: i contratti di licenza software, i contratti di sviluppo software, i contratti di *hosting e cloud*, e i contratti di servizi web.

In Italia, il Decreto-legge del 11 febbraio 2019 n. 12, conosciuto come "Decreto semplificazioni", ha introdotto disposizioni riguardanti gli *smart contract*, definiti come programmi informatici che operano su tecnologie basate su registri distribuiti e che vincolano automaticamente due o più parti in base a effetti predefiniti. Sebbene ci siano state critiche sulla definizione giuridica e sulla mancanza di una regolamentazione organica, il fatto che il legislatore italiano abbia affrontato esplicitamente la questione dell'uso dell'intelligenza artificiale nella contrattualistica è un passo significativo che mira a promuovere l'adattamento del sistema giuridico italiano ai nuovi sviluppi tecnologici.

L'adozione di tali disposizioni legislative pionieristiche rappresenta un segnale di apertura e adattamento del sistema giuridico italiano ai nuovi sviluppi tecnologici, fornendo maggiore certezza giuridica agli attori coinvolti nell'utilizzo di queste tecnologie e promuovendo l'innovazione e lo sviluppo tecnologico nel settore (Bellomia 2020).

3.2. La responsabilità civile nel settore cyber-automotive

Il settore automotive in Italia ha mostrato variazioni significative negli incidenti stradali nel periodo dal 2017 al 2022. Secondo l'Istituto Nazionale di Statistica (ISTAT), nel 2017 c'è stato un aumento del 3% nelle vittime stradali, seguito da una diminuzione dei decessi nel 2018, ma un aumento degli incidenti autostradali dell'18,5%. Nel 2022, gli incidenti sono aumentati del 9,9%, con un totale di 165.889 incidenti e 3.159 morti, oltre a 223.475 feriti.

L'Unione Europea ha l'ambizioso obiettivo di "Zero morti sulle strade entro il 2050" e ha manifestato la necessità di implementare l'utilizzo dell'intelligenza artificiale nei veicoli per ridurre gli incidenti stradali; questo obiettivo si è tradotto in una proliferazione normativa che impone ai produttori l'implementazione di dispositivi informatici nei nuovi veicoli al fine di migliorare la sicurezza stradale.

In questo contesto di evoluzione tecnologica e normativa, è importante considerare la responsabilità legale derivante dall'utilizzo dell'intelligenza artificiale.

Il concetto di responsabilità derivante dall'utilizzo dell'intelligenza artificiale è estremamente complesso e, ad oggi, rappresenta ancora un oggetto di studio approfondito.

In primo luogo, deve evidenziarsi l'assenza di una definizione precisa di intelligenza artificiale in letteratura.

Il termine Intelligenza Artificiale è stato coniato per la prima volta nel 1956 da John McCarthy, il quale ha sostenuto che per intelligenza artificiale si dovesse intendere "far comportare le macchine in modi che sarebbero chiamati intelligenti se un essere umano dovesse comportarsi allo stesso modo" (McCarthy 1950, p. 417).

Successivamente, Giovanni Sartor ha elaborato la seguente definizione:

> l'intelligenza si rivela nella capacità di svolgere diverse funzioni come l'adattamento all'ambiente, l'apprendimento dall'esperienza, la percezione, l'intuizione, il pensiero astratto, l'utilizzo efficiente di risorse limitate, la comunicazione. Tali funzioni, tanto diverse tra loro, sono unite dal fatto che consentono a chi le possieda di migliorare le proprie prestazioni (Sartor 2022, p. 1).

Da questa definizione emergono questioni centrali che i giuristi devono affrontare: fino a che punto siamo disposti a limitare i nostri diritti fondamentali per ottenere miglioramenti prestazionali? Siamo inclini a compromettere la salute, la privacy e la dignità in cambio di veicoli completamente informatizzati? Inoltre, i consumatori finali sono consapevoli delle implicazioni e delle possibili limitazioni dei loro diritti quando scelgono queste tecnologie, o sono forse meno informati di quanto credano?

Recentemente, si è iniziato a discutere se il sistema della responsabilità civile vigente possa essere applicato dopo la diffusione del pilota automatico. Questa ridefinizione del rapporto tra la responsabilità del conducente e quella del produttore potrebbe essere affrontata in fasi distinte e successive. In definitiva, emerge la necessità di delineare linee guida transitorie per sviluppare un quadro normativo adeguato che possa garantire un efficace controllo della circolazione stradale, specialmente nei contesti in cui l'intervento umano sarà progressivamente minimizzato fino a diventare trascurabile (Calabresi, Al Mureden 2021).

4. I rischi connessi alla informatizzazione automotive

4.1. Un primo campo d'indagine

L'analisi della responsabilità civile nel settore automobilistico si divide in due ambiti: il trattamento dei dati personali degli utenti tramite i sistemi informatici e l'automazione della guida. Un tipico caso rientrante nella prima ipotesi è, senza dubbio, l'utilizzo illecito dei servizi di geolocalizzazione presenti nell'autovettura:

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

> nel 2022 le auto circolanti con connettività integrata saranno 125 milioni in tutto il mondo. Questo scenario comprenderà cloud, IoT e 5G, che genereranno anche un'enorme superficie di attacco di milioni di utenti finali. In tale contesto un hacker avrebbe la possibilità, per esempio, di iniettare un virus attraverso l'installazione di una nuova app nel sistema infotainment della vettura, riuscendo in tal modo a effettuare un'operazione di sniffing come il tracciamento degli spostamenti o l'intercettazione delle conversazioni […]. Con la normativa Unece in arrivo a giugno, però, i nuovi modelli dovranno ottenere l'omologazione anche per la cybersecurity. Saranno essenzialmente tre i vincoli: progettazione dell'elettronica di bordo con algoritmi crittografici di protezione dati, monitoraggio delle flotte per il rilevamento dei cyber-attacchi e aggiornamento dei software per evitare l'obsolescenza dei sistemi (Cruciani 2022, p. 1).

Tra i principali rischi per la privacy connessi ai sistemi informatici presenti sulle automobili smart, emerge anzitutto il tracciamento costante della posizione del veicolo, il quale potrebbe essere sfruttato da terzi per monitorare i movimenti degli utenti. Un ulteriore rischio è rappresentato dal monitoraggio del comportamento di guida, che registra dati come la velocità e le frenate, senza il consenso esplicito dell'utente e potrebbe essere utilizzato per valutare il rischio di incidenti stradali e determinare le tariffe assicurative.

Inoltre, le case automobilistiche e i fornitori di servizi potrebbero condividere i dati raccolti con terze parti, esponendo gli utenti al rischio di accesso non autorizzato ai propri dati personali.

La connettività Internet delle automobili smart le rende vulnerabili ad intrusioni informatiche, come hackeraggi e accessi non autorizzati. La mancanza di consenso e controllo dell'utente implica che molti conducenti potrebbero non essere pienamente informati o consapevoli delle implicazioni sulla propria privacy derivanti dall'utilizzo di queste tecnologie (Mauro 2017).

Ebbene, la mancanza di trasparenza e dei meccanismi di acquisizione del consenso limita la capacità degli utenti di gestire e proteggere le proprie informazioni personali.

In questa specifica categoria, sia la normativa italiana che quella europea presentano una lacuna sostanziale nella determinazione del soggetto responsabile in caso di illecita sottrazione di informazioni personali e tale carenza legislativa, tra l'altro, veniva già evidenziata dal Parlamento europeo nel 2017:

> considerando che sono palesi le carenze dell'attuale quadro normativo in materia di responsabilità contrattuale, dal momento che le macchine progettate per scegliere le loro controparti, negoziare termini contrattuali, concludere contratti e decidere se e come attuarli rendano inapplicabili le norme tradizionali, il che pone in evidenza la necessità di norme nuove più al passo con i tempi (Parlamento europeo 2017, p. 6).

Attualmente, gli operatori del diritto dovrebbero concentrarsi sull'individuazione precisa del soggetto responsabile in scenari di furto illegittimo di dati personali attraverso il veicolo e ciò è fondamentale poiché i rischi sono elevati, mentre la consapevolezza dell'utente medio riguardo a tali questioni è molto limitata e le relative norme sulla responsabilità non sono ancora vigenti. La mancanza di chiarezza normativa in questo contesto potrebbe avere impatti significativi sulla tutela della privacy e sulla responsabilità legale e la collaborazione tra istituzioni europee e nazionali potrebbe rivelarsi fondamentale per l'elaborazione di normative coerenti e armonizzate in grado di affrontare le sfide emergenti nel contesto della sicurezza dei dati personali.

Continuando l'analisi dei problemi esistenti nella materia di cybersicurezza automobilistica, oltre all'illegittima geolocalizzazione, l'acquisizione malevola dei dati personali da parte del sistema informatico delle autovetture è connessa anche al problema della cosiddetta profilazione degli individui.

