NUOVI PROFILI DI RESPONSABILITÀ PENALE PER L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE: IL PARADIGMA DELLA CIRCOLAZIONE STRADALE

SIMONE TARANTINO

1. INTRODUZIONE

Il progresso tecnologico rappresenta la chiave dello sviluppo dell'umanità e *l'artificial intelligence* (d'ora in avanti *A.I.*), emergendone fiera protagonista[1], promette e prospetta prodigiosi ed innumerevoli nuovi prototipi.

L'attribuzione di un significato univoco alla nozione di sistemi di *A.I.* appare tutt'altro che scontato. Per delineare il fenomeno, si può muovere i primi passi dall'ideatore del termine *A.I. John McCarthy*, professore dell'Università di *Standford* che, nel 1956, ebbe modo di organizzare un evento relativo a questo tema, coniando la seguente definizione: «*the science and engineering of making intelligent machines, especially intelligent computer programs*[2]».

Quando si parla di sistemi di *A.I.*, dunque, si fa riferimento ad una disciplina della *computer science*[3] la quale ha l'obiettivo di ideare, progettare e programmare sistemi informatici intelligenti in grado di realizzare operazioni, non solo computazionali, ma anche tecnico-valutative riconducibili al processo logico-cognitivo umano. I sistemi di *A.I.*, nel loro apprendimento, sfruttano meccanismi di *machine*[4] *e deep learning*, che permettono loro di imparare e migliorare le proprie *performance* grazie all'utilizzo di una vastissima gamma di dati, detenuti negli archivi

[1] Dirompente come *Marianne* nel quadro "*la Libertà che guida il popolo"*, del pittore esponente del romanticismo francese *Eugène Delacroix*, l'*A.I.* si erge come protagonista della rivoluzione che l'utilizzo di questi sistemi porterà a livello sociale.

[2] L'A.I. è, quindi, «*la scienza e l'ingegneria che si occupa di creare macchine intelligenti, specialmente programmi informatici intelligenti*», cfr. MCCARTHY J., *What Is Artificial Intelligence*? (Nov. 12, 2007), consultabile alla pagina web < https://perma.cc/N5YZ-QYS7 >.

[3] "*L'I.A. è una disciplina della computer science che si occupa di sviluppare e creare sistemi computazionali in grado di realizzare operazioni tipicamente riconducibili alle capacità cognitive e decisionali degli esseri umani, come l'apprendimento, il problem solving, il riconoscimento di volti e linguaggi, e così via",* cfr. PANATTONI B., *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale,* in *Il diritto dell'informazione e dell'informatica*, n. 2 – 2021, pp. 317- 368, p. 317.

[4] *"Machine learning involves computer algorithms that have the ability to learn or improve in performance over time",* cfr. SURDEN H., *Machine Learning and Law*, in *Washington Law Review*, Vol. 89, No. 1, 2014, pp.87 – 115, p.89.

digitali. Il programmatore imposta un determinato obiettivo che la macchina deve realizzare: a partire da un *input* preciso e da un *output* prestabilito, il software dovrà essere in grado di portarne a compimento l'operazione richiesta, nel modo più logico e funzionale.
Gli agenti artificiali odierni si connotano, però, per l'automazione non ancora per la piena autonomia: automazione caratterizza i sistemi di intelligenza artificiale c.d. deboli *o weak A.I.*, mentre l'autonomia caratterizza i sistemi di *strong A.I.*, come ampiamente dimostrato negli studi del professor Searle[5]. Non tutti i sistemi di *A.I.*, però, sono in grado di rielaborare le informazioni allo stesso modo: si definiscano, infatti, sistemi sistemi di *strong* o *weak A.I.*
Gli agenti automatici o sistemi artificiali deboli (o *automatic agents*) sono quei sistemi informatici che simulano la conoscenza umana, ne riproducono le sfaccettature, ma non sono in grado, valutando la mole di dati a cui sono sottoposti, di assumere decisioni autonome. Questi sistemi di *A.I.* agiscono come se rappresentassero un'intelligenza tramite algoritmi che riproducono lo schema decisionale umano, ancorché affinato dalla profondità dei database detenuti ed in grado di risolvere problemi di ragionamento con dimestichezza e velocità maggiori rispetto alle capacità di un'ordinaria intelligenza umana. Materialmente, però, questi ne rappresentano solo un'imitazione.
Diversamente da questi sistemi, invece, i sistemi di *A.I.* c.d. forte[6] (o *autonomous agents*) si connotano per essere autonomi dall'agire dell'uomo; ed infatti, detengono una capacità cognitiva non distinguibile dal fare umano. Il sistema intelligente, qui, si caratterizza per autonomia decisionale, operativa e tecnico-valutativa, cosicché questo possa individuare in autonomia i pattern da seguire, senza concreta programmazione *ex ante* dell'uomo.
Raggiunta questa capacità tecnologica, il *software* agirà in autonomia senza più necessitare della programmazione umana.

2. IL QUADRO GIURIDICO EUROPEO DEI SISTEMI DI *A.I.: L'A.I. ACT*

Diritto e tecnologia rappresentano mondi a velocità diverse: troppo rapido l'avanzamento tecnologico, quanto affaticato il diritto nel rincorrerlo. I progressi tecnologici, infatti, si replicano ad una velocità così elevata da impedire ai legislatori, nazionali ed internazionali, di adottare tempestive regolamentazioni atte ad arginare le conseguenti derive sociali del fenomeno.
Uno dei settori che, con più evidenza, prospetta molteplici applicazioni è quello dell'*A.I.*: la versatilità e la funzionalità sono i baluardi imprescindibili per raggiungere obiettivi di miglioramento della vita dell'uomo. Proprio la varietà d'utilizzi possibili di questi sistemi impone necessariamente una presa di posizione unitaria per stabilizzare in modo coerente gli usi.
A sottolineare la sensibilità del tema, l'Unione europea sta lavorando attivamente alla costruzione di un tessuto normativo comune, preordinato a tessere tra gli Stati membri una fitta rete di collaborazione e cooperazione armonica per affrontare al meglio il fenomeno.
Il primo tentativo operato dall'Unione in quest'ottica è dato dalla Proposta di Regolamento, pubblicata nell'aprile 2021, definita *Artificial intelligence Act*[7], il cui testo è stato approvato dal Parlamento europeo il 14.6.2023. Con questa proposta, la Commissione intende promuovere una

[5] SEARLE J., *Minds, brains, and programs. Behavioral and Brain Sciences*, 1980, 3(3), pp. 417 – 424.
[6] TURING A.M.., *Computing Machinery and Intelligence*, 1950, Mind 49: 433-460, «*According to strong AI, the computer is not merely a tool in the study of the mind; rather, the appropriately programmed computer really is a mind*».
[7] Parlamento europeo (a cura di), Proposta di regolamento che stabilisce *regole armonizzate sull'intelligenza artificiale* e modifica di alcuni atti legislativi dell'Unione, COM (2021) 206 final.

regolamentazione comune in materia, in modo da garantire alla legislazione di fronteggiare, in modo coordinato, lo sviluppo tecnologico di questo settore. Quest'obiettivo potrà essere realizzato per il tramite di una costante revisione dell'adeguatezza applicativa del Regolamento, da attuarsi con cadenza quinquennale dalla sua data di entrata in vigore. Il timore è che una regolamentazione troppo stringente risulti evidentemente soffocante, con la conseguenza di raggiungere ben presto l'obsolescenza. Il monitoraggio e la revisione continua, invece, consentono al legislatore europeo di utilizzare gli strumenti più idonei per affrontare consapevolmente le sfide del progresso che la corsa digitale cela.

Resa obbligatoria con le nuove modifiche alla Proposta, ora, è un'*A.I. Board* composta dai vari rappresentanti degli Stati membri e che avrà il compito di monitorare il mercato con particolar riferimento ai rischi di natura sistematica, insiti nell'uso dei sistemi di *A.I.*

Per quanto attiene alla competenza territoriale di applicazione di questa proposta, lo strumento regolamentare eletto non può essere considerato casuale: la scelta è di agire direttamente nei confronti di chiunque voglia investire nel mercato europeo in materia di *A.I.* e non solo nei confronti di coloro che in Europa detengono le sedi sociali delle loro imprese produttive. Data la difficoltà di individuare attualmente una normazione capillare sugli aspetti fondamentali del fenomeno, l'Unione assume un approccio basato sul rischio[8]: per il tramite di questo, infatti, un prodotto algoritmico viene valutato in base alla sua incidenza sui diritti fondamentali dell'uomo. L'obiettivo dell'Unione è quello di creare regole armonizzate a livello comunitario che, tutelando i diritti fondamentali, prevedano, nei confronti dei produttori, degli obblighi continuativi di monitoraggio dei comportamenti di questi sistemi. L'algoritmo, per semplificarne la previsione, dovrà mostrarsi chiaro, trasparente e di facile consultazione per i tecnici tenuti al controllo.

I criteri di classificazione del rischio prevedono tre possibili livelli: basso o minimo, alto od inaccettabile. Con «rischio» si intende l'eventualità di un danno arrecato a un determinato settore o interesse tutelato dalla legislazione: la probabilità di questo contraddistingue la categoria di appartenenza del sistema intelligente, con annessa indicazione delle prescrizioni finalizzate alla sua gestione e minimizzazione.

La difficoltà della questione si coglie sin dalla rubrica: i sistemi ad alto rischio (Titolo II, art. 6), pur potendo produrre maggiori innovazioni, risultano chiaramente accompagnati da una serie di prospettive potenzialmente pericolose. Poche problematicità, infatti, detengono i sistemi a basso o minimo rischio nell'*A.I. Act*, in quanto sistemi di utilizzo comune, con automazione minima e processi automatizzati controllati dall'utente umano agevolmente.

In contrapposizione a questi sistemi si trovano quelli il cui rischio viene classificato come inaccettabile. Relativamente a questi, si segnalano quei sistemi caratterizzati da una capacità di incidere profondamente sui diritti fondamentali dell'uomo, dunque contrari ai principi cardine dell'Unione europea.

I sistemi con rischio inaccettabile nella Proposta di Regolamento[9] prevedono, al titolo II, art. 5 e ss., un elenco di attività illecite che involgono l'uso di sistemi di *A.I.* La Commissione, che ha dato impulso alla proposta, evidenzia come debba vietarsi «*l'immissione sul mercato, la messa in*

[8] Commissione europea (a cura di), Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Libro bianco sull'intelligenza artificiale. Un approccio europeo e alla fiducia*, COM (2020) 65 final.

[9] Parlamento europeo (a cura di), Proposta di regolamento, COM(2021) 206 final, cit.

servizio o l'uso[10]» di quei sistemi atti a distorcere il comportamento di un soggetto, mediante tecniche subliminali o di sfruttamento delle sue vulnerabilità. La tutela della persona appare, quindi, pilastro imprescindibile nello sviluppo di questi sistemi.
Allo stesso modo è vietato l'uso di sistemi intelligenti strumentali all'attribuzione di punteggi sociali (c.d. *social scoring*): con questi algoritmi si classifica l'affidabilità di un gruppo di persone fisiche, spesso i più poveri, in base a caratteristiche personali quali abitudini, etnie, religioni o razza. La pratica, utilizzata negli ambiti commerciali, è sottoposta a divieto di utilizzo qualora comporti un trattamento pregiudizievole o sfavorevole di determinate persone fisiche in contesti sociali non collegati a quelli in cui i dati sono originariamente raccolti o generati.
Allo stesso modo, la pratica è vietata qualora il medesimo trattamento pregiudizievole o sfavorevole risulti ingiustificato o sproporzionato rispetto al loro comportamento sociale.
Ulteriore applicazione tecnologica vietata coinvolge i sistemi di identificazione biometrica remota, «in tempo reale», in spazi accessibili al pubblico. Con questa pratica l'algoritmo è utilizzato come strumento di rilevazione a distanza delle persone fisiche mediante il confronto di dati biometrici detenuti all'interno di *dataset* mondiali.
La connotazione particolare di questi sistemi è che il rilevamento dei dati raccolti avviene in tempo reale, in modo simultaneo agli eventi: chiari emergono i problemi relativi alla protezione dei dati personali disciplinati nel Regolamento UE 2016/679 nonché, da ultimo, nel recente regolamento definito *Digital services act*[11].
Una deroga a questa pratica vietata è stabilita laddove l'interesse pubblico e la sicurezza sociale imponga l'intervento delle forze di sicurezza: l'attività di contrasto appare, infatti, il settore in cui più evidenti si manifestano le potenzialità di questa tecnologia. L'attività di identificazione biometrica «*in tempo reale*» in spazi accessibili al pubblico è, pertanto consentita solo con limitazioni spazio-temporali ed in ipotesi di minacce rilevanti. I sistemi algoritmici possono essere utilizzati per ricercare potenziali vittime di reato, compresi i minori, ovvero in attività di prevenzione di una minaccia specifica, tangibile, materiale ed imminente per la vita o l'incolumità delle persone fisiche, finanche nel sospetto di un attentato terroristico.
Applicazione fondamentale nella lotta europea al crimine appare l'utilizzo di questi sistemi nella localizzazione, identificazione, esercizio dell'azione penale e rilevamento degli autori o sospettati di reati, per cui è previsto il mandato d'arresto europeo, elencati nella decisione 2002/584/GAI del Consiglio[12] se questi siano punibili nello Stato membro con una pena o una misura di sicurezza privativa della libertà personale della durata stabilita nel massimo ad almeno tre anni. In tale categoria di reati emerge la partecipazione ad organizzazioni criminali, il terrorismo, la tratta degli esseri umani, lo sfruttamento sessuale dei minori e la pornografia infantile, il traffico illecito di stupefacenti, di armi, di organi, il riciclaggio di denaro, la frode e, soprattutto, la criminalità informatica.
L'uso dei sistemi di identificazione biometrica da remoto per attività di contrasto non può essere privo di limitazioni: questo dev'essere infatti parametrato agli obiettivi di cui all'art. 5 paragrafo

[10] *Ibid*., p.65.
[11] Parlamento europeo e Consiglio (a cura di) Regolamento (UE) 2022/2065, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).
[12] Consiglio europeo (a cura di), Decisione quadro: 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri - Dichiarazioni di alcuni Stati membri sull'adozione della decisione quadro. Gazzetta ufficiale n. L. 190 del 18/07/2002, disponibile alla pagina web: < https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32002F0584 >.

1, lett d)[13], bilanciando la gravità, la probabilità e l'entità della minaccia con le relative conseguenze incidenti sulle libertà fondamentali dei soggetti coinvolti.
Baluardo della tutela dell'integrità e dell'uso di questi sistemi ai fini di attività di contrasto è, in ogni caso, l'autorizzazione dell'autorità giudiziaria o di un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso. Tale autorità è chiamata a valutare la proporzionalità della richiesta effettuata da attuarsi nel rispetto dei principi sostanziali e processuali. Tuttavia, una deroga al regime ordinario è data dalle situazioni di urgenza, debitamente giustificate, quando il rispetto di *iter* formali potrebbe comportare un *vulnus* ai soggetti coinvolti. In questi casi, l'utilizzo del sistema è effettuato senza la richiesta all'autorità giudiziaria che verrà effettuata solamente *ex post.*
Disciplina delle modalità, degli usi, dei limiti spazio-temporali, nonché delle relative autorizzazioni richieste, è demandata agli Stati membri chiamati ad esercitare, nei limiti della proposta europea, la potestà legislativa.
Il cuore pulsante della regolamentazione è, però, la disciplina dei sistemi di *A.I.* ad alto rischio: in questo modo vengono definiti i sistemi il cui utilizzo espone salute, sicurezza, ma soprattutto i diritti fondamentali del cittadino a possibili compressioni o lesioni non trascurabili. Tali sistemi si ritengono leciti ed utilizzabili solo sulla base di una serie elevata di controlli non solo *ex ante* sul rispetto dei requisiti obbligatori ed una valutazione di conformità alla legge, ma anche in un obbligo di trasparenza da parte dei fornitori di includere l'*output* atteso nelle istruzioni per l'uso. In questo modo, nella catena di controllo degli utilizzi di questi sistemi, un ruolo importante lo giocano anche i consumatori stessi, i quali dovranno comunicare loro le eventuali anomalie riscontrate nei sistemi.
Quanto alla collocazione topografica, la disciplina relativa a questi sistemi trova sede nel Titolo III, Capo I, art. 6 e ss. della Proposta. Qui sono specificate alcune caratteristiche proprie delle macchine, imprescindibili per i rispettivi costruttori.
L'art. 6, infatti individua come sistema ad alto rischio quello che soddisfi entrambe alcune caratteristiche di sicurezza e conformità all'immissione nel mercato europeo.[14]
Accanto ad una lettura dei parametri sopra elencati, per individuare il rischio di danno per la salute e la sicurezza ovvero un rischio di impatto negativo sui diritti fondamentali, la Commissione tiene conto delle finalità previste dal sistema di *A.I.*, la probabilità del suo utilizzo, l'incidenza sui diritti fondamentali, la portata potenziale di danno o di impatto negativo, la vulnerabilità del target di destinatari del danno, ecc.
Gli obblighi di mantenimento di un sistema di gestione dei rischi sono specificati nel capo II, all'art. 9: in assenza di questi, il sistema non può essere ritenuto lecito. L'obiettivo che i produttori di sistemi devono compiutamente realizzare è la creazione di *hardware*s *e softwares* muniti, fin dal momento della progettazione, di architetture algoritmiche trasparenti e chiare, dimodoché possa essere esperito in modo agevole il controllo degli *outputs* emessi.

[13] Parlamento europeo (a cura di), Proposta di regolamento COM 206 final, cit.
[14] Tali caratteristiche sono:
A) "*il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II*;
B) *il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II*", cfr. *Ibid*., art.7 par. 2.

Il sistema di *A.I.* dev'essere monitorato per l'intero ciclo di vita, richiedendone un aggiornamento costante e sistematico. Una volta immesso sul mercato, dunque, il sistema dovrà essere costantemente monitorato, proprio per evitare la proliferazione di falle di sicurezza, zone di rischio non delineate o consentite, che impongano un intervento congiunto del produttore e del fornitore di essi.I sistemi vengono, poi, sottoposti a rigorose prove di conformità all'utilizzo, idonee ad individuarne le misure di gestione più appropriate.
Il capo III individua, infine, gli obblighi dei fornitori e degli utenti dei sistemi di *A.I.* ad alto rischio e di altre parti, artt. 16 e seguenti.
L'uso dei dati per l'addestramento, convalida e prova dei sistemi di *A.I.* ad alto rischio sono soggetti ad adeguate pratiche di *governance* e gestione dei dati. Le pratiche hanno ad oggetto la raccolta, le operazioni di trattamento e gestione ai fini della preparazione dei dati (es. annotazione, etichettatura, pulizia, arricchimento e aggregazione), le formulazioni di ipotesi pertinenti, una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari, ma soprattutto un esame sulle possibili distorsioni che questi sistemi possono detenere.
Adottando meccanismi avanzati di *machine learning,* si rendono altresì necessarie efficienti reti di sicurezza atte ad impedire una disattivazione «dall'interno» delle chiavi di autorizzazione dei *software* adibiti al controllo e all'individuazione di potenziali rischi di modifica sostanziale delle funzionalità informatiche.
Il rischio sottostante, con l'aumentare della loro autonomia, è legato all'opacità decisoria che tali sistemi detengono gelosamente insiti nella loro natura. Spesso gli algoritmi, infatti, sviluppano delle decisioni in modo autonomo dall*'input* ricevuto e differenti dall'*output* previsto, rendendo difficile per l'operatore ricostruire i *pattern* utilizzati.
Con la crescita dell'autonomia dei sistemi, di conseguenza aumenta il rischio che il loro sviluppo decisionale appaia di difficile comprensione: questo fenomeno è individuato nelle *black boxes*[15].
La conformità ai modelli, ai sistemi di gestione del rischio ed alle funzionalità algoritmiche adeguate all'utilizzo consente di mitigare questo fenomeno, le cui implicazioni vengono, però, studiate con molta attenzione.
I sistemi a basso o minimo rischio detengono una definizione resa *a contrariis:* tali sistemi non sono né a rischio inaccettabile, né a rischio alto, rappresentandone l'odierna fenomenologia più sviluppata nel mercato unico europeo.
Punto di sutura conclusivo nella composizione di questi sistemi è la loro cybersicurezza: resilienza, accuratezza e robustezza ne devono rappresentare i presupposti specifici.
I sistemi di *A.I., software* o *hardware* umanoidi, devono presentare idonei *firewalls* di sicurezza appositamente designati a prevenire tentativi di sabotaggio, danneggiamento o accesso da parte di soggetti terzi non autorizzati. Obblighi di creazione di una impalcatura crittografica di sicurezza, aperta al monitoraggio continuo degli operatori ma sufficientemente isolata, sono attribuiti tecnicamente agli ingegneri informatici, mentre un generale obbligo di predisposizione di questi modelli si associa genericamente a qualunque casa produttrice che detenga l'obiettivo dello sviluppo dei sistemi intelligenti.

[15] CASONATO C., MARCHETTI B. *Prime osservazioni sulla proposta di regolamento dell'unione europea in materia di intelligenza artificiale*, in *Biolaw journal - rivista di biodiritto,* fascicolo n. 3, 2021, pp. 415-437, p. 427.

3. LA CIRCOLAZIONE STRADALE: DAL CONDUCENTE AI SENSORI DI GUIDA AUTONOMA

I settori nei quali l'utilizzo della tecnologia di *A.I.* prospetta significative modifiche sono molteplici: si può immaginare il settore medico sanitario[16], dove, ad esempio, il *Da Vinci Surgical System* coadiuva gli esperti nelle operazioni chirurgiche di altissima precisione, spaziando dall'urologia alla ginecologia, dalla chirurgia toracica a quella generale; si può poi immaginare il settore aviatorio, dove il pilota automatico stabilizza l'operato del velivolo; il settore della logistica; il manufatturiero-industriale; ma soprattutto il settore *automotive.* È in questo settore, infatti, che i sistemi di *A.I.* mostrano, in misura esplosiva, le loro capacità di innovazione: i sistemi algoritmici di *A.I.* gestiscono i comandi longitudinali (accelerazione e frenata) e trasversali (sistemi di sterzo) della vettura, esternando le loro abilità di gestione delle situazioni di traffico, in piena autonomia.