Attraverso la profilazione e il monitoraggio costante degli utenti attraverso le smart cars, è possibile categorizzare e classificare gli utilizzatori dei veicoli. Questa pratica solleva gravi preoccupazioni in termini di privacy e sicurezza delle informazioni personali, poiché la raccolta sistematica di dati sugli spostamenti e le abitudini degli utenti potrebbe consentire la creazione di profili dettagliati degli individui, mettendo a rischio la riservatezza e la protezione delle loro informazioni personali.

Il problema della profilazione illegittima dei dati degli utenti raccolti dai sistemi informatici è stato denunciato per la prima volta da Christopher Wylie, data scientist canadese ed ex dipendente di Cambridge Analytica che, nel 2018, ha rivelato di aver acquisito i profili Facebook di milioni di individui residenti negli Stati Uniti al fine di utilizzare le loro informazioni personali per la creazione di profili psicologici e politici sofisticati, influenzando così il loro convincimento politico (Cadwalladr 2017).

Questo scandalo, noto come lo "scandalo Facebook-Cambridge Analytica", ha suscitato l'indignazione delle Istituzioni democratiche mondiali e ha portato, da parte della Federal Trade Commission americana, l'avvio di un'indagine sulle politiche e sulle pratiche di Facebook riguardanti la raccolta, l'uso e la condivisione dei dati degli utenti, che si è conclusa con una sanzione di 5 miliardi di dollari inflitta a Facebook nel 2019 e con l'obbligo di implementare misure correttive e restrittive a tutela della protezione della privacy. Questo scandalo ha evidenziato la necessità di norme più stringenti e di meccanismi di sicurezza per proteggere gli individui dall'abuso dei loro dati personali in tutti i contesti tecnologici (Hu 2020).

Per quanto riguarda il settore automobilistico, però, questo rischio ancora non è stato adeguatamente affrontato perché non ancora completamente riconosciuto come pericolo concreto ed attuale.

Tuttavia, la minaccia è reale ed attuale e meccanismi di sicurezza avanzati, come crittografia e protezione dei dati, devono essere integrati, nel più breve

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

tempo possibile, anche nei sistemi informatici delle autovetture per mitigare il rischio di accessi non autorizzati e abusi. Parallelamente, è molto importante iniziare a sensibilizzare gli utenti sia sulle implicazioni della profilazione sia sulla portata cibernetica della propria vettura e, contemporaneamente, promuovere pratiche trasparenti nel trattamento dei dati. Quest'ultimo aspetto è fondamentale per garantire che gli individui siano pienamente consapevoli di come vengono utilizzate le loro informazioni e possano esercitare un controllo significativo sulla gestione dei propri dati personali.

In definitiva, la manipolazione a fini di marketing rappresenta una seria minaccia ed è, quindi, fondamentale sviluppare strategie e regolamenti mirati a prevenire, anche nel settore automobilistico, l'uso improprio delle informazioni personali per influenzare il comportamento individuale.

La frequenza degli episodi di profilazione illecita continua, poi, ad essere notevole: nel mese di novembre 2021, l'Autorità garante della concorrenza e del mercato ha inflitto a Google una sanzione di 10 milioni di euro a causa di una mancata informazione agli utenti-consumatori riguardo la raccolta dei loro dati sensibili a scopi commerciali. Tale sanzione è stata applicata al termine della fase istruttoria, durante la quale è emerso che i dati di ciascun utente venivano impiegati per scopi commerciali anche in assenza di un'autorizzazione esplicita da parte dei consumatori stessi.

Nel settore automobilistico, la questione della profilazione dei dati degli utenti rappresenta una sfida significativa. Occorre, infatti delineare come ottenere il consenso per la divulgazione dei suoi dati sensibili non solo del conducente ma anche di tutti i soggetti terzi presenti nell'abitacolo del veicolo stesso. Il rischio di profilazione persiste in tutti i casi in cui le smart cars raccolgono e conservano i dati degli utenti, un'eventualità che potrebbe coinvolgere tutti coloro i quali entreranno in un veicolo nel prossimo futuro. La raccolta dati può avvenire attraverso sensori integrati nel veicolo, sistemi di infotainment collegati a Internet e dispositivi di monitoraggio dell'efficienza e della sicurezza del veicolo. Alcuni veicoli più avanzati possono raccogliere numerosi dati personali, come la posizione GPS, i comportamenti di guida e i dati biometrici tramite sistemi di riconoscimento facciale. Queste informazioni possono essere utilizzate per creare profili dettagliati degli utenti e possono essere vulnerabili ad attacchi informatici, violazioni della privacy o abusi da parte di terze parti non autorizzate. La geolocalizzazione è spesso utilizzata per perpetrare reati sia in ambito familiare che in contesti criminali, evidenziando ulteriormente i rischi associati alla profilazione e alla raccolta di dati sensibili tramite le automobili smart.

Per mitigare e ridurre questi rischi, è necessario un quadro normativo chiaro che regoli la raccolta, l'elaborazione e l'utilizzo dei dati personali nei veicoli. Queste norme dovrebbero includere disposizioni specifiche sulla protezione dei dati personali, sul consenso informato degli utenti, sulla

trasparenza nelle pratiche di trattamento dei dati e meccanismi efficaci di controllo per gli utenti che ritengono violati i propri diritti alla privacy.

In relazione al rapporto smart cars – privacy interessante è la distinzione, elaborata da alcuni studiosi, in veicoli autonomi e veicoli interconnessi: mentre i primi non inoltrano le informazioni raccolte all'esterno, i veicoli interconnessi, al contrario, trasmettono i dati reperiti all'esterno dell'abitacolo ad altri dispositivi o altri smart veicoli che si incontrano lungo il tragitto; in quest'ultimo caso

> si assiste a un continuo scambio di informazioni relative all'ambiente stradale circostante, al percorso che sta percorrendo e che verrà percorso, ma anche i messaggi che vengono scambiati dagli altri passeggeri. Questi due modelli di driverless car pongono differenti implicazioni in tema di privacy. Il primo modello non porrà alcuna problematica posto che i dati personali che vengono raccolti rimangono all'interno del veicolo medesimo. Il secondo, proprio perché pensato per interagire con una rete esterna, potrà, alternativamente, fornire solamente le informazioni ritenute come strettamente necessarie per determinare il modus operandi degli altri veicoli presenti, oppure, comunicare anche quanto avviene al proprio interno (Della Giustina 2023, pp. 12-13).

Per tali ragioni il veicolo autonomo è considerato il più sicuro in relazione alla tutela della privacy.

Si confida, dunque, in un intervento normativo molto incisivo perché, attualmente, i legislatori, sia a livello nazionale che internazionale, concentrano la propria attenzione principalmente sul fenomeno della guida automatica, trascurando di analizzare le altre importanti problematiche correlate alla diffusione dei veicoli intelligenti, mentre è essenziale far comprendere l'importanza di un intervento legislativo e di un coinvolgimento da parte degli esperti giuridici anche in questa sotto categoria del diritto automobilistico, dato che il numero di vendite delle autovetture connesse è in costante aumento.

4.2. Un secondo campo d'indagine

> Il veicolo automatico deve anche essere considerato come un vero e proprio robot, definito come una macchina dotata di consapevolezza, in grado di interagire con l'ambiente circostante e di prendere decisioni "indipendentemente dal controllo o da influenze esterne" (Parlamento Europeo 2017, p. 5).

In Italia dal 2018 è consentito richiedere l'autorizzazione per condurre test di guida completamente autonoma e, da allora, i giuristi hanno cominciato a interrogarsi sulla determinazione della responsabilità in caso di inci-

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

denti stradali derivanti da tali veicoli. È bene precisare, però, che, secondo il Decreto smart roads, le vetture completamente automatizzate possono circolare solo se autorizzate e impiegate per esperimenti pianificati e controllati. Tuttavia, gli esperti stimano che, nel prossimo decennio, si assisterà verosimilmente a una proliferazione di veicoli automatici che condivideranno le strade con le vetture a guida umana, per poi diventare progressivamente le uniche ad essere immesse sul mercato.

Correntemente, nel dibattito sulla responsabilità legale del pilota automatico, vari orientamenti dottrinali propongono una riforma del codice delle assicurazioni. Questo mirerebbe a definire modalità risarcitorie per incidenti stradali causati da veicoli autonomi, simili a quelle previste per i droni nel Regolamento ENAC del 2019.

Un'opinione distinta, sostenuta da autorevole dottrina (Ruffolo 2020), al contrario, fa notare che le automobili a guida umana sono state brevettate solo alla fine del XIX secolo, con la prima autovettura, la *Patent motorwagen*, ideata dall'ingegnere tedesco Karl Benz e realizzata nel 1886 e subentrate ad un'altra modalità di trasporto. Ebbene, secondo questa prospettiva, poiché il codice della strada già disciplina il comportamento degli animali, l'intelligenza artificiale potrebbe essere interpretata giuridicamente assimilandola agli animali stessi, evitando così la necessità di modifiche normative sostanziali ma piuttosto richiedendo un'interpretazione aggiornata delle leggi in linea con l'evoluzione tecnologica.