Tale settore, però, risente maggiormente dell'influsso antropocentrico che connota lo sviluppo dell'automobile fin dalle origini del fenomeno. Il progresso delle vetture in telaio, motorizzazioni, prestazioni e funzionalità ha rappresentato l'obiettivo frenetico di tutti gli ingegneri impegnati nel settore *automotive*, lungi da loro il superamento di quel connubio tra automobile e conducente che, per tutto lo scorso secolo, sembrava rappresentare una chimera difficilmente realizzabile.

A conferma di ciò, nel 1968, durante i lavori per la preparazione della Convenzione sulla circolazione stradale di Vienna[17], un numero elevato di paesi decise di attribuire alla figura del guidatore il pilastro imprescindibile di un articolato comune atto ad uniformare la mobilità internazionale ed accrescerne la sicurezza nelle strade.

L'art. 8 della sopra menzionata Convenzione, al comma uno, stabilisce infatti che «*ogni veicolo in movimento*» dovesse avere necessariamente «*un conducente*»[18]. Per i paesi firmatari in cui permaneva tale obbligo, vi sono stati seri problemi relativamente alla programmazione ed alla produzione di questi veicoli; ma soprattutto il risvolto della sperimentazione su strada emergeva come ambito maggiormente frustrato dal divieto previsto dalla normativa. Mentre in paesi come gli Stati Uniti d'America, l'Australia, la Cina o Singapore la guida autonoma macinava già kilometri e kilometri di sperimentazione, viaggiando ed imparando, tramite sistemi di apprendimento profondo, le abitudini, le segnaletiche, la viabilità e gli aspetti più peculiari della guida quotidiana, in Europa tutto rimaneva fermo ed ancorato dai dettami normativi.
Il divieto celato dalla norma è stato recepito come anacronistico ed in controtendenza rispetto le nuove frontiere che la circolazione stradale stava assumendo nel mondo, cosicché con un emendamento, introdotto il 14 dicembre 2020[19], in vigore dal 14 luglio 2022, l'approdo delle auto a guida autonoma nei tracciati stradali dei paesi contraenti è divenuto realtà.

La rottura definitiva del modello di guida tradizionale è avvenuta, dunque, nel luglio scorso quando è entrata in vigore la modifica della Convenzione di Vienna che ha equiparato la figura del conducente, persona fisica, a quella di un sistema intelligente.

---

[16] Per un approfondimento sul tema consulta LAGIOIA F., *L'intelligenza artificiale in sanità: un'analisi giuridica,* Torino, Giappichelli, 2020.

[17] Convenzione di Vienna sulla circolazione stradale, conclusa a Vienna l'8 novembre 1968.

[18] *Ibid*., art. 8: «Ogni veicolo in movimento o ogni complesso di veicoli in movimento deve avere un conducente».

[19] Convenzione di Vienna sulla circolazione stradale, emendamento del 14 dic. 2020, in vigore dal 14 lug. 2022 (RU 2022/51).

La Convenzione è ora implementata dall'art. 34-*bis*[20] il quale tratta, in chiusura del capitolo II, i sistemi di guida autonoma. La novella apre alla sperimentazione dei veicoli a guida autonoma su strada urbana, prescindendo dal requisito del conducente. Tale requisito è ritenuto soddisfatto quando l'autovettura è animata da un sistema di intelligenza artificiale tale da sostituire, inizialmente in ridotte, ma via via in sempre maggiori funzionalità, il conducente del veicolo. Tale sistema, però, necessariamente dev'essere conforme ai regolamenti tecnici nazionali ed internazionali applicabili ai veicoli, nonché alle legislazioni nazionali che regolano il settore della circolazione stradale.

3.1 IL REGOLAMENTO EUROPEO 2019/2144: I REQUISITI DI OMOLOGAZIONE DEI VEICOLI

La sicurezza nelle strade è un tema fondamentale nell'ottica non solo nazionale, ma anche europea ed internazionale. Gli studi dell'Unione stimano infatti come il 90% dei sinistri stradali sono provocati, in diverse misure, da errori umani[21]. L'obiettivo che l'Unione persegue entro il 2030 è quello di dimezzare il numero di decessi e feriti della strada, che ogni anno falcidia vite umane e ne ferisce gravemente molte altre. La prospettiva c.d. «*zero vittime entro il 2050*», invece, appare chiaramente tanto ambiziosa, quanto necessaria per sfruttare in sicurezza le potenzialità che il settore della circolazione offre agli utenti[22].

Al fine di ordinare e armonizzare il sistema della mobilità stradale dell'Unione, il Parlamento europeo ha emanato il Regolamento (UE) 2019/2144 [23], in vigore dal 6 luglio 2022, che ha stabilito i requisiti sull'omologazione dei veicoli a motore e dei loro rimorchi.

Questo Regolamento impone l'adozione immediata di precisi sistemi di sicurezza (ADAS: *advanced driver assistance system)*, che avranno la funzione di assistenza all'esperienza di guida del conducente. Questi sistemi si identificano come sistemi di frenata di emergenza, di adattamento intelligente della velocità, nei sistemi di mantenimento della corsia, di avviso di disattenzione, stanchezza o distrazione del conducente, nonché i sistemi di rilevamento di ostacoli in retromarcia, contribuendo all'adozione comune di standard minimi di sicurezza.

Altri dispositivi sono stati ideati per coadiuvare l'esperienza di guida del conducente, in grado di assisterlo con sensori che rilevano la stanchezza, l'imprecisione negli spostamenti, la distrazione

---

[20] Convenzione di Vienna sulla circolazione stradale, art. 34 *bis*: «*Si considera soddisfatto il requisito della presenza di un conducente in ogni veicolo o complesso di veicoli in movimento quando tale veicolo (o complesso di veicoli) utilizza un sistema di guida autonoma conforme:*

1. *a) ai regolamenti tecnici nazionali, e a qualsiasi strumento giuridico internazionale, applicabili ai veicoli a motore, agli accessori e alle parti che possono essere installati e/o utilizzati sui veicoli a motore;*
1. *b) alla legislazione nazionale che regola il funzionamento del veicolo.*

Il campo di applicazione del presente articolo è limitato al territorio della Parte contraente nel quale si applicano i regolamenti tecnici nazionali e la legislazione nazionale che regola il funzionamento del veicolo».

[21] Parlamento europeo e Consiglio (a cura di), Regolamento (UE) 2019/2144 del 27 novembre 2019, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010,(UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011,(UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012,(UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 della Commissione**,** n° 23.

[22] Parlamento europeo e Consiglio (a cura di), Risoluzione del 6 ottobre 2021 sul quadro strategico dell'UE per la sicurezza stradale 2021-2030 – Raccomandazioni sulle prossime tappe verso l'obiettivo "zero vittime" (2021/2014(ini)).

[23] Parlamento europeo e Consiglio (a cura di), Regolamento (UE) 2019/2144, cit.

nel suo operato. Questi sistemi sono stati ideati proprio per rafforzare e tutelare la debolezza insita nel fattore umano, di per sé sua ineliminabile peculiarità.
Il legislatore europeo individua nel suddetto regolamento, al capo II, l'art. 11[24], rubricato «*requisiti specifici relativi ai veicoli automatizzati e completamente automatizzati*», nel quale vengono identificate le specifiche tecniche a cui i veicoli automatizzati devono conformarsi. La lista, che comprende sistemi di sostituzione di guida longitudinale e trasversale, sistemi di *infotainment* sullo stato della viabilità, della sicurezza e delle condizioni del veicolo, sistemi di registrazione di dati di evento per i veicoli automatizzati, evidenzia una strumentazione essenziale per la definizione di guida autonoma. Tali requisiti, specificati nell'articolato dalla lettera a) alla lettera f), sono ideati per stabilire elevati sistemi di sicurezza idonei ad affrontare le nuove sfide che la guida autonoma porterà con sé.
Se, da un lato, è chiaro qual è l'obiettivo dei sistemi di A.I. che animeranno le scocche metalliche dei veicoli, non è altrettanto chiaro quali siano questi modelli.
Per classificarne i diversi livelli autonomia, illuminante è stato l'intervento della S.A.E. (*Society of Automotive Engineers*)[25], la quale ha previsto una suddivisione crescente in sei livelli di guida, laddove l'autonomia dei sistemi cresce in misura inversamente proporzionale al controllo della vettura da parte dell'uomo. Al crescere dei livelli, cui corrisponde la crescita dell'autonomia dei sistemi intelligenti, diminuisce il potere di gestione dell'uomo.
La spinta tecnologica della guida totalmente autonoma apre moltissime nuove opportunità in termini di progresso sociale: basti pensare all'apertura del mercato dell'automobile a coloro che hanno delle disabilità o delle lesioni fisiche, che li estrometterebbero dalla conduzione stradale.
La spinta dei nuovi mezzi è caratterizzata da un motore *green*, in grado di limitare potenzialmente a zero le emissioni grazie ad una propulsione *full electric*[26], silenziosa ed ecologica.
In queste trasformazioni tecnologiche, come anticipato, l'uomo verrà traghettato da conducente a supervisore prima, per poi divenire un mero trasportato, in quanto il sistema di *A.I.* sarà in grado di attendere tutte le occupazioni necessarie alla guida autonoma.
Il cambiamento epocale ricadrà a cascata anche sul regime dell'imputazione della responsabilità in caso di sinistri, che dovrà essere ricucito a pelle sulla nuova figura del conducente. Sarà questo ritenuto responsabile? O sarà chiamato l'ente produttore? Che ruolo avranno, poi, i programmatori e gli sviluppatori del *software* montato sulla vettura? Se ci fossero manomissioni di un terzo agente?
Prospettive affascinanti, ma ad ora *de iure condendo*.
Affinché lo sviluppo previsto finora possa espletare le sue enormi potenzialità ed in un'ottica di modernizzazione del settore della circolazione stradale, una trasformazione necessaria dovrà essere progettata anche per l'infrastruttura stradale.
La nuova frontiera della mobilità appare quella digitale[27]: automazione ed autonomia dei veicoli

[24] Parlamento europeo e Consiglio (a cura di), Regolamento (UE) 2019/2144, cit.
[25] Si passa da un livello zero, ad autonomia assente, ad un livello 5 di autonomia massima, in cui l'uomo diviene mero passeggero della vettura, cfr. S.A.E. *International, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, Standard* J3016, 2014.
[26] MAGNANI A., *Parlamento Ue approva stop a vendita auto a benzina e diesel dal 2035, si spacca maggioranza*, in *Il sole 24 ore,* 9 giugno 2022, consultabile al seguente link: < https://www.ilsole24ore.com/art/salta-riforma-mercato-ue-emissioni-gas-serra-attesa-voto-auto-AEOFiYeB?refresh_ce=1 >.
[27] Commissione europea (a cura di), Comunicazione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: Verso la mobilità automatizzata: una strategia dell'UE per la mobilità del futuro, COM (2018) 283 final.

necessiterà di correre su un'infrastruttura stradale digitale dotata di ecosistemi connessi, in grado di coordinare in modo pressoché simultaneo automobili, centri di info-viabilità e satelliti grazie a connessioni e radio frequenze sempre più veloci, stabili e con copertura capillare nel territorio.
In simbiosi con questa previsione, assumendo il *full electric* come unica motorizzazione prescelta, emergerà il problema dell'autonomia della ricarica, quale elemento ostativo dell'uso prolungato di queste vetture. Una prima sperimentazione di cui l'Italia, con il progetto «*Arena del futuro*» mostra già d'essere all'avanguardia, però, è il *dynamic wireless power transfer* (*D.W.P.T.*)[28]ovvero un sistema di ricarica ad induzione *wireless* inserito al di sotto del manto stradale, con cui le vetture vengono ricaricate direttamente percorrendone la superficie. Questi sistemi si servono di spire metalliche, installate sotto l'asfalto, che trasferiscono l'energia direttamente al veicolo in movimento, garantendo in questi tratti di strada rifornimento senza l'arresto alle colonnine. Affinché questo sistema possa realizzare il circuito di ricarica, sarà necessario dotare il manto di un trasmettitore nonché la vettura di un ricevitore; così facendo l'energia potrà trasferirsi rapidamente al vettore in movimento.
Questa sperimentazione, che in Italia è prevista lungo l'autostrada A35 BreBeMi, ma che viene replicata in Svezia, Cina, Corea del Sud, Germania, ecc., potrebbe rappresentare una svolta per l'elettrico non solo dal punto di vista sociale, eliminando la *range anxiety* – ovvero il timore di non raggiungere la colonnina di ricarica prima che sia terminata l'autonomia –ma consentirebbe anche ai costruttori di progettare alimentazioni a batteria di dimensioni ridotte, nondimeno in grado di garantire una durata maggiore nel tempo.

3.2 IL CONTESTO MONDIALE DEI SISTEMI DI GUIDA AUTONOMA: I REGOLAMENTI DELL'ONU.

Il tema della regolamentazione del fenomeno della guida autonoma ha assunto, negli ultimi anni, connotati sempre più tangibili tanto che persino l'ONU, è intervenuto con tre regolamenti nel 2021, rispettivamente il n. 155[29], n. 156[30] e n. 157[31], che rappresentano il frutto del lavoro della Commissione Economica per l'Europa delle Nazioni unite (*U.N.E.C.E.*) e sono diretti a disciplinare al meglio i requisiti standard dei nuovi veicoli automatizzati, senza i quali l'omologazione alla circolazione non potrà essere concessa.
Il Regolamento n.157, innesta come supporti obbligatori nelle autovetture i sistemi definiti *A.L.K.S.*: *automated lane keeping system*. tali sistemi, di tipico utilizzo nel terzo livello d'automazione, consentiranno al sistema di mantenere centrata la corsia di marcia tramite un controllo della sterzata del veicolo. Questi sistemi presentano, però, delle rigorosissime restrizioni d'uso, atte a ridurre in modo sensibile il rischio agli occupanti la strada. Questi, infatti, potranno essere utilizzati su vie di rapido scorrimento, laddove la circolazione sia adibita esclusivamente ad automobili e motoveicoli, con espresso divieto di transito a pedoni e biciclette. L'elemento

[28] Ansa, Auto: è realtà l'Arena del futuro, test ricarica elettriche, in Torino, 2 dicembre 2021, consultabile alla pagina web: <https://www.ansa.it/canale_motori/notizie/attualita/2021/12/02/auto-e-realta-larena-del-futuro-test-ricarica-elettriche_b7f98c8a-1f1a-4862-aea5-b957ccfac0a5.html >. Sul tema confronta anche Moveo by Telepass, 26 luglio 2022: *Perché l'asfalto che ricarica potrebbe spingere il mercato delle auto elettriche*, consultabile alla pagina web: < https://moveo.telepass.com/asfalto-ricarica-auto-elettriche/ >.
29 United Nation (ed.), ECE/TRANS/WP.29/2020/79: Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.
30 United Nation (ed.), ECE/TRANS/WP.29/2020/80: Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system.
31 United Nation (ed.), ECE/TRANS/WP.29/2020/81: Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems.

soggettivo di diniego non è il solo esplicitato nel regolamento, ma questo deve aggiungersi quello oggettivo delle carreggiate: tali sistemi potranno essere attivati, infatti, solamente in quelle carreggiate laddove le direzioni dei due sensi di marcia siano separate da spartitraffico invalicabile. In definitiva, si può affermare che tali sistemi possano essere adottati nelle autostrade o nelle tangenziali a scorrimento veloce, i cui sensi di marcia siano invalicabilmente separati.
Per massimizzare i livelli di sicurezza, è stata prevista una limitazione della velocità di crociera realizzabile con questi sistemi: 60 km/h è il tetto fissato dal regolamento, che nei sistemi di guida autonomi di livello tre non potrà essere superato.
Ad emendare questa previsione, ampliando il raggio d'utilizzo, è stata proposta ed approvata una disciplina di modifica al previsto regolamento che estende la velocità massima dei sistemi di guida automatizzata (A.D.S.) per autovetture e veicoli commerciali leggeri: dai precedenti 60 km/h si passa ai 130 km/h sulle autostrade. La previsione, adottata durante il Forum mondiale per l'armonizzazione dei regolamenti sui veicoli[32], entrata in vigore nel gennaio del 2023.

3.3. UNA VISIONE COMPARATA: LE NORMATIVE DI GERMANIA E FRANCIA

Appurato che all'interno dell'UE manca una regolamentazione quadro in materia di guida autonoma, molto è demandato ai legislatori nazionali, chiamati ad interpretare un articolato e frastagliato quadro, tutt'altro che sistematico, nell'emanazione delle disposizioni interne. A fronte di questa lacuna ordinamentale, l'investimento *extra* europeo in questi sistemi genera già profitti vertiginosi per un mercato potenzialmente in grado di modificare permanentemente il concetto di mobilità su strada. Cogliendo le preoccupazioni di chi richiede una regolamentazione netta nella gestione del rischio e chiara nei profili d'imputazione giuridica in ipotesi critiche, i governi dei principali paesi stanno adottando degli articolati normativi atti a disciplinare il fenomeno nei termini e con le condizioni necessarie per garantire il massimo espletamento del potenziale di questo nuovo settore.

3.3.1 I VEICOLI A MOTORE CON FUNZIONI AUTOMATIZZATE: L'ESPERIENZA TEDESCA

All'interno dell'eurozona, un paese è emerso per la sua scelta lungimirante nell'investimento del digitale e nello sviluppo tecnologico: figlia di quelle scelte di politica industriale è la odierna posizione di leader assoluto nel nuovo settore dell'*automotive* che sta sorgendo.
Il primo paese di cui è importante trattare il quadro ordinamentale è la Germania.
La prima proposta di disciplina della guida automatizzata risale al 2015 con un *iter* che proponeva la modifica del codice della strada, atta a consentire il transito di queste vetture nei tracciati pubblici[33]. L'iter parlamentare è iniziato nel gennaio 2017 quando il governo tedesco ha presentato un progetto di legge, prima al *Bundesrat*, che emendato è passato al *Bundestag* il quale, nel marzo dello stesso anno, lo ha trasmesso alla commissione competente per il traffico. L'iter di perfezionamento della legge si è concluso il 30 marzo 2017 quando il *Bundestag* ha approvato il progetto di legge del governo federale, modificando la legge sui trasporti (L.18/11776) ed introducendo, come prima regolamentazione europea, la normativa sulla guida autonoma.

[32] *United Nation* (*ed.*), ECE/TRANS/WP.29/2022/59/Rev.1: *Proposal for the 01 series of amendments to UN Regulation No. 157 (Automated Lane Keeping Systems).*
[33] LOSANO M. *Il progetto di legge tedesco sull'auto a guida automatizzata*. Appendice: il progetto di legge e le relazioni illustrative, in *Diritto dell'informazione e dell'informatica*, xxxiii, 2017, pp. 1-25, p. 4.

L'emendamento al codice della strada tedesco ha apportato molteplici mutamenti al concetto di guida, ora non più demandata unicamente alla figura storica del conducente. Affinché un veicolo autonomo possa circolare in modo libero all'interno del manto pubblico è necessario il superamento di diversi test e l'ottenimento di un'omologazione tecnica, che ne certifichi l'assenza di rischi gravi per la circolazione: la licenza d'utilizzo o autorizzazione dovrà certificare il rispetto formale e sostanziale dei requisiti stabiliti dalle norme internazionali (es. R.157 dell'ONU), dei requisiti europei previsti in materia (es. Regolamento UE 2018/858 e 2019/2144) e della regolamentazione nazionale in materia circolazione (*Strassenverkehrsordnung*).

I veicoli assumono la denominazione di «*veicoli a motore con funzioni di guida altamente o completamente automatizzate*», connotandosi per sistemi di bordo capaci di controllo longitudinale (accelerazione e frenata) nonché trasversale (sterzate), idonei a rispondere in modo preciso alle sollecitazioni del traffico[34]. Il sistema autonomo è posto sotto il controllo del conducente, il quale potrà attivarlo quando vi sono le condizioni conformi all'utilizzo e dovrà disattivarlo, invece, nel momento in cui queste dovessero venire meno. Evidente appare come non si possa, allo stato attuale, rinunciare alla figura del conducente, che di conseguenza diviene non solo colui che conduce il veicolo, ma anche colui che attiva i sistemi di guida autonoma, con evidenti implicazioni in tema di responsabilità. La scelta del legislatore tedesco è stata quella di identificare una *fictio iuris*, nel senso di ricondurre al concetto di conducente anche colui che non stava materialmente esercitando il controllo sul veicolo[35], ma ne stava solo sorvegliando l'operato. La legge stabilisce, inoltre, quelli che sono i rapporti diretti nella collaborazione tra il sistema autonomo ed il conducente, i quali si devono tradurre in un uso corretto, coordinato e cooperante per l'ottimizzazione dell'esperienza di guida. L'art. 1b comma 1 consente, per la prima volta nella storia, ad un conducente di distogliere l'attenzione dal traffico stradale e dal controllo del veicolo, mentre questo è sottoposto ai sistemi intelligenti. Il conducente mantiene, però, l'obbligo di intervenire immediatamente qualora lo ritenesse opportuno, secondo le condizioni del traffico, ovvero quando è il sistema stesso a richiederne l'intervento: l'omissione di questa imposizione, in caso di sinistro, comporta gravi conseguenze giuridiche nei suoi confronti.

Emblematica è, però, la materia della responsabilità del conducente in quanto è rimasta essenzialmente immutata. Dal punto di vista civile, questa è regolata dall'art. 823 del *BGB* (Codice civile tedesco*)* e dall'art. 18 dello *StVG*, a cui si affianca la responsabilità oggettiva del proprietario, il quale sarà chiamato a rispondere al di là della colpa, non potendo essere esonerato qualora il danno dipendesse dal malfunzionamento del sistema di guida, come invece vale per il conducente[36].