Attualmente, la classificazione gerarchica dei livelli di automazione, elaborata dalla *Society of automotive engineers* (SAE), varia dal livello 0, privo di automazione, al livello 5, rappresentante una completa autonomia che non richiede alcun intervento umano. Questa classifica è predisposta a seconda dell'incrementale coinvolgimento dell'automazione nelle varie fasi del processo di guida, fondato principalmente sulla cooperazione di sensori quali telecamere, lidar, radar e sensori ad ultrasuoni, deputati alla raccolta di dati ambientali (SEA 2024). Tuttavia, solo i livelli dal tre fino al cinque supportano la guida autonoma: il livello tre indica l'automazione condizionale, il livello quattro indica un'automazione avanzata ed il livello cinque indica l'automazione completa. Detti livelli, inoltre, variano anche a seconda della presenza di algoritmi decisionali che operano sulla base dei dati raccolti durante la guida al fine di assumere decisioni informate in merito alla guida autonoma stessa e che tengono conto di vari aspetti quali l'accelerazione, il cambio di corsia e le manovre di sorpasso. Il controllo del veicolo è, poi, delegato a sistemi che utilizzano gli *output* degli algoritmi decisionali per impartire comandi specifici al sistema di sterzata, all'acceleratore e ai freni, dando così attuazione alle decisioni autonome adottate dall'intelligenza artificiale.

Gli algoritmi incorporati nei veicoli autonomi, inoltre, svolgono ruoli di fondamentale importanza, inclusa la percezione dell'ambiente esterno, at-

traverso l'uso di sensori come lidar, radar e telecamere, supportati da algoritmi di visione artificiale come le reti neurali convoluzionali (CNN), che sono in grado di identificare e categorizzare oggetti e riconoscere schemi visivi complessi.

In conformità con la classificazione SEA, anche nel quinto livello di automazione il conducente dovrebbe mantenere la massima diligenza nella custodia del veicolo, come prescritto dall'articolo 2051 del codice civile, che regola la responsabilità del custode per i danni causati dalle cose sotto la sua custodia, di conseguenza, non sarebbe necessaria alcuna modifica legislativa sostanziale, poiché le disposizioni esistenti sono sufficienti a regolare la responsabilità legale. Per i livelli di automazione inferiori al quinto, poi, potrebbe essere applicata la responsabilità prevista dall'articolo 2051 combinata con l'articolo 2054 del codice civile, che disciplina le responsabilità del conducente in caso di danni derivanti dalla circolazione del veicolo: mentre l'articolo 2051 enfatizza il principio della massima diligenza del custode nella custodia della cosa, l'articolo 2054 stabilisce la responsabilità oggettiva del conducente per i danni causati durante la circolazione del veicolo, salvo prova contraria di forza maggiore o condotta colposa della vittima (Russo 2023).

Tuttavia, la questione si complica in presenza di un controllo della guida automatica via etere (livelli 4 e 5) e, per queste ipotesi, ci si chiede se la responsabilità da custodia debba estendersi ad altri soggetti, come ad esempio, nel caso di utilizzo di un servizio cloud in cui gli algoritmi di guida automatica sono inseriti, potrebbe essere ritenuto responsabile il gestore del servizio informatico, oltre al guidatore fisicamente presente che potrebbe governare l'autovettura.

La risposta a questa domanda potrebbe variare a seconda del livello di automazione della guida: se il guidatore può intervenire e assumere il controllo del veicolo, potrebbe sussistere un proprio concorso di colpa nel caso in cui non agisca prontamente con la diligenza richiesta; se, però, non vi sono margini di intervento, il concorso di colpa del conducente dovrebbe essere escluso. Infatti, in presenza di un servizio cloud per l'elaborazione e l'invio di dati relativi alla guida automatica, il gestore del servizio informatico potrebbe essere ritenuto esclusivamente responsabile (o in concorso col produttore) per eventuali difetti o malfunzionamenti nel sistema, compresi errori nell'elaborazione dei dati, problemi di sicurezza informatica o malfunzionamenti dei server che influenzano le prestazioni della guida automatica. Parimenti il gestore del cloud potrebbe essere considerato responsabile nel caso in cui un incidente o un danno sia causato da un difetto nel software di guida, comprendente errori nel codice, problemi di progettazione o mancanza di aggiornamenti di sicurezza (Kaiser 2019).

Ad ogni modo, attualmente, con la rete infrastrutturale tecnologica (in) esistente in Italia, l'immatricolazione e la vendita di veicoli aventi un livello

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

superiore al 3 è, pressoché, impensabile e, come se non bastasse, l'adeguamento delle leggi in questo settore è ancora in fase di sviluppo.

Orbene, è pacifico che la questione della responsabilità può variare notevolmente in base al livello di automazione presente nel veicolo: in un veicolo a guida autonoma di livello 5, dove non è richiesto l'intervento umano ed il pilota automatico può operare in modo completamente autonomo, la responsabilità potrebbe gravare principalmente sul produttore e ciò perché, in questo contesto di automazione completa, la responsabilità per il corretto funzionamento e la sicurezza del veicolo ricade, verosimilmente, sulle decisioni di progettazione e implementazione fatte dal produttore. C'è da precisare che, ad oggi, un veicolo di livello cinque di automazione non è ancora stato immesso in commercio a livello globale. Al contrario, nei veicoli di livello inferiore al quinto, in cui il conducente assume il ruolo di supervisore e deve essere sempre pronto a intervenire, la responsabilità, ragionevolmente, concorre tra il conducente e il produttore del veicolo autonomo, perché in questo scenario, il conducente deve assumere sempre una condotta attiva alla guida ed ha il compito di monitorare attentamente il sistema di guida autonoma e di intervenire se necessario.

Con l'avvento dei veicoli a guida totalmente autonoma, che eliminerebbero i profili di pericolosità associati alla presenza del conducente, si potrebbe configurare un nuovo sistema di responsabilità civile, il cui scopo principale sarebbe quello di tutelare terzi ed occupanti dell'autoveicolo. Immaginando tale scenario, caratterizzato, sostanzialmente, da una "responsabilità dell'auto" chiamata a rispondere per i danni causati a terzi e agli occupanti, illustri studiosi hanno ideato un innovativo sistema di responsabilità civile in cui il danneggiato verrebbe risarcito automaticamente. In questa prospettiva, un ruolo dinamico è assunto dal produttore che, a monte e durante le scelte di politica aziendale che compie, deve pensare di socializzare i costi dei nuovi incidenti derivanti dall'automazione della circolazione stradale. Secondo questa teoria, infatti, si propone l'introduzione di un sistema aziendale denominato *Market enterprise responsibility* che presuppone l'istituzione di un fondo finanziato dai produttori stessi e finalizzato a creare risorse per fronteggiare i danni eventualmente causati (Calabresi 2020).

Secondo tale principio, le imprese devono operare in modo responsabile e, soprattutto, etico all'interno del mercato, considerando non solo il perseguimento del profitto, ma anche l'impatto delle proprie azioni sugli altri soggetti del mercato e sulla società nel suo complesso.

Questo approccio dovrebbe, appunto, fondarsi sulla responsabilità del produttore, il quale è tenuto a garantire un adeguato risarcimento sia ai terzi danneggiati sia agli occupanti del veicolo.

Sempre secondo questa teoria, in un contesto in cui il numero di incidenti stradali sarebbe notevolmente ridotto grazie all'implementazione dei veicoli completamente automatizzati, potrebbe essere ipotizzata, sulla scia

degli ordinamenti del Common law, l'ammissibilità di un'eccezionale forma di responsabilità civile punitiva; detta forma di responsabilità costituirebbe uno strumento utile e di condanna contro condotte particolarmente gravi e censurabili da parte del produttore dei veicoli smart (Calabresi 2021).

Con riferimento alla relativa responsabilità, le norme attualmente in vigore stabiliscono l'obbligo del conducente del veicolo di dover sempre prendere il controllo dell'autovettura, indipendentemente dal grado di automatizzazione raggiunto. In altre parole, in questo scenario, l'Intelligenza Artificiale non sostituisce completamente il guidatore, piuttosto, quest'ultimo ha non solo la possibilità ma anche l'obbligo di riprendere il controllo del veicolo quando richiesto dal sistema ed ogni volta che lo ritenga necessario.

Questo assunto si traduce in una ipotesi di responsabilità oggettiva del conducente, soprattutto nei casi di incidenti che causino danni a terzi. Tuttavia, è importante sottolineare che questa responsabilità si può configurare solo in situazioni in cui l'incidente non sia causato da un malfunzionamento tecnico del sistema del veicolo, in tal caso sia il conducente che il proprietario sarebbero esonerati dalla responsabilità.

Il Decreto smart road, come precisato, ha recepito la riforma del 2014 della Convenzione di Vienna e ha introdotto il comma 5 bis all'articolo 8, regolamentando le modalità e gli strumenti per la sperimentazione su strada della guida connessa e automatica. Questo decreto ha anche elaborato la figura del supervisore, obbligato ad intervenire sul sistema automatico in caso di necessità.

Tuttavia, l'articolo 34 bis della Convenzione di Vienna, introdotto lo scorso anno e relativo alla guida autonoma, non è ancora stato recepito dall'Italia né nel decreto infrastruttura 68/2022 né nella sua legge di conversione n. 108 del 5 agosto 2022. Questo articolo autorizza la circolazione dei veicoli autonomi senza richiedere la presenza di un conducente nell'abitacolo del veicolo.

Nel nostro ordinamento, l'esclusione della circolazione dei veicoli di livello 3 o superiore dalle strade nazionali può essere collegata all'articolo 46 del codice della strada, il quale definisce i veicoli come "tutte le macchine di qualsiasi specie, che circolano sulle strade, guidate dall'uomo". Finché non verrà apportata una modifica al codice della strada, sarà impensabile vedere circolare veicoli con guida automatica superiore al secondo livello in Italia.

Questa restrizione indica che, per il momento, la questione della responsabilità legale per incidenti causati da veicoli automatizzati non è un tema rilevante nel contesto legislativo italiano poiché, sarebbe prima necessaria la modifica al codice della strada per poter iniziare a discutere di responsabilità.

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

4.3. La responsabilità del produttore

Volendo tracciare un punto in comune a tutte le teorie analizzate in materia di responsabilità civile derivante dall'uso dell'intelligenza artificiale nel veicolo avente un livello di automazione superiore al terzo, si può sostenere che tutte, tra le alternative prospettate, ritengono che il produttore debba essere considerato soggetto attivo e potenzialmente responsabile in caso di danni a terzi.

Innanzitutto, in questo specifico settore è sempre opportuno richiamare le disposizioni del Codice civile e, nello specifico, l'articolo 2054 c.c., il che delinea la responsabilità del conducente del veicolo e del suo proprietario; prima dell'entrata in vigore del codice del consumo, la responsabilità del produttore trovava la sua fonte nell'articolo 2043 c.c. che recita "qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno".

Attualmente, poi, in virtù delle modifiche introdotte dal Codice del Consumo, il produttore del veicolo è tenuto a rispondere dei danni arrecati all'utilizzatore dello stesso secondo quanto stabilito dagli articoli 114 e successivi del Codice del Consumo. Secondo tale disposizione normativa, il produttore deve rispettare, una serie ulteriore di regole che riguardano la fase di progettazione, quella di fabbricazione e quella di informazione e

> per ogni fase sono sancite norme diverse, rispettivamente, in ambito d'ideazione del prodotto, di costruzione dello stesso e di informazione necessaria che deve essere fornita al consumatore per un corretto utilizzo del prodotto. Il mancato rispetto di tali norme comporta l'obbligo, in capo a una o più figure di produttore, di risarcire i danni subiti a causa di un prodotto difettoso; prodotto che, nei casi di cui ci occupiamo, sarà un dispositivo automatico ovvero il computer di bordo (Gaeta 2016, p. 18).

Nel contesto normativo attuale, la responsabilità del produttore nei veicoli dotati di intelligenza artificiale può manifestarsi in diverse forme: potrebbe essere chiamato a rispondere per difetti nel design o nella produzione che causino danni o incidenti; potrebbe essere considerato responsabile se non fornisce informazioni sufficienti sul funzionamento dell'IA presente sui veicoli, inclusa l'omissione di avvisi sui limiti dei sistemi informatici. Questo aspetto è stato recentemente sottolineato dalla Corte di Giustizia dell'Unione Europea in una sentenza del 9 novembre 2023. Inoltre, potrebbe essere considerato responsabile se non fornisce aggiornamenti adeguati o se un aggiornamento introduce difetti dannosi. Allo stesso modo, deve garantire la sicurezza e la privacy dei dati sensibili degli utenti. Infine, nei veicoli autonomi di livello cinque, potrebbe essere considerato responsabile per incidenti, anche in presenza di un supervisore.

In un'ottica di eccessiva responsabilizzazione, la dottrina ha elaborato quattro istituti per limitare la responsabilità del produttore nascenti dall'uso dell'AI nei veicoli. Il primo riguarda la negligenza comparativa, dove il produttore potrebbe non essere considerato responsabile se dimostra che la negligenza del conducente ha contribuito al sinistro. In secondo luogo, vi è l'uso improprio, dove il produttore può sostenere che il conducente non ha utilizzato correttamente il sistema informatico del veicolo, non rispettando la sua destinazione d'uso. Un terzo istituto è lo stato dell'arte e l'assunzione del rischio, dove il produttore può invocare il progresso tecnologico non conosciuto al momento della commercializzazione del veicolo. Infine, i limiti tecnologici possono esonerare il produttore dalla responsabilità se il malfunzionamento è causato da limiti intrinseci che non potevano essere previsti o superati al momento della produzione (Gaeta 2016).

In generale, come precisato e, in particolare, secondo il D. Lgs. n. 206 del 2005[5], il produttore di un bene è responsabile in caso di prodotto difettoso e, nel caso di un'autovettura occorre, dapprima, capire cosa si intende, appunto, per prodotto difettoso. Una teoria, troppo de-responsabilizzante, sostiene che, una volta ottenuta l'omologazione alla costruzione, dunque una volta seguiti gli standard minimi di produzione, il prodotto non può ritenersi difettoso, ed in conseguenza verrebbe meno la responsabilità della casa automobilistica.

Infatti, e soprattutto in relazione ai veicoli smart, questa tesi deve essere scartata anche solo analizzando la ratio sottesa all'emanazione dei Regolamenti UNECE, che impongono al costruttore di monitorare, per tutta la vita di un veicolo, i rischi di una intrusione malevola nel sistema informatico e di cercare di limitarli; questo perché l'esposizione del veicolo ad un potenziale rischio di intrusione malevola nel sistema informativo rende il veicolo non sicuro e, quindi, difettoso.

In questo scenario occorre anche domandarsi se, essendo ancora elevati e poco controllabili i rischi di *hackeraggio*, si debbano far rientrare le attività derivanti dall'uso di auto automatiche nell'art. 2050 c.c., secondo cui "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" e se, in caso di risposta affermativa, responsabili ai sensi dell'art. 2050 c.c. debbano considerarsi solo i produttori del veicolo o anche gli stessi conducenti. In tal caso, si obietta che, in base ad un'analisi economica del diritto, la riconducibilità a questa responsabilità semi-oggettiva della condotta del costruttore disincentiverebbe fortemente, la produzione delle auto auto-

5 L'art. 111 del Codice del consumo recita: "Sono fatte salve le disposizioni di cui al titolo secondo in materia di responsabilità per danno da prodotti difettosi", mentre l'art. 114: "Il produttore è responsabile del danno cagionato da difetti del suo prodotto" (DLGS 2005).

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

matizzate la cui diffusione, invece, sarebbe maggiormente sostenuta dalle Istituzioni perché esse sono considerate, sostanzialmente, più sicure.

In quest'ottica di idee ed in considerazione della circostanza in base alla quale la commercializzazione dei veicoli automatici ha l'obiettivo di ridurre drasticamente i sinistri stradali, si ravvisa l'opportunità di promuovere l'incentivazione della loro commercializzazione mediante l'emanazione di disposizioni legislative che limitino i costi e le responsabilità in capo ai produttori, al fine, proprio, di incentivare gli investimenti per l'introduzione sul mercato di questa tipologia di prodotti (Brancaccio 2020). Per tale ragione, emerge la necessità di istituire adeguati meccanismi di compensazione economica a favore di coloro che potrebbero subire danni derivanti dai rischi connessi a tali veicoli, la cui portata non può essere completamente definita durante una fase sperimentale e che si prospetta prolungata per un significativo periodo di tempo:

> proprio in ragione di queste considerazioni, sembrano da osservare con favore le letture interpretative che, in una prospettiva de iure condendo, suggeriscono l'adozione di un approccio caratterizzato da una particolare cautela e lumeggiano l'introduzione di strumenti idonei a evitare che i costi dei futuri incidenti, ancorché cagionati da veicoli conformi agli standard legislativi, possano ricadere sui danneggiati ai quali, invece, appare ragionevole garantire la piena compensazione dei pregiudizi subiti, talvolta attraverso lo strumento della responsabilità civile, talvolta ricorrendo a quello dell'indennizzo e infine mediante l'operare sinergico dei due diversi strumenti indicati (Calabresi 2021, p. 160).

Questo autorevole filone dottrinale ha sostenuto che le regole di responsabilità, sapientemente combinate e supportate da efficienti meccanismi assicurativi, dovrebbero mirare a minimizzare i costi sociali degli incidenti e, cioè, il costo dei sinistri, ma anche quello per evitare i sinistri stessi. Secondo questa tesi, l'obiettivo principale del legislatore deve essere la riduzione del costo degli incidenti per la società nel suo complesso e, per raggiungerlo, la soluzione preferita sembra essere quella di far ricadere il danno su chi può sopportarlo, il produttore assicurato, riducendo così l'impatto sociale complessivo e individuando il punto di equilibrio più efficiente tra i costi di prevenzione e i costi derivanti dagli incidenti. Inoltre, la soluzione cui giunge questa parte di dottrina è quella di prevedere una revisione del concetto di colpa nell'ambito della responsabilità delle imprese: innanzitutto bisogna minimizzare il rischio che i prodotti aziendali possano arrecare danni a terzi e per fare ciò bisognerebbe ottimizzare le pratiche preventive degli operatori economici, che sono incentivati dalla prospettiva di una responsabilità oggettiva. In secondo luogo, deve essere distribuito in modo efficiente il residuo costo sociale rappresentato dal rischio residuo di incidenti, nonostante le predette misure preventive. Infine, devono essere previsti degli incentivi

per le imprese più responsabili e sicure, al fine di escludere dal mercato quelle che comportano un rischio eccessivo rispetto al beneficio sociale che producono (Di Ciommo 2017).