La più rilevante problematicità riguarda il caso di sinistri stradali con imputazione penale dell'autore, in quanto non vi sono state modificazioni né al Codice penale, né al Codice di procedura penale, né all'articolato relativo alla responsabilità per danno da prodotto difettoso. Di conseguenza, in caso di difetto di un prodotto, produttore o gestore del sistema tecnologico possono essere ritenuti responsabili per l'evento occorso.

---

[34] JUHASZ A., *The Legal Framework of Autonomous Driving in Germany, MultiScience - XXXIII. microCAD International Multidisciplinary Scientific Conference University of Miskolc, 23-24 May, 2019*, consultabile alla pagina web: < https://www.uni-miskolc.hu/~microcad/cd2019/e1/E_Juhasz_Agnes.pdf >.

[35] *Ibid*.

[36] JUHASZ A., *The Legal Framework of Autonomous Driving in Germany*, cit.

Le evidenti criticità correlate allo sviluppo manifestate nel corso degli anni, nonché la parallela espansione del mercato mondiale, hanno portato il legislatore tedesco ad intervenire nuovamente, nel 2021, con alcune disposizioni di emendamenti al codice della strada.
La proposta di emendamento al *Straßenverkehrsgesetzes und des Pflichtver- sicherungsgesetzes – Gesetz zum autonomen Fahr*[37] (*Road traffic act and the compulsory insurance act)*, entrato in vigore nello stesso anno, implementa le misure di sicurezza previste per l'omologazione dei veicoli e garantisce la certezza del diritto nel settore della guida autonoma di livello quattro della classificazione S.A.E. L'avanzamento scientifico nel mondo digitale, oltre che portare con sé molti miglioramenti ed apparecchiature innovative, ha evidenziato la necessità di innalzare *firewalls* difensivi sempre più complessi contro minacce esterne alla cybersicurezza. Il legislatore tedesco mostra di aver ben chiara questa problematica ed inserisce nel paragrafo 1f del StVG[38] delle specifiche tecniche di cui i software devono dotarsi. Si afferma infatti la necessità dei costruttori di dimostrare sia all'autorità competente che l'architettura tecnica ed elettronica del veicolo autonomo è efficiente nel suo utilizzo e protetta da accessi esterni.
Il documento di valutazione dei rischi associati deve essere esibito, se richiesto dall'autorità pubblica, in modo da garantire robustezza, organicità e chiarezza dei sistemi. Altrettanto importante è, poi, l'istruzione di colui che acquista il veicolo autonomo in quanto dev'essere al corrente delle modalità di guida ed informato relativamente gli obblighi di revisione del veicolo, controllo del funzionamento e denuncia ai costruttori ed alle autorità di vigilanza di malfunzionamenti, errori o manomissioni dall'esterno.
Proprio dall'esterno, un potere di controllo del veicolo è definito «*supervisione tecnica*[39]»: un operatore avrà accesso ai dati di traffico del veicolo supervisionandone le funzioni di guida e, in caso di emergenza, disattivandone le funzioni autonome. Qualora riscontri pericoli o malfunzionamenti interni, potrà intervenire direttamente sulla vettura a supporto del conducente per garantirne affidabilità e sicurezza.
Il sistema tedesco rimane fortemente ancorato alla presenza del conducente all'interno dell'autovettura, considerandolo il soggetto chiamato ad intervenire nelle ipotesi critiche. Tale aspetto spiega la scelta operata dal legislatore, che mantiene il profilo della responsabilità penale, che rimane ancorata ai produttori, per danni causati da prodotto difettoso, o dal conducente del veicolo, nelle ipotesi in cui il sinistro sia derivato da negligente sorveglianza od omessa transizione di guida quando richiesta dal veicolo. Un'impostazione, quella tedesca, che sebbene abbia dimostrato l'apertura al settore dell'*automotive*, dimostra la volontà di garantire certezza di attribuzione della responsabilità nella fase più critica della transizione digitale.

3.3.2 I VEICOLI CON DELEGA DI GUIDA: L'ESPERIENZA FRANCESE

Il secondo paese di rilievo, intento a non perder terreno in questa corsa a distanza, è la Francia.

---

[37] BMDV, *Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtver- sicherungsgesetzes – Gesetz zum autonomen Fahren*, 08 febbraio 2021, consultabile alla pagina web: < https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze- 19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes- fahren.pdf?__blob=publicationFile >.
[37] Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), d*as zuletzt durch Artikel 1 des Gesetzes vom 12. Juli 2021 (BGBl. I S. 3108) geändert worden ist.*
[38] S*traßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003* (BGBl. I S. 310, 919), d*as zuletzt durch Artikel 1 des Gesetzes vom 12. Juli 2021 (BGBl. I S. 3108) geändert worden ist.*
[39] BMDV, *Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtver- sicherungsgesetzes – Gesetz zum autonomen Fahren*, cit.

La Francia è intervenuta nell'impalcatura penale, modificando il codice della strada, il Codice penale e quello di procedura penale, introducendo i nuovi profili di responsabilità connessi alla guida autonoma. Tale impalcatura potrà essere utilizzata come struttura, poi, per la prossima regolamentazione in materia civile.

L'ordinanza n. 443 del 14 aprile 2021[40] rappresenta il primo intervento sistematico che ha aperto definitivamente le porte all'utilizzo ed alla sperimentazione su strada delle vetture a guida autonoma, quando conformi alle prescrizioni legislative (internazionali ed europei). La svolta è epocale, poiché con queste disposizioni si autorizza di fatto il conducente a staccare le mani dal volante per lunghi tratti, attribuendo il governo del veicolo all'*A.I.*

La prima modifica al *Code de la Route* abbraccia la figura del conducente: tradizionalmente questo era colui che governava, controllava e garantiva il corretto comportamento prudente nel traffico del veicolo, accentrando su di sé la responsabilità in caso di sinistri stradali. Con la recente modifica, invece, è mutata la figura del conducente, che esula ora dalla carnalità di una persona fisica e viene trasmessa ai *chip* degli algoritmi negli *hardware* dell'*A.I.*. Connessi a questo importante riconoscimento, mutano di conseguenza gli obblighi legali del conducente, che passano dal controllo del veicolo alla vigilanza sul corretto funzionamento del sistema. Qualora ci si trovasse in una condizione stradale favorevole al sistema e dall'interno delle condizioni di utilizzo prescritte dalla legge (nazionale e regolamento UE 2018/858[41]) il conducente consegnerebbe automaticamente l'obbligo legale di condurre il veicolo al sistema di *A.I.* attivato. Il suo unico obbligo legale diviene quello di intervenire, quando sollecitato dai sistemi, a fronte di una situazione di potenziale pericolo per sé, l'autovettura o terzi. Conseguentemente, in caso di evento dannoso generato in costanza di funzionamento del sistema intelligente, attivato nel rispetto delle condizioni di utilizzo dal conducente (di cui si deve dare informativa: modifica dell'art. 224-68-1 *Code de la Consommation* introdotto dall'art. 4 dell'ordinanza), questo si vedrebbe esonerato da responsabilità penale per il fatto accaduto, in quanto non responsabile dell'operato dell'*A.I.*.[42]

Tali sistemi, infatti, vengono denominati «*veicoli con delega di guida*», con ciò sottolineando il mutamento del regime di responsabilità che, a determinate condizioni, esonera il conducente.

Il cambio di regime è manifesto in quanto responsabile non è più il guidatore, ma l'auto stessa, quindi il costruttore del veicolo, che sarà tenuto a rispondere penalmente in caso di sinistri con lesioni (art. 1 dell'ordinanza introduce l'art. 123-2 del *Code de la Route*). Affinché il conducente possa definirsi esente da responsabilità, però, il modificato codice francese prevede un rigoroso insieme di requisiti di omologazione cui il veicolo deve essere sottoposto (quelli nazionali ed anche europei), un uso conforme ai sistemi di guida (l. 319-1 *Code de la Route*), una documentata conoscenza di tali condizioni che il costruttore deve aver dato durante l'atto di vendita all'acquirente (L. 224-68-1 e 242- 25-1 *Code de la Consommation*), nonché l'assenza di una richiesta di intervento della vettura al conducente. Questo, infatti, è comunque ancora tenuto,

---

[40] *Ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation,* consultabile alla pagina web: < https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043370894 >.

[41] Parlamento europeo e Consiglio (a cura di), Regolamento UE 2018/858 del 30 maggio 2018 relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli.

[42] MAROTTA M., *La Francia avvia ufficialmente la legislazione sulla guida autonoma*, in *Diritto di internet*, 2021, consultabile alla pagina web: < https://dirittodiinternet.it/la-francia-avvia-ufficialmente-la-legislazione- sulla-guida-autonoma/ >.

soprattutto al livello tre e meno al livello quattro, a prestare attenzione ai movimenti del veicolo, perché lo stesso potrà intimargli di assumere il controllo della guida: se il conducente non dovesse obbedire a questa transizione e si verificasse il sinistro, la responsabilità ricadrebbe su di lui per omissione di un atto dovuto. Nell'allocazione corretta della responsabilità penale, quindi, sarà utilizzato come discrimine il requisito della titolarità delle funzioni di effettiva guida.
Il produttore ovvero un suo mandatario, ai sensi dell'articolo 3 del Regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, in quanto responsabile del veicolo, potrà essere chiamato a rispondere dei «*reati di lesione involontaria della vita e dell'integrità della persona, art. 221-6-1, 222-19-1 e 222-20-1 del Codice penale, quando è accertata una colpa, ai sensi dell'articolo 121-13 dello stesso codice*»[43]. Inoltre, al comma successivo è previsto l'obbligo di pagamento dell'ammenda da parte dei costruttori prevista per la violazione di una disposizione presente nel codice della strada operata da un veicolo con delega di condotta nell'espletamento delle sue funzioni.
Per una corretta allocazione dell'imputazione penale, appare evidente che le transizioni di guida siano costantemente registrate ed annotate in un *database* che consenta, senza inquinamenti o manomissioni, una rendicontazione della titolarità effettiva della guida: *ad hoc* saranno installate nelle autovetture delle scatole nere[44] atte propriamente a questa finalità.
Ad essere modificato, in aggiunta, non è solamente il Codice penale ma anche il codice di procedura penale: l'art. 2[45] della suddetta ordinanza modifica l'art. 529-10 inserendo e disciplinando le formalità per invocare la circostanza esimente della conduzione dei sistemi di guida autonoma, opposta dal conducente al momento dell'infrazione. Le esimenti di responsabilità penale identificate per il conducente umano potranno essere applicate solo se il conducente non era in controllo del veicolo oppure non ne aveva omesso la transizione quando richiesto dal sistema stesso. Affinché possa ritenersi esente da responsabilità il conducente, quindi, non deve essergli imputata né una negligenza o imprudenza nella guida né una negligenza od omessa transizione.
La normativa è entrata in vigore nel settembre 2022, momento dal quale la svolta epocale in Francia potrà essere tangibile e manifesta sotto gli occhi di tutti. L'efficacia della normativa dovrà essere valutata nella forma della viabilità mista: non solo pedoni, ciclisti, ciclomotori ed automobili, ma anche, appunto, i veicoli con deroga di condotta.