Un'altra soluzione potrebbe essere quella di adottare una normativa simile all'*Automated and electric vehicle Act* pubblicato nel 2018 in Gran Bretagna e che impone ai produttori dei veicoli automatici di stipulare una polizza assicurativa e che prevede espressamente una responsabilità generale del produttore del veicolo autonomo in caso di sinistro stradale ed una eventuale e concorrente responsabilità del proprietario nel caso del mancato aggiornamento del software ovvero dell'alterazione dello stesso:

> il software iniziale ritrae mappe e luoghi e, più in generale, situazioni che possono divenire presto obsolete e, dunque, essere cagione di danno. Al fine di evitare ciò, il dovere di adeguamento dovrebbe non tanto evitare domande risarcitorie di danni nei confronti del produttore, quanto piuttosto di consentire allo stesso di sollevare eccezioni, finanche scriminanti, le objections, ad usare la terminologia inglese, nell'ambito dei relativi giudizi risarcitori. Peraltro, la norma suggerisce che, dato l'obbligo per il proprietario di aggiornare il software, un migliore sistema di tutela per il produttore potrebbe essere quello di avere un registro delle macchine automatizzate, presso cui vengano iscritti i diversi proprietari che si susseguono nella titolarità del veicolo. Ciò consentirebbe anche di evitare che il produttore debba fronteggiare domande di natura speculativa, in casi di incertezza generale relativa alla titolarità dei beni, a fronte delle quali il produttore potrebbe sopportare costi, in realtà non giustificati (Della Giustina 2023, p. 8).

In definitiva, accettare senza riserve un sistema di responsabilità del produttore per un incidente causato da difetto di costruzione del veicolo comporterebbe la sua esposizione ad una vasta gamma di tipi di danni che vanno oltre il semplice sinistro e proprio questa previsione contrasta con il principio di prevedibilità dei costi di risarcimento, che costituisce un corollario del già menzionato *Market enterprise responsibility*.

Si confida, dunque, che, oltre a definire chiaramente il soggetto responsabile in caso sia di incidenti *cyber* sia di sinistri stradali con automobili automatiche, il legislatore delinei anche una nuova forma di copertura assicurativa obbligatoria in questo ambito.

4.4. Conclusione

Nel breve periodo, l'applicazione dell'intelligenza artificiale nel settore automobilistico comporterà un aumento dei costi, soprattutto nel settore *after-sales*, a causa dei nuovi obblighi finalizzati a garantire la sicurezza e la privacy dei dati.

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

L'Unione Europea, preoccupata per l'impatto dell'IA sui diritti fondamentali, ha istituito l'Agenzia europea dei diritti fondamentali, che ha precisato che, al momento, non ci sono prove empiriche sufficienti per garantire che l'IA sia conforme ai diritti fondamentali, essendo necessario raccogliere prove sull'impatto dell'IA sui diritti fondamentali ed assicurarsi che le restrizioni rispettino i principi di necessità e proporzionalità.

Per quanto riguarda la responsabilità civile derivante da incidenti stradali causati dall'IA, gli attuali articoli del codice della strada, concepiti per il conducente umano, dovranno essere interpretati o modificati per regolare l'operatività dei veicoli autonomi; potrebbe essere opportuno istituire un regime di assicurazione obbligatoria integrato da un fondo per garantire il risarcimento dei danni in caso di mancanza di copertura assicurativa e detto fondo potrebbe essere finanziato dalle compagnie assicurative e garantirebbe un risarcimento per le vittime di incidenti stradali causati da anomalie nell'IA dei veicoli o dalla difficoltà nell'attribuire la responsabilità (Scagliarini 2019).

5. L'informatizzazione totale vale tanto da compromettere i diritti fondamentali

La rapida diffusione dell'intelligenza artificiale richiede una riflessione ponderata sulla tutela dei diritti fondamentali. Oltre alla privacy, bisogna considerare l'obbligo di non discriminazione, affinché gli algoritmi non perpetuino *bias* ingiusti; la trasparenza nei processi decisionali degli algoritmi è fondamentale, così come garantire la sicurezza, specialmente in settori vitali. Infine, è fondamentale proteggere la dignità umana, soprattutto nelle applicazioni come la sorveglianza di massa o l'automazione del lavoro.

La consapevolezza e l'alfabetizzazione digitale diventano, inoltre, fari illuminanti nel percorso verso una comprensione approfondita e partecipata del dibattito sull'intelligenza artificiale e le sue influenze sulla società:

> ciò che può essere valutato nei prossimi anni è se il progresso tecnologico valga tanto da limitare i diritti fondamentali delle persone e soprattutto se, almeno in questo settore, sia necessario comunque non eliminare l'intervento umano giacché innumerevoli sono le circostanze imprevedibili e nuove che possono presentarsi durante la guida di un veicolo e che un soggetto pensante – utilizzando la diligenza richiesta – potrebbe risolvere più tempestivamente e meglio di una macchina intelligente. Infatti, c'è un punto essenziale da tenere in considerazione: per quanto la macchina intelligente sia capace di autocorreggersi, pur sempre si basa su informazioni che riguardano il passato (Ferrari 2022, p. 12).

Nell'odierno contesto giuridico-sociale emerge una doppia sfida: ottimizzare la completa digitalizzazione della vita quotidiana, che cerca di governare variabili complesse tramite algoritmi e limitare l'erosione della privacy.

La Commissione europea, ad esempio, nel 2018, ha istituito un Gruppo di esperti di intelligenza artificiale, il quale ha elaborato un dossier intitolato "Orientamenti etici per una IA affidabile". Questo documento fornisce linee guida per garantire un utilizzo etico e responsabile dell'intelligenza artificiale e cerca di bilanciare i vantaggi e le criticità legate alla crescente connettività e digitalizzazione nel settore automobilistico e in altri settori. In questo documento si legge:

> L'obiettivo degli orientamenti è promuovere un'IA affidabile. Un'IA affidabile si basa su tre componenti che dovrebbero essere presenti durante l'intero ciclo di vita del sistema: a) legalità, l'IA deve ottemperare a tutte le leggi e ai regolamenti applicabili, b) eticità, l'IA deve assicurare l'adesione a principi e valori etici, e c) robustezza, dal punto di vista tecnico e sociale poiché, anche con le migliori intenzioni, i sistemi di IA possono causare danni non intenzionali. Ciascuna componente in sé è necessaria ma non sufficiente per realizzare un'IA affidabile. Idealmente le tre componenti operano armonicamente e si sovrappongono; qualora, nella pratica, si dovessero verificare tensioni tra di esse la società dovrebbe adoperarsi per risolverle (Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale 2019, p. 5).

Tra i principi etici delineati dal Gruppo di esperti, il rispetto dell'autonomia umana è al centro delle considerazioni mentre, viene identificata quale criticità principale la potenziale supremazia delle macchine sull'essere umano, tale da ingenerare una dipendenza da esse. Questa minaccia però non risiede tanto in scenari apocalittici di ribellione delle macchine contro l'umanità, come spesso rappresentato nei film di fantascienza, ma piuttosto nel pericolo più sottile di adattare le nostre preferenze in modo che diventino sempre più elementari da soddisfare nel tempo, attraverso algoritmi di intelligenza artificiale. Stuart Russell, professore dell'Università di Stanford, ha proprio rappresentato questo possibile problema durante le sue lezioni del 2021 intitolate "The reith lectures", evidenziando che la crescente dipendenza dall'intelligenza artificiale può spingere le persone a comportarsi come individui deboli e infantili, simili a quelli del film "WALL-E"[6]. La

6 Il regista Andrew Stanton ha rappresentato la storia di Wall-E, un robot rimasto unico abitante sulla terra, ormai inabitata perché eccessivamente inquinata e piena di rifiuti. "Due analisi, quella sociale e quella ecologica sono fortemente correlate e soggiacciono alla trama del film. L'intera storia è disseminata di feroci critiche alla burocrazia. Le decisioni più importanti, infatti, vengono prese in stanze segrete, mentre il resto della popolazione viene tenuta all'oscuro. Il burocrate supremo, addetto a far rispettare lo status quo, è Auto; si tratta di un'intelligenza artificiale, liberamente ispirata a HAL di 2001: Odissea nello spazio di Stanley Kubrick. Gli umani, però, appaiono come vittime non tanto della burocrazia, quanto

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

preoccupazione, dunque, è che, affidando gradualmente la gestione della civiltà alle macchine, si possa perdere la capacità di compiere azioni autonomamente, con la generazione successiva che potrebbe perdere l'incentivo ad "imparare a fare", creando così una dipendenza e una rottura nella catena delle competenze umane:

> la nostra dipendenza crescente dall'IA ci spinge a comportarci come individui deboli e infantili, simili a quelli del film WALL-E; quando affideremo gradualmente la gestione della nostra civiltà alle macchine, perderemo la capacità di farlo noi stessi, e la generazione successiva perderà l'incentivo a imparare a farlo, e la catena si spezzerà (Russell 2021, p. 10).

Questa prospettiva etica pone un'enfasi fondamentale sull'assicurare che l'intelligenza artificiale si conformi alle necessità umane anziché il contrario. Affrontare queste sfide richiede un approccio etico e responsabile nello sviluppo e nell'utilizzo dell'intelligenza artificiale, con particolare attenzione ai principi di autonomia umana e controllo. Negli anni a venire, il compito degli studiosi sarà orientato alla difesa di coloro che desiderano preservare il proprio diritto alla riservatezza, inteso come il diritto di mantenere segreti aspetti, comportamenti e atti relativi alla sfera intima della persona. Questa esigenza di riservatezza è intrinseca all'essere umano, come dimostra il fatto che la necessità di tutelare questo diritto è emersa negli Stati Uniti già nel 1890 con la pubblicazione del saggio intitolato "The Right to Privacy" ("Il diritto alla privacy") di Warren e Brandeis (1890). Questo saggio, pubblicato sulla rivista Harvard Law Review, analizza il diritto fondamentale "ad essere lasciati soli". Gli autori proclamano con enfasi l'esistenza di un diritto alla privacy, sottolineando la sua necessità di essere riconosciuto e protetto. Warren e Brandeis hanno analizzato le sempre più frequenti intrusioni nella sfera privata delle persone, attribuendole all'evoluzione tecnologica e alla diffusione della stampa. Essi sostengono che la legge dovrebbe riconoscere e difendere il diritto delle persone di essere lasciate sole e di non essere sottoposte a un'attenzione pubblica non necessaria.

L'articolo di Warren e Brandeis è diventato un punto di riferimento nello sviluppo del concetto di privacy nella giurisprudenza statunitense, contribuendo in modo significativo a plasmare l'interpretazione legale della privacy nell'ambito della moderna società tecnologica.

---

della loro stessa pigrizia, la quale non permette loro di guardare oltre il proprio display e di aprire gli occhi sulla propria situazione" recensione consultabile sul seguente sito internet: https://www.theserendipityperiodical.it/2022/04/15/wall-e-analisi-e-recensione-del-film/.

6. Conclusioni

Per sottolineare l'importanza del diritto all'autonomia umana, si riportano le parole pronunciate dal Professor Russell al termine di quattro giorni di conferenze trasmesse dalla BBC nell'ambito delle c.d. "The reith lectures[7]":

> l'autonomia è un valore umano fondamentale, il che significa che i sistemi di IA benefici non potranno garantire il miglior futuro possibile se garantire ciò comporta una perdita di autonomia per gli esseri umani. È possibile che le macchine debbano astenersi dall'usare i loro poteri per prevedere come ci comporteremo, affinché possiamo mantenere l'illusione necessaria del libero arbitrio. Qualunque sia la soluzione a questo rompicapo auto-referenziale, i nostri sistemi di IA devono e impareranno a fare un passo indietro, come fanno i genitori, alla fine dicendo: no, oggi non ti lego i lacci delle scarpe. Devi farlo da solo. Non creeranno il mondo di WALL-E a meno che non li costringiamo a farlo. Ma la relazione genitore-figlio non è la metafora giusta, perché noi (i bambini) avremo tutto il potere, anche se le macchine saranno di fatto molto più potenti. Abbiamo bisogno di una nuova metafora, di un nuovo modo di vederci, e avremo bisogno di tutti gli scrittori, i cineasti e i poeti per guidare la nostra cultura in questo processo (Russell 2021, p. 11).

A livello europeo, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) rappresenta il principale trattato per la protezione dei diritti umani nei paesi europei. Articoli chiave come il diritto alla vita (articolo 2), il divieto di trattamenti inumani o degradanti (articolo 3), il diritto a un processo equo (articolo 6) e il diritto al rispetto della vita privata e familiare (articolo 8) hanno implicazioni importanti per l'autonomia umana, anche in contesti legati all'intelligenza artificiale. La CEDU costituisce un quadro normativo vincolante per gli Stati membri e viene considerata fondamentale nell'affrontare le sfide etiche e giuridiche poste dall'uso dell'intelligenza artificiale, garantendo il rispetto dei diritti umani.

L'intelligenza artificiale è un campo interdisciplinare che unisce principi della teoria dell'informazione, della statistica, dell'ottimizzazione e dell'informatica; si può definire come la ricerca e l'applicazione di strumenti tecnici per risolvere problemi pratici, ottimizzare procedure, prendere decisioni e perseguire obiettivi specifici (Treccani). Questa definizione include le conoscenze matematiche, informatiche e scientifiche utilizzate per sviluppare soluzioni che emulano il pensiero e il comportamento umani. In ultima anali-

7 Ogni anno, dal 1948 la BBC invita un'illustre personalità a tenere un ciclo di conferenze radiofoniche, oggi chiamate *podcast*, su determinati argomenti. Le Reith Lectures sono state inaugurate nel 1948 dal matematico Bertrand Russel che, durante il ciclo di lezioni intitolato "Authority and the Individual", il 9 gennaio 1949 ha tenuto una lezione ad oggetto "The role of individuality".

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

si, l'intelligenza artificiale si basa sull'asservimento nei confronti dell'uomo, poiché mira a creare sistemi in grado di assistere o migliorare le capacità umane. L'asservimento dell'intelligenza artificiale nei confronti dell'uomo riflette la necessità di rimarcare (e di non dimenticare mai) la supremazia umana nel dirigere e regolare il ciclo di vita dell'intelligenza artificiale stessa, garantendone il corretto utilizzo nel rispetto di limiti etici, legali e sociali.

Da questo concetto si desume prima di tutto che deve essere posta un'enfasi particolare sulla responsabilità umana nel processo di progettazione e implementazione degli algoritmi e dei modelli di intelligenza artificiale. Gli esseri umani devono assumersi la responsabilità di guidare e supervisionare l'intero processo, definendo obiettivi specifici e stabilendo parametri etici che influenzino il comportamento dei sistemi tecnologici. In secondo luogo, si evidenzia l'importanza di stabilire limiti e controlli per garantire che l'intelligenza artificiale operi entro confini ben definiti e in conformità con principi etici e normativi predefiniti e ciò implica che i sistemi di intelligenza artificiale devono essere progettati e implementati in modo da rispettare standard etici e normativi, con eventuali restrizioni alle loro capacità decisionali autonome, se necessario. Poi, deve essere chiesto agli sviluppatori dell'intelligenza artificiale ed ai suoi utilizzatori di assicurarsi che dette tecnologie rispettino i principi etici fondamentali di uno Stato di diritto, come la giustizia, la trasparenza e il divieto di discriminazione. Ciò implica che le tecnologie vengano progettate ed utilizzate in modo da garantire un trattamento equo e trasparente per tutte le persone coinvolte (Cristianini 2023).

È anche essenziale, si ripete, attribuire chiaramente la responsabilità per le azioni degli algoritmi di intelligenza artificiale ed avere la capacità di tracciare e tutte le decisioni assunte da tali sistemi. Questo permette sia di valutare le eventuali conseguenze negative, sia di attribuire responsabilità in caso di errori o danni causati dagli algoritmi. Infine, si rimarca ancora una volta l'importanza dell'addestramento continuo e del monitoraggio dei sistemi informatici per assicurare che essi rimangano allineati agli obiettivi prefissati e per correggere eventuali deviazioni o rischi nel loro funzionamento: ciò significa che i sistemi di intelligenza artificiale devono essere costantemente valutati e aggiornati per garantire che siano in grado di raggiungere i risultati desiderati in modo etico e responsabile. Nell'ambito di tale prospettiva, l'intelligenza artificiale deve essere concepita come un mezzo destinato a servire l'uomo che, attraverso questa tecnologia, ottimizza le proprie capacità, supera ulteriormente i propri limiti e mitiga i rischi associati alle sue operazioni. Indubbiamente, l'intelligenza artificiale non dovrebbe essere concepita con l'obiettivo di sostituire l'uomo, piuttosto dovrebbe essere vista come una risorsa complementare all'abilità umana, in grado di affrontare compiti specifici in modo efficiente ed accurato.