4. NUOVI PROFILI DI RESPONSABILITÀ PENALE: I SISTEMI DI GUIDA AUTONOMA

Come detto, l'automazione nei veicoli può divenire fonte di novità significative nel campo della mobilità su quattro ruote, apportando sensibili modificazioni all'intera infrastruttura sociale e giuridica.
Ed in Italia, qual è lo stato dell'arte? Al centro del dibattito si colloca il tema sociale: gli investimenti operati in tal settore hanno l'obiettivo di ridurre drasticamente il numero di sinistri

[43] *Ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation, chapitre III, art. L. 123- 2, cit.*
[44] Per una espletazione del valore probatorio delle scatole nere in ipotesi di sinistro stradale, cfr. PELLEGATTA S., *Il valore probatorio della scatola nera installata sui "veicoli connessi" al vaglio della giurisprudenza: verso un regime speciale di responsabilità civile*, in *Diritto di internet*, fascicolo n.1, 2022, pp.103 – 118.
[45] Art. 2 *ordonnance* n°2021-443: «*Le 1° de l'article 529-10 du code de procédure pénale est complété par un dainsi rédigé: «d) Un document attestant, selon des modalités précisées par arrêté conjoint des ministres chargé des transports, de la sécurité routière et de la justice, qu'un système de délégation de conduite automatisé était activé conformément à ses conditions d'utilisation au moment de l'infraction*».

stradali e le relative conseguenze, quali decessi e lesioni gravi. Lo sviluppo della guida autonoma prospetta altresì una migliore gestione del traffico tipicamente urbano, con ciò riducendo l'impatto ambientale connesso alla circolazione. In questa sede, però, sarà interessante individuare i profili di allocazione della responsabilità penale in caso di sinistri stradali, tralasciando le altrettanto interessanti problematiche aventi natura civile[46].

Il nocciolo della questione è rappresentato dall'individuazione del soggetto colpevolmente e personalmente responsabile dell'evento che ha arrecato l'offesa ad un bene giuridico protetto[47]. La criticità è dovuta al fatto che, per la prima volta nella storia, alla conduzione del veicolo non si trova più – o solamente – un soggetto umano, bensì anche un sistema di *A.I.*, rispetto ai quali è ancora prematuro il riconoscimento di una personalità giuridica.

A fronte di un sinistro stradale in cui è coinvolto un veicolo a conduzione autonoma o automatizzata, quale sarà il soggetto a cui dovrà imputarsi l'evento lesivo occorso?

In Italia, solo in tempi recenti vi è stata una prima apertura al tema della guida automatizzata[48] grazie al decreto del Ministero delle infrastrutture e dei trasporti del 28 febbraio 2018 (c.d. *smart road)* il quale permette al «*costruttore del veicolo equipaggiato con le tecnologie di guida automatica, nonché dagli istituti universitari e dagli enti pubblici e privati di ricerca che conducono sperimentazioni su veicoli equipaggiati con le tecnologie di automazione della guida*»[49] di richiedere l'autorizzazione allo sviluppo di questi sistemi intelligenti, purché la conduzione del veicolo sia monitorata da un supervisore umano.

L'autorizzazione alla sperimentazione e la presenza del conducente, dunque, rappresentano le *conditiones* senza le quali la circolazione è da ritenersi vietata, con ciò attuando implicitamente le previsioni stabilite dell'art. 46 del Decreto legislativo n° 285 del 1992[50]. Questa disposizione associa, infatti, il governo dell'autovettura ad un conducente, persona fisica, dotato di tutti i requisiti previsti per una prudente nonché legale conduzione del veicolo sulla strada pubblica.

Proprio questa prospettiva di mutamento dell'ordinaria modalità di conduzione del veicolo impone riflessioni necessarie da un punto di vista giuridico in quelle che sono le ipotesi penalmente rilevanti di omicidio stradale, ex art. 589 *bis* c.p., nonché di lesioni colpose stradali, ex 590 *bis* c.p.. Tali rappresentano due reati di evento, in quanto il fatto tipico non consta solo di un'azione o di una omissione, ma anche di più eventi, conseguenze ulteriori dell'azione od omissione.

---

[46] Per completezza sul tema, cfr., PRETE CAPASSO TORRE DI CAPRARA G., *Auto a guida autonoma e regole assicurative* in *Il diritto nell'era digitale,* GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie, pp. 315 – 331; cfr. TEDESCO A.P., *Smart mobility e rischi satellitari e informatici: i possibili scenari di allocazione della responsabilità civile*, in *Diritto del commercio internazionale*, n. 4, 2019, pp. 801 – 824 et *alt*.

[47] PICOTTI L., PANATTONI B., *Traditional Criminal Law Categories and AI: Crisis or Palingenesis*? (*International Colloquium Section I, Siracusa*, 15-16 *September* 2022), in R.I.D.P. - *Revue Internationale de Droit Pénal*, Vol. 94, issue 1, 2023.

[48] Per una disamina approfondita del fenomeno, cfr. PICOTTI L., *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma* in *Studi in onore di Antonio Fiorella*, vol. I, CATENACCI M., NICO D'ASCOLA V., RAMPIONI R. (a cura di), *Romatre-press*, 2021, in specie pp. 813 – 837 *et* PICOTTI L., *Veicoli a guida autonoma e responsabilità penale*, in *Veicoli a guida autonoma. Veicoli a impatto zero. Regole, intelligenza artificiale, responsabilità*, CASSANO G., PICOTTI L., (a cura di), Pacini Giuridica, 2023, in specie pp. 255 – 269.

[49] Decreto ministeriale del 28 febbraio 2018: modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di *smart road* e di guida connessa e automatica (18A02619), (GU serie generale n.90 del 18-04-2018), art. 9, comma 2.

[50] Decreto legislativo 30 aprile 1992, n. 285: "*Nuovo codice della strada" (Gazzetta Ufficiale n.114 del 18-5- 1992 - Suppl. Ordinario n. 74),* art. 46, comma 1: «Ai fini delle norme del presente codice, si intendono per veicoli tutte le macchine di qualsiasi specie, che circolano sulle strade guidate dall'uomo».

In caso di sinistro stradale, dunque, quando la conduzione del veicolo è affidata ad un sistema di *A.I.*, chi è tenuto a rispondere dal punto di vista penale?
Interessante, è, dunque valutare le posizioni dei tre soggetti che rilevano in trattazione: il conducente, l'ente produttore del veicolo ed il sistema di intelligenza artificiale che gestisce il veicolo stesso.

4.1 L'EMBLEMATICA FIGURA DEL CONDUCENTE

Di interesse meno centrale in questa trattazione, i sistemi di guida di livello uno e due si innestano nell'ordinario quadro d'imputazione giuridica del conducente: minimo è infatti l'apporto che l'automazione, intesa come assistenza alla guida al conducente, attribuisce alla figura di quest'ultimo, il quale si identifica come penalmente responsabile nelle ipotesi delittuose sopra indicate.
Per analizzare compiutamente il quadro occorre, invece, riprendere le distinzioni che connotano i livelli di guida automatizzati (o semi autonomi) da quelli totalmente autonomi. I sistemi di guida automatizzata, ovvero quelli ricompresi al livello tre della classificazione operata dalla S.A.E., costituiscono algoritmi in grado di condurre lungo le strade il veicolo in autonomia per lunghi tratti, ma richiedono un costante monitoraggio delle operazioni operate dal conducente. Questo assume giuridicamente una posizione di garanzia[51], «*funzionalmente inquadrabile nella categoria delle posizioni di controllo*[52]»: su di lui gravando, dunque, un dovere di impedire, *ex* art. 40 ultimo capoverso, l'accadimento di un evento lesivo. La posizione di garanzia assunta dal conducente richiama generalmente gli obblighi di comportamento prudente, stabiliti agli art. 140 e 141 del codice della strada, cosicché costui sia obbligato a «*comportarsi in modo da non costituire pericolo o intralcio per la circolazione ed in modo che sia in ogni caso salvaguardata la sicurezza stradale*», a «*regolare la velocità del veicolo* [...] *dimodoché sia evitato ogni pericolo per la sicurezza delle persone*».
La ricostruzione dell'imputazione penale, in questo caso, appare legata alla figura del conducente, senza mostrare particolari torsioni con la paradigmatica tradizionale, ascrivendo causalmente l'evento lesivo occorso (omicidio o lesione grave o gravissima stradale) ad una sua imperizia, negligenza o imprudenza.
L'innovazione tecnologica e la sistematica penale sono destinate a compenetrarsi, in quanto «*il tema più importante sta nel decidere quale sia il campo del rischio permesso nel concedere autonomia all'A.I.*[53]». La concretizzazione dell'area lecita all'interno della quale la condotta ascrivibile al tutor (ipotizzabile una denominazione tale al conducente della vettura) sia o meno scevra di conseguenze dal punto di vista penale, risponde ai patemi sociali che tormentano l'opinione pubblica quantomai spaccata tra fiducia nel progresso tecnologico e vigoroso rigetto della conduzione autonoma.
La formalizzazione dell'area di rischio consentito, scelta certamente politica, ne rappresenterà la conseguenza: mappato l'insieme dei protocolli che istituiscono il confine del lecito con l'illecito,

[51] CAPPELLINI A., *Profili penalistici delle self-driving cars*, in *Diritto penale contemporaneo - rivista trimestrale*, 2019, fasc. 2, pp. 325 – 353, p. 334.
[52] PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in *Rivista italiana di diritto e procedura penal*e, fasc. 4, 2020, pp. 1743 – 1772, p. 1751.
[53] FIORELLA A., *Responsabilità penale del tutor e dominabilità dell'intelligenza artificiale. Rischio permesso e limiti di autonomia dell'intelligenza artificiale* in *Il diritto nell'era digitale*, GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie pp. 651 – 664, p. 656.

il quadro permetterà di attribuire alla figura del conducente che abbia rispettato le prescrizioni previste, delle ipotesi di oggettiva esenzione da responsabilità.
L'elemento certificatore dell'imputazione penale nei confronti del conducente sarà l'istallazione all'interno delle vetture di sistemi di registrazione delle fasi di guida, con la conseguenza che, funzionando come scatole nere, attribuiranno con chiarezza la titolarità della conduzione della vettura al momento del sinistro.
Il discorso muta di regime quando il veicolo assume livelli di automazione più elevati, ovvero le *autonomous cars* di livello quattro e cinque.
Le vetture i cui sistemi si identificano con il livello quattro della classificazione S.A.E. vengono considerate veicoli autonomi, poiché in grado di affrontare, in modo compiuto, le mansioni di guida all'interno del traffico urbano. Controllo longitudinale e trasversale del veicolo, rispetto della segnaletica verticale ed orizzontale, coordinamento intelligente con le strade e gli altri veicoli sono solo alcuni dei grandi obiettivi che la guida autonoma promette di realizzare.
Dal punto di vista puramente teorico, questa considerazione dovrebbe spingere il legislatore ad optare per una scelta fortemente politico-sociale di riflessione sistematica, volta all'identificazione di una disciplina composita della figura del conducente. Il conducente, nel significato etimologico, è colui che detiene il governo ed i comandi della vettura, colui che è in grado di determinarne i mezzi e raggiungere destinazioni, colui che guida, appunto. La ricostruzione, nel livello quattro (ma il discorso assume tratti ancora più chiari con i sistemi di guida di livello cinque), della figura del conducente potrebbe rappresentare una scelta di forte impatto sociale, con echi giuridici importanti: attribuire unicamente al sistema di *A.I.* la conduzione della vettura potrebbe scindere dalla schiavitù del volante la persona fisica, tramutandola ora a mero passeggero del proprio veicolo.
Molteplici e rilevanti sarebbero poi le conseguenze, dal punto di vista giuridico, rappresentate da tale scelta: una fra tutti l'impossibilità, dal punto di vista teorico, di attribuire una colpevolezza alla persona fisica, proprio per l'impossibilità di ricostruire un nesso eziologico di correlazione tra l'evento occorso e la titolarità nella conduzione della vettura all'uomo.
L'automazione del livello quattro dei sistemi di *A.I.* della summenzionata classificazione certifica un livello di autonomia nella conduzione del veicolo che può considerarsi quasi completo.
Il conducente persona fisica, dunque, trasfigura la sua funzione a quella di mera sorveglianza, priva di un qualsivoglia intervento attivo anche per lunghi periodi. La svolta nell'autonomia, già dal livello quattro, promette al conducente di fissare la destinazione del mezzo e, durante la crociera, distrarsi, persino lavorare, il tutto senza necessità di un costante monitoraggio.
Quanto fin qui evidenziato impone necessariamente un ampliamento delle ordinarie modalità di ascrizione di un evento lesivo alla figura del conducente che, da un modello d'imputazione generalmente commissivo deve necessariamente modularsi in uno anche omissivo.
Nella ricostruzione dell'elemento soggettivo della colpa per imprudenza o violazione di una regola cautelare, atta a circoscrivere il rischio durante la circolazione stradale, l'omissione viene ricondotta al comportamento complessivo di guida del conducente che, inevitabilmente, ha carattere commissivo[54].

[54] CAPPELLINI A., *Profili penalistici delle self-driving cars*, in *Diritto penale contemporaneo - rivista trimestrale*, cit., p. 335.

Il modello commissivo, però, nell'automazione a partire dal livello quattro, subisce una battuta di arresto critica: considerare colpevole un conducente in un'ipotesi di sinistro nel quale la conduzione del veicolo era attribuita unicamente al sistema di *A.I.* appare difficilmente sostenibile. Di converso, qualora la conduzione manuale del conducente comportasse una lesione ovvero questa dipendesse da un errata valutazione operata dal conducente, tornerebbe attuale il modello commissivo. In breve: dal modello di «*evento lesivo cagionato commissivamente per colpa dei conducenti di veicoli tradizionali, rispetto alle semi-autonomous cars si passerebbe a un modello imputativo alternativamente commissivo ed omissivo*»[55].

Il regime giuridico così delineato, però, tende ad attribuire la responsabilità penale al conducente, ancora una volta, in quasi tutte le situazioni critiche o pericolose che riguardano la circolazione. Questa scelta è legata al generale principio di affidamento che viene applicato in questo settore particolare: tale principio, soprattutto in attività che coinvolgono l'operato di molteplici soggetti, consente all'agente di confidare nel rispetto degli standard di diligenza, prudenza e perizia da parte dei soggetti coinvolti.

Si è parlato espressamente della figura del conducente nelle sue caratteristiche, ma soprattutto vanno considerate le prescrizioni che gli sono attribuite: è corretto allora continuare a denominarlo tale? Ed ancor di più: la licenza per la conduzione del veicolo potrà ritenersi ancora condizione necessaria? Da quanto emerge, fintantoché il livello quattro non viene superato, la risposta potrebbe pendere nel senso affermativo, poiché un margine, sebbene potenziale, è ancora attribuito ad una conduzione manuale del veicolo.

Come evidenziato in questa analisi, molteplici sono ancora le problematiche non solo giuridiche, ma anche sociali che si attestano, critiche, rispetto all'avanzare imperterrito degli sviluppi tecnologici.

Uno dei rapporti di forza secolarmente presenti che la guida autonoma promette di spezzare ma che maggiormente risulta, dunque, frustrato, è la c.d. schiavitù dal volante: emblematico appare infatti legittimare il conducente a svolgere attività differenti dalla guida come leggere o lavorare, nonostante su di sé permangano doveri di vigilanza e monitoraggio del sistema di intelligenza artificiale. Non è un caso che tale problema venga definito in letteratura come «*control dilemma*», evidenziando come nonostante l'automazione stia apportando innumerevoli cambiamenti sociali, a tali non corrisponde un eversivo adattamento giuridico. L'attenzione maggiore che viene data dalla giurisprudenza alla vittima di un sinistro, inoltre, intralcia la creazione di un'area di non punibilità nei confronti del conducente, il quale continua ad essere tenuto a rispondere per una serie quasi indefinita di eventi lesivi. Emblematica permane, dunque, la «(s)*confortante figura parafulmine del conducente*»[56], obbligata, suo malgrado, ad assorbire tutte le relative imputazioni, indipendentemente da una possibile esigibilità di un potere di controllo.

L'ultimo passo nella classificazione futura delle automobili a conduzione autonoma abbraccia il quinto livello ovvero il livello d'automazione massima prevedibile. Questo livello, già in fase di sperimentazione in alcune realtà, prospetta di offrire un'esperienza di guida totalmente autonoma: il sistema di *A.I.* si dimostrerà in grado di gestire la meccanica trasversale e longitudinale del veicolo, in qualsiasi condizione (sia di traffico che atmosferica), rispettando le prescrizioni imposte

[55] *Ibid*., p. 336.

[56] CAPPELLINI A., *Profili penalistici delle self-driving cars*, in *Diritto penale contemporaneo - rivista trimestrale*, cit., p. 337.

dalla segnaletica stradale e dal codice della strada. Il conducente del veicolo è ora definitivamente (ed in tutti gli aspetti) il sistema di *A.I.* insito nell'autovettura, destinato ad assumere, in modo autonomo, ogni decisione attinente alla circolazione stradale. In quest'ottica di mutamento radicale, la persona fisica diviene ora un mero trasportato, un passeggero della propria vettura che elimina, al suo interno, gli strumenti tipici del controllo manuale: sparisce il volante, spariscono i pedali che azionano i sistemi di frizione, frenatura ed accelerazione, spariscono i controlli di aspersione del parabrezza, di illuminazione del manto stradale.

In una locuzione: tramonta l'era del dominio dell'uomo sull'automobile e sorge l'era dell'autonomia dei sistemi di *A.I.*. In quest'ottica, dunque, tramonta altresì l'imputazione personale dell'uomo, declassato a passeggero e non più conducente della vettura.

Le prospettive sociali che questa svolta epocale promette di realizzare sono molteplici: un'automazione totale delle vetture comporta l'estinzione dei reati connessi alla circolazione stradale, come quelli di corsa clandestina o competizione in velocità non autorizzata[57], spariscono le sanzioni amministrative per violazione del codice della strada (come l'eccesso di velocità, l'attraversamento semaforico quando non consentito), o i reati di guida sotto l'effetto dell'alcool o sostanze stupefacenti[58].

In questa prospettiva, lungi dal legislatore legittimare la guida in stato di alterazione alcolica, stimolante potrebbe divenire l'adozione del «*Take me home, I'm drunk button*»[59]: un bottone ideato per sottrarre dalla strada i conducenti il cui tasso alcolemico superi le prescrizioni limite stabilite dalla legge.

Un profilo di responsabilità in caso di evento di danno causalmente ascrivibile al conducente potrebbe emergere qualora la causazione del sinistro fosse eziologicamente riconducibile ad un errore dei sistemi di info-viabilità della vettura, evitabile previa opportuna manutenzione. Tale impatto, sebbene rappresenti un numero limitato ipotesi, è da prendere in considerazione per completezza di trattazione: evidente appare come l'imputazione al conducente potrebbe reggere, sotto il profilo causale, solo ed esclusivamente qualora questo fosse anche il proprietario della vettura. Fondamento causale necessario per ascrivere la colpevolezza al proprietario, però, è dato da una o più disposizioni di carattere giuridico che impongano la manutenzione del proprio mezzo, alcune di queste, rinvenibili nel codice della strada, altre, di necessario nuovo conio del legislatore.

Di fronte a un tale quadro ricco di argomenti, «*ad impossibilia nemo tenetur*[60]» direbbe un giureconsulto latino: estromesso da qualsivoglia operatività nella conduzione del veicolo e retrocesso necessariamente a mero passeggero, la figura del conducente appare definitivamente scomparire dietro le potenzialità dei sistemi di *A.I.* nel quadro dell'imputazione penale nell'ipotesi di sinistro stradale.

---

[57] D. L. n. 285/1992, cit., art. 9 *bis*, rubricato*: «Organizzazione di competizioni non autorizzate in velocità con veicoli a motore e partecipazione alle gare»;* l'art. 9 *ter, rubricato: «Divieto di gareggiare in velocità con veicoli a motore»*.

[58] D. L. n. 285/1992, cit., art. 186, rubricato «*Guida sotto l'influenza dell'alcool*»; art. 186 *bis*, rubricato «*Guida sotto l'influenza dell'alcool per conducenti di età inferiore a ventuno anni, per i neopatentati e per chi esercita professionalmente l'attività di trasporto di persone o di cose*»; l'art. 187, rubricato «*Guida in stato di alterazione psico-fisica per uso di sostanze stupefacenti»*.

[59] DOUMA F., PALODICHUK S. A., *Criminal liability issues created by autonomous vehicles,* in *Santa Clara Law Review, 1157, n. 4 vol. 52, 2012,* consultabile alla pagina web*:* <https://digitalcommons.law.scu.edu/lawreview/vol52/iss4/2 >, p.1163.

[60] CAPPELLINI A., *Profili penalistici delle self-driving cars*, in *Diritto penale contemporaneo - rivista trimestrale,* cit., p.338.

In un quadro così profondamente mutato, radicalmente differente di quello che è ora vigente, per evitare lacune ordinamentali che possano condurre a pericolose derive sociali e giuridiche, è importante vagliare i profili di responsabilità che connotano l'ente produttore.

4.2 IL MODELLO IMPUTATIVO DELLA SOCIETÀ DEL RISCHIO

Per completezza di trattazione, ed in contrapposizione alla tradizione tedesca in cui non è previsto un modello di responsabilità penale per le persone giuridiche, è necessario analizzare le possibili ipotesi di responsabilità da reato degli enti, qualora l'evento lesivo di un interesse giuridicamente tutelato possa ascriversi, unicamente o in concorso con la figura del conducente, alla persona giuridica.

Nei confronti dell'ente, cui si riconducono il progettatore e lo sviluppatore di sistemi di *A.I.* destinati alle *self-driving cars*, emergono due profili imputativi degni di interesse: un primo profilo attiene alla responsabilità colposa per violazione di modelli di organizzazione, idonei a strutturare ed a gestire il rischio d'impresa; il secondo attiene, invece, al profilo della responsabilità per danno da prodotto difettoso[61].