È, poi, quasi obbligatorio riconoscere che anche l'intelligenza artificiale presenta dei limiti intrinseci: pur avanzando rapidamente nelle sue capaci-

tà, rimane vincolata dalle sue programmazioni e dalle informazioni di cui dispone; non può sempre replicare la complessità del pensiero umano né comprendere appieno il contesto emotivo, sociale e culturale in cui opera. In questo senso, è anche importante adottare un approccio bilanciato nell'utilizzo dell'intelligenza artificiale, considerandola come uno strumento potente ma non omnicomprensivo. Difatti, questo strumento dovrebbe essere integrato nella quotidianità umana con consapevolezza dei suoi limiti e delle sue potenzialità, al fine di massimizzare i benefici e mitigare eventuali rischi o sfide che potrebbero sorgere. Analizzando proprio i limiti dell'intelligenza artificiale, da un'analisi condotta da Giovanni Sartor, emblematico è il confronto eseguito con il linguaggio umano:

> nella comunicazione umana il linguaggio non si limita a combinare parole, esso fa riferimento al mondo fisico e sociale. Per capire pienamente cosa significhi un enunciato non basta collegare tra loro le parole che lo compongono […] Bisogna invece collegare le parole alle cose cui si riferiscono, e gli enunciati alle situazioni che descrivono, costituiscono o prescrivono, nel contesto in cui quelle parole vengono usate (Sartor 2022, p. 22-23).

Nel processo comunicativo umano, il linguaggio non si limita a una mera combinazione di parole; esso è intrinsecamente legato al mondo fisico e sociale. Difatti, per ottenere una comprensione completa di un'affermazione, non è sufficiente solamente collegare tra loro le parole che la compongono, è, invece, essenziale stabilire connessioni tra le parole e gli oggetti a cui fanno riferimento, così come tra le dichiarazioni e le situazioni che descrivono, delineano o prescrivono, all'interno del contesto in cui tali parole vengono impiegate. Le attuali intelligenze artificiali apprendono attraverso il metodo dell'imitazione, eseguono operazioni e conducono dialoghi utilizzando algoritmi. A tal proposito è importante sottolineare che questi oggetti non possiedono una comprensione intrinseca del significato o del senso delle loro azioni. In altre parole, mentre possono emulare comportamenti e compiere azioni basate su algoritmi, manca loro la capacità di intraprendere un'apprensione concettuale del linguaggio.

Un'ulteriore limitazione dell'intelligenza artificiale è la sua propensione a diventare obsoleta ed a questo processo naturale si aggiunge, molto spesso, un meccanismo economico che incorpora l'obsolescenza programmata come uno dei metodi per stimolare l'attività del mercato, sia dal punto di vista produttivo che gestionale.

In questo contesto si inserisce l'automobile che, oltre alla sua funzione intrinseca di facilitare il movimento di persone e merci, ha assunto una connotazione di *status symbol*, influenzando l'identità sociale e l'assimilazione a una determinata età o contesto sociale. È paradossale notare che, nonostante l'automobile sia spesso considerata un simbolo di libertà e autonomia per la

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

sua capacità di esplorare nuovi luoghi, il progresso tecnologico ha portato a una situazione in cui essa può effettivamente limitare questa libertà individuale. Un'altra questione etica nel settore delle automobili a guida autonoma riguarda la pianificazione anticipata delle decisioni che tradizionalmente derivano da reazioni istintive, individuali e non soggette a valutazione legislativa in caso di ostacoli improvvisi lungo il percorso. La necessità che le scelte relative a situazioni critiche siano prese in anticipo, al momento della programmazione dei veicoli, costituisce la vera sfida posta dall'avvento dei veicoli automatici. In questo ambito, è interessante il risultato emerso da uno studio eseguito sull'emotività degli umani in conseguenza degli incidenti cagionati da automobili automatiche. L'analisi si fonda sul presupposto che i veicoli autonomi rappresentino un'opzione più sicura e riducano il numero degli incidenti stradali. Se da un lato i veicoli autonomi contribuiscono ad aumentare la sicurezza stradale, dall'altro sono considerati agenti morali attivi, poiché ogni azione intrapresa da essi può riallocare i livelli relativi di sicurezza tra gli utenti della strada circostanti. Durante questo studio, si è osservato che le persone tendono ad essere meno severe nei confronti degli esseri umani responsabili di un incidente rispetto alle macchine che provocano un incidente comparabile. Tuttavia, in modo sorprendente, questa dinamica si inverte quando sia l'essere umano che la macchina contribuiscono congiuntamente a un incidente. Ad esempio, quando un veicolo semiautonomo e il suo conducente umano non riescono ad evitare un pedone, le persone tendono generalmente ad attribuire maggior colpa all'essere umano per la conseguente collisione. Non è ancora chiaro il motivo per cui le persone tendano a incolpare maggiormente le macchine rispetto agli esseri umani quando queste ultime falliscono da sole, ma poi incolpano maggiormente gli esseri umani rispetto alle macchine quando falliscono insieme (Bonnefon 2023). Ebbene, il dilemma etico di un veicolo autonomo che deve decidere se privilegiare la vita dei suoi passeggeri o quella degli altri utenti della strada rappresenta un tema di notevole rilevanza, il cui impatto sulle scelte dei consumatori è significativo a tal punto da essere citato come uno dei principali fattori determinanti nell'acquisto dei veicoli automatici stessi (Gill 2021). In tale contesto, l'acquisizione delle preferenze dei consumatori non è solamente un'attività di natura commerciale, ma riveste un'importanza fondamentale poiché la promessa principale delle smart cars è quella di contribuire a ridurre il numero di vittime della strada, essendo più sicure dei conducenti umani; tuttavia, tale obiettivo non potrà essere raggiunto se i consumatori rinunceranno ad usare questa tecnologia a causa, proprio, di insoddisfazione o addirittura indignazione riguardo al modo in cui questi veicolo affrontano i dilemmi morali. Pertanto, l'acquisizione delle (eventuali) scelte morali dei consumatori potrebbe risultare un prerequisito indispensabile affinché le macchine possano incamerare decisioni morali ed essere considerate più etiche dagli individui (Bonnefon 2023). Inoltre,

non bisogna dimenticare che i veicoli autonomi non incidono soltanto sulla sicurezza dei loro passeggeri, ma distribuiscono anche il rischio a tutti gli altri utenti della strada circostanti, inclusi i pedoni. Di conseguenza, gli altri utenti della strada dovrebbero essere coinvolti nel processo decisionale riguardante le preferenze morali che guidano il comportamento del pilota automatico.

In conclusione, si ritiene sia necessaria un'attenta raccolta delle preferenze morali umane al fine di orientare il comportamento dei veicoli autonomi. Tale processo, secondo la scienza umanistica, implica la necessità di prendere decisioni riguardo ai valori da tutelare e alla loro ponderazione, soprattutto quando diversi gruppi esprimono preferenze contrastanti.

Va anche evidenziato che tale argomentazione sembra sovrastimare la complessità morale intrinseca alla responsabilità civile; le situazioni di pericolo derivanti dalla circolazione stradale, che in passato richiedevano risposte basate su valutazioni individuali soggettive, verranno trasferite in un nuovo scenario in cui tali valutazioni saranno ponderate in anticipo attraverso un'analisi dei costi e dei benefici condotta mediante metodi scientifici. L'analisi sarà condotta, verosimilmente, da comitati incaricati di valutare le implicazioni etiche, che dovranno tener conto sia della prospettiva individuale che di quella collettiva (Calabresi 2020). I rischi intrinseci legati alle attività che impattano sulla vita umana sono accentuati dalla tecnologia, soprattutto quando si tratta di intelligenza artificiale. Il Libro bianco evidenzia la rilevanza delle conseguenze degli errori, sia a livello individuale che sociale, richiamando l'attenzione sulla necessità di riconoscere e affrontare le limitazioni nell'attribuzione di capacità decisionali all'intelligenza artificiale. L'adozione di intelligenza artificiale senza un giudizio critico potrebbe minacciare una serie di diritti fondamentali, tra cui la privacy; in questo contesto si comprende l'importanza di considerazioni etiche e legali per preservare la libertà individuale.

La fiducia nell'intelligenza artificiale richiede chiarezza sui profili di responsabilità associati. Identificare i soggetti responsabili, come produttori, operatori informatici o consumatori finali, rappresenta una rivoluzione tecnologica cruciale. Inoltre, rendere le macchine ispezionabili è essenziale per instaurare la fiducia e garantire la sicurezza dell'intelligenza artificiale. La crescente consapevolezza dei rischi e delle sfide associate all'intelligenza artificiale è stata evidenziata da diversi leader nel campo tecnologico, tra cui Elon Musk. Questi individui hanno espresso preoccupazioni riguardo alla sicurezza, alla responsabilità etica e alle implicazioni socioeconomiche dell'adozione diffusa dell'intelligenza artificiale. Uno dei principali punti sollevati proprio da Musk riguarda la necessità di una cornice legislativa che guidi lo sviluppo e l'implementazione dell'intelligenza artificiale in modo responsabile e sicuro. Tale cornice dovrebbe, come sostenuto, affrontare temi come la trasparenza nei processi decisionali degli algoritmi, la responsabilità delle

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760

azioni compiute da sistemi autonomi e la gestione delle conseguenze sociali dell'automatizzazione (Benanti 2023). Inoltre, deve essere confermata l'importanza della collaborazione internazionale e dell'approccio interdisciplinare per affrontare queste sfide in modo efficace. Ciò implica coinvolgere governi, industrie, istituti accademici e organizzazioni della società civile nel processo di definizione di linee guida e normative che regolino l'uso dell'intelligenza artificiale.

Bibliografia

Bellomia, V., (2020), Il contratto intelligente: questioni di diritto civile, *Judicium. Il processo civile in Italia e in Europa*. [Online] Consultabile all'indirizzo: https://www.judicium.it/wp-content/uploads/2020/12/Valentina-Bellomia.pdf (Data di accesso: 17 marzo 2024).

Benanti, P., Maffettone, S., (1 aprile, 2023), Se l'intelligenza artificiale rischia di sfuggirci di mano. *Corriere della sera*, consultabile all'indirizzo: https://www.corriere.it/opinioni/23_aprile_01/se-l-intelligenza-artificiale-rischia-sfuggirci-mano-ed0f1e94-d0a9-11ed-8952-10f6bf0a23fa.shtml

Bianca, C.M., (2019), *Diritto civile. Il contratto*, Milano, Giuffrè-Francis Lefebvre.

Bonnefon, J.F., Rahwan, I. e Shariff, A., (2023), The Moral Psychology of Artificial Intelligence, *Annual Review of Psychology*, 75, pp. 653-675.

Brancaccio, G., Tortora, C., (2020), *Gli effetti dell'AEB nella riduzione dei sinistri. Il sostegno della tecnologia nella lotta agli incidenti*. [Online] Consultabile all'indirizzo: https://fondazionecaracciolo.aci.it/notizie-ed-eventi/gli-effetti-dellaeb-nella-riduzione-dei-sinistri-2/ (Data di accesso: 28 marzo 2024).

Cadwalladr, C., (7 maggio, 2017), The great British Brexit robbery: how our democracy was hijacked. *The Guardian*, consultabile all'indirizzo: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Calabresi, G., Al Mureden, E., (2020), Driverless car e responsabilità civile, *Rivista di diritto bancario*, supplemento gennaio/marzo, pp. 7-21.

Calabresi, G., Al Mureden, E., (2021), *Driverless cars*, Bologna, Il Mulino.

Carere, M., La responsabilità del conducente di un veicolo a guida autonoma: uno sguardo comparatistico fra Germania e California. [Online] Consultabile all'indirizzo: https://www.andig.it/saggi/la-responsabilita-del-conducente-di-un-veicolo-a-guida-autonoma-uno-sguardo-comparatistico-fra-germania-e-california (Data di accesso: 14 marzo 2024).

Carrà, M., (18 febbraio, 2021), I rischi 'nascosti' dell'auto a guida autonoma e il pericolo dell'hackeraggio. *Forbes*, consultabile all'indirizzo: https://forbes.it/2021/02/18/i-rischi-nascosti-dellauto-a-guida-autonoma-e-il-pericolo-dellhackeraggio/

Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*. [Online] Consultabile all'indirizzo: https://op.europa.eu/it/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1 (Data di accesso: 17 agosto 2023).

Cristianini, N., (2023), *La scorciatoia. Come le macchine sono diventate intelligenti senza pensare in modo umano*, Bologna, Il Mulino.

Cruciani, A., (19 giugno, 2022), Hacker e auto, violare una vettura auto è fin troppo facile. I rischi e come difendersi. *Corriere della sera*, consultabile all'indirizzo: https://www.corriere.it/tecnologia/22_giugno_19/hacker-auto-violare-vettura-auto-fin-troppo-facile-rischi-come-difendersi-91adca52-efa7-11ec-8f59-93717c23f0aa.shtml

Della Giustina, C., De Gioia Carabellese, P., (2023), Il futuro ruolo dell'assicuratore nei rischi legali dei veicoli automatici Unmanned vehicles, trolley problems and data protection, *Rivista Trimestrale di Diritto e Procedura Civile*, 4, p. 1235.

Di Ciommo, F., (2017), Principio indennitario e traslazione dei costi sociali, in Landini, S., Ruggeri, L., a cura di, *Il mercato assicurativo nell'unitarietà dell'ordinamento giuridico*, Roma, Edizioni Scientifiche Italiane, pp. 33-61.

Faralli, C., (2019), Diritti e nuove tecnologie, *Rivista di scienze della comunicazione e di argomentazione giuridica*, XI, 2, pp. 44-55.

Federal Trade Commission, (2024), *In the Matter of Facebook*, Inc.. [Online] Consultabile all'indirizzo: https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter (Data di accesso: 15 marzo 2024).

Ferrari, V., (2022), Diritto robotizzato? Riflessioni socio-giuridiche sulle nuove tecnologie della comunicazione, *Annali del Dipartimento Giuridico dell'Università degli Studi del Molise*, 23, 3, pp. 3-14.

Gaeta, M.C., (2016), Automazione e responsabilità civile automobilistica, *Responsabilità Civile e Previdenza*, 5, pp. 1718-1750.

Gill, T., (2021), Ethical dilemmas are really important to potential adopters of autonomous vehicles, *Ethics and Information Technology*, 23, pp. 657-673.

Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, (2019), Orientamenti etici per un'IA affidabile. [Online] Consultabile all'indirizzo: file:///C:/Users/Stefania/Downloads/ethics_guidelines_for_trustworthy_ai-it_87FEA6D2-977E-4064-0532C4315EB55247_60430+(5).pdf

Hu, M., (2020), Cambridge Analytica's Black Box, *Big Data & Society*, 7, 2, pp. 1-6.

Istat, (2023), Report incidenti stradali Anno 2022. [Online] Consultabile all'indirizzo: https://www.istat.it/it/files/2023/07/REPORT_INCIDENTI_STRADALI_2022_IT.pdf (Data di accesso: 15 marzo 2024).

Kaiser, B., (2019), *La dittatura dei dati*, New York, HarperCollins.

Limone, D., (1995), *Dalla giuritecnica all'informatica giuridica*, Milano, Giuffrè-Francis Lefebvre.

Mauro, V., Dalla Chiara, B., Deflorio, F. e Carboni, A., (2017), *Auto-matica il futuro prossimo dell'auto: connettività e automazione*, Roma, Fondazione Caracciolo per Aci.

McCarthy, J., Minsky, M.L., Rochester, N. e Shannon, C.E., (1950), Proposta di un Progetto di ricerca estivo sull'intelligenza artificiale presso il Dartmouth College, *Sistemi intelligenti. Rivista quadrimestrale di scienze cognitive e di intelligenza artificiale*, 3, pp. 413-428.

Parlamento europeo, (16 febbraio, 2017), Norme di diritto civile sulla robotica. [Online] Consultabile all'indirizzo: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html#title2 (Data di accesso: 17 agosto 2023).

Parlamento europeo, (3 marzo, 2024), Il Parlamento europeo approva la legge sull'intelligenza artificiale. [Online] Consultabile all'indirizzo: https://www.europarl.europa.eu/news/it/press-room/20240308IPR19015/il-parlamento-europeo-approva-la-legge-sull-intelligenza-artificiale (Data di accesso: 13 marzo 2024).

Procida Mirabelli di Lauro, A. e Feola, M., (2020), *Diritto delle obbligazioni*, Napoli, Edizioni Scientifiche Italiane.

Proietti, G., (2020), *La responsabilità nell'intelligenza artificiale e nella robotica*, Milano, Giuffrè-Francis Lefebvre.

Ruffolo, U., eds, (2020), *Intelligenza artificiale. Il diritto, i diritti e l'etica*, Milano, Giuffrè-Francis Lefebvre.

Russell, S.J., (2021), *Living with artificial intelligence, The Reith Lectures*, consultabile all'indirizzo: https://www.bbc.co.uk/programmes/-m001216k (Data di accesso: 17 agosto 2023).

Russo, G., (2023), La responsabilità civile auto nell'era digitale. Inapplicabilità e re- interpretazione dell'attuale assetto normativo dell'art. 2054 c.c., *Actualidad Jurídica Iberoamericana*, 18, pp. 1218-1241.

Sartor, G., (2022), *L'intelligenza artificiale e il diritto*, Torino , Giappichelli.

Scagliarini, S., a cura di, (2019), *Smart roads e driverless cars: tra diritto, tecnologia, etica pubblica*, Milano, Giappichelli.

Society of Automotive Engineers, (2021), Livelli di automazione. [Online] Consultabile all'indirizzo: https://www.sae.org/news/2021/06/sae-revises-levels-of-driving-automation (Data di accesso: 17 marzo 2024).

Taddei Elmi, G., Romano, F., (2016), Il robot tra ius condendum e ius conditum, *Rivista di Informatica e Diritto*, XLII, pp. 115-137.
Teubner, G., (2019), *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, Napoli, Edizioni Scientifiche Italiane.
Treccani vocabolario, Tecnologia, consultabile all'indirizzo: https://www.treccani.it/vocabolario/tecnologia/ (Data di accesso: 17 agosto 2023).
Warren, S.D., Brandeis, L.D., (1890), The Right to Privacy, *Harvard Law Review*, 4, 5, pp. 193-220.

SOCIOLOGIA DEL DIRITTO, Vol. 51, Numero 2, 2024
ISSN 0390-0851 – ISSNe 1972-5760