L'assunto di queste discipline muove dal fatto che autovetture i cui sistemi sono riconducibili ai livelli tre (quindi semiautonome) ovvero quattro e cinque (quasi o totalmente autonome), durante la fase di crociera possano causare un sinistro la cui derivazione sia ascrivibile colposamente alla persona giuridica e/o ad un soggetto a questa ascrivibile. Il profilo di connessione può identificarsi in un'omissione grave di valutazione ed organizzazione rispetto ad una situazione potenziale di rischio; ovvero un errore nella progettazione del sistema, l'attribuzione personale del quale risulti particolarmente complessa.

L'impalcatura giuridica del decreto legislativo n.231 del 8 giugno 2001 si basa, come emerge, su un dovere generale di auto-organizzazione della *societas*, orientato finalisticamente all'adozione di modelli idonei ad evitare la commissione di reati. Tre si identificano quali principali direttive d'ascrizione all'ente della responsabilità da reato: la prima si configura nell'ipotesi di omessa auto-organizzazione, la seconda nell'ipotesi di inadeguata auto-organizzazione, mentre la terza si trasforma in un rimprovero mosso all'ente nell'ipotesi in cui non sia possibile individuare l'autore materiale del reato.

Accanto alla proiezione relativa alla più grave omissione di modelli auto-organizzativi, ipotesi di più difficile realizzazione, si può rinvenire l'imputazione dell'ente per inadatta o difettosa previsione di adeguati modelli organizzativi e di gestione, atti a neutralizzare il rischio della commissione di un reato. La previsione normativa dell'art. 6, comma 1, lett. a), b), c), d) del d.lgs. 231/2001, implicitamente, impone all'ente di adottare modelli preventivi di valutazione delle possibili conseguenze derivanti dall'attività d'impresa svolta, con ciò identificando compiutamente un'area di rischio permesso all'interno della quale operare.

L'ente, necessariamente, ha l'obbligo di adottare dei modelli preventivi idonei ad individuare e mappare le aree di rischio lambite, al di fuori delle quali si configura la c.d. «*colpa di organizzazione*[62]», quale emerge dagli articoli 6 e 7 del d.lgs. 231 del 2001.

---

[61] PIERGALLINI C., *Danno da prodotto e responsabilità penale. Profili dogmatici e politico-criminali*, Milano, Giuffrè, 2004.

[62] FIORELLA A., VALENZANO A.S., *Colpa dell'ente e accertamento*, Roma, Sapienza Università editrice, 2016, in specie cap. II, *La colpa dell'ente per la "difettosa organizzazione" nel sistema italiano*, pp. 53 – 60, p.53.

L'adozione di modelli preventivi, satisfattivi della neutralizzazione dei rischi connessi, nonché del rispetto delle regole cautelari individuate dal legislatore, sancisce l'esenzione di responsabilità dell'ente per il reato ipoteticamente ascritto. Importante, in quest'ottica, è poi l'onere probatorio, che grava in capo a quest'ultimo, ovvero l'obbligo di provare che l'agente avesse agito fraudolentemente per eludere i modelli di direzione e coordinamento adottati. L'agire fraudolento del soggetto apicale evidenzia l'incompatibilità del suo operato rispetto ai modelli adottati dall'ente[63].

Quando il tema dell'*A.I.* si lega al mondo della *societas,* imperniata sull'operato dei propri ingegneri e tecnici informatici che progettano e programmano i sistemi, non volendo considerare le pur interessanti ipotesi di reati in cui il sistema di *A.I.* sia utilizzato dolosamente come strumento dall'autore, il tema da analizzare è quello del reato colposo[64] nell'ambito di un'attività lecita. Il *many hands problem* apparirà emergente anche quando verrà trattata la responsabilità per danno da prodotto difettoso.

A livello giuridico, per garantire un'aspettativa di sviluppo alle società che maggiormente stanno investendo in questo settore, sarebbe opportuno istituire un quadro normativo chiaro e trasparente, che abbia il pregio di delimitare un'area di rischio permesso nello sviluppo di questi sistemi. Quest'analisi comporta un dovere di riflessione sul valore della regola cautelare: demarcazione dell'area del rimprovero penale per colpevolezza oppure demarcazione della tipicità del reato colposo? Ed ancora: realizzazione di una perimetrazione del rischio consentito o delineazione di una funzione permissiva, al di fuori del quale si ritiene esclusa la fattispecie di reato?

Gli algoritmi di tali sistemi di *A.I.,* una volta immessi sul mercato ed applicati alle vetture intelligenti, perdono il legame con lo sviluppatore, in quanto dotati di capacità decisionale indipendente. Il comportamento dei sistemi di *A.I.,* in alcune circostanze, però, potrebbe esternare problemi di comprensione e di *explainability* delle decisioni assunte, come nel campo delle decisioni etiche. Nelle situazioni non programmate, infatti, emerge come il programmatore e lo sviluppatore non siano in grado di prevedere e di gestire il comportamento dell'*A.I.*, per via di un'opacità tecnologica che annebbia l'ascrizione eziologica tra l*'input* e l'*output* decisionale[65].

Il profilo critico in questa disciplina involge proprio la riconducibilità causale delle decisioni dei sistemi di *A.I.* al programmatore ed alle altre figure, per cui la paternità riconosciuta (laddove certamente possibile) della sua costruzione potrebbe attribuire un automatismo imputativo in caso di evento lesivo occorso. È evidente come in questa materia, la previsione di ogni possibile decisione del sistema di *A.I.* appare in concreto difficilmente attuabile. Nonostante questo, però, una possibile soluzione ascrittiva potrebbe essere quella della c.d. «*colpa eventuale*»: qualora si realizzasse un evento tipico, essa sarebbe ascrivibile al programmatore, poiché «*la prevedibilità astratta non richiede alcuna previsione dettagliata e specifica dell'eventuale evento dannoso*»[66].

Da un punto di vista dogmatico, però, sul piano causale delle attività lecite, occorre verificare se normativamente sia stata individuata un'area di rischio permesso: l'imputazione penale per reato

---

[63] *Ibid.*

[64] Per completezza d'analisi, cfr. LIMA D., *Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law*, in *South Carolina L. Rev.*, 69, 2018, pp. 677 – 696, p. 690; cfr. SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale*, n. 1, 2021, pp. 83-118, p. 94, *et alt.*

[65] MAGRO M. B., *Decisione umana e decisione robotica: un'ipotesi di responsabilità da procreazione robotica*, in *Legislazione penale* (*Giustizia penale e nuove tecnologie),* 2020, pp.1 – 22, p. 5

[66] *Ibid*., p.19.

colposo, infatti, sarebbe ascrivibile al programmatore qualora con la sua condotta avesse oltrepassato il c.d. rischio consentito.
Tale previsione ricomprenderebbe *in nuce* un particolare regime imputativo per gestire tutte le ipotesi che, per definizione, nell'area dei sistemi di *A.I.* non sono totalmente prevedibili.
La scelta di normativizzare queste aree, però, potrebbe essere osteggiata dal principio di precauzione? Come è noto, il diritto penale, a cui è ascritta la funzione di tutela prediletta dei beni giuridici fondamentali, potrebbe geneticamente optare per una scelta conservativa, vietando lo sviluppo di quei sistemi le cui decisioni si trovino al fuori dal dominio dell'uomo.
Il rischio di arrestare lo sviluppo tecnologico, per un mero timore non provato, non sarebbe, però, compatibile con i principi tecnico-scientifici che, da sempre, muovono le innovazioni e le scoperte. Laddove, infatti, l'utilizzo dei sistemi di *A.I.*, in situazioni connotate da rischio elevato per l'uomo, prospettasse una riduzione drastica del numero di potenziali incidenti, si potrebbe ancora sostenere che il rischio di un margine di imprevedibilità nelle decisioni debba paralizzarne gli sviluppi? Segnatamente nel settore della circolazione stradale un esempio appare illuminante: qualora l'utilizzo dei sistemi di *A.I.* prospettasse una neutralizzazione del numero di sinistri derivanti da errori del conducente, potrebbe, al contrario, ancora sostenersi che il rischio insito nel loro utilizzo fosse da ritenersi insostenibile? È forse auspicabile la creazione di un'area di «*rischio permesso, normativamente riconosciuto*» ed in grado di «*escludere in radice qualsiasi responsabilità penale*?»[67]. Dietro questa provocatoria richiesta d'impunità, si cela il timore dei programmatori di divenire il bersaglio prediletto su cui scaricare il rischio del progresso.
Inoltre, un dovere di diligenza oggettiva, indirizzato alla previsione di un numero indefinito di eventi, non è da ritenersi concepibile «*nell'espletamento di attività lecite che non siano correlate ad un'area di rischio lecito, all'interno del quale non vi è tipicità colposa*».[68]
«L'impiego di tali sistemi avrebbe come conseguenza la neutralizzazione della tipicità del reato nell'ipotesi di un evento lesivo, qualora l'operato del programmatore si fosse attenuto alle prescrizioni che perimetrino il rischio permesso, ciò in quanto assente «*un quadro nomologico causale che possa definire l'efficienza eziologica della condotta*»[69].
In quest'ottica, la scelta del legislatore dovrà tenere in considerazione le potenzialità che i sistemi di *A.I.* hanno insite al loro interno: gli aumenti degli standard di sicurezza avranno il pregio di «*vicariare l'uomo nell'espletamento di attività complesse*»[70].
L'inquietudine che accompagna la gestione dell'*output* delle macchine, però, rischia di presentarsi come un falso problema, in quanto la codificazione di aree di rischio permesso all'interno delle quali ottenere delle autorizzazioni, che certifichino il superamento di controlli preventivi sul rispetto di standard tecnologici e giuridici, potrà senz'altro portare ad una «*contrazione del perimetro dei casi di responsabilità per colpa nella causazione dell'evento*»[71].

---

[67] PREZIOSI S., *La responsabilità penale per eventi generati da sistemi di IA o da processi automatizzati* in *Il diritto nell'era digitale,* GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie pp. 712-726, p. 719.
[68] *Ibid.*
[69] *Ibid.*, p.720.
[70] BORGOGNO R., *La responsabilità penale nei processi ad elevata automazione* in *Il diritto nell'era digitale,* GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie pp. 727- 744, p.737.
[71] *Ibid.*

L'analisi dei rischi in materia di *A.I.* ha portato ad ampliare la conoscenza potenziale degli effetti collaterali derivanti dal loro uso. Da una prevedibilità in astratto dei rischi connessi all'utilizzo di questi sistemi non può, però, discenderne in automatico un'imputazione penale. La creazione di un'impalcatura basata sul rischio a livello normativo normerà l'accettazione delle potenzialità dei sistemi di *A.I.*, sebbene insita in questi permanga un'area di aleatorietà decisoria.
Di pari passo rispetto ai profili d'imputazione del conducente, il modello di responsabilità vicaria, ovvero quella forma di responsabilità imperniata sul principio *respondeat superior*, che lega la responsabilità dello strumento di *A.I.* al suo ideatore, in questa materia, rischia di scomparire definitivamente. Questa previsione è dovuta all'avanzamento strutturale delle loro capacità computazionali e di autonomia decisionale, che li rende prodotti industriali soggettivizzati, capaci di prendere decisioni anche fuori dagli schemi programmati[72].
Il comportamento dell'*A.I.*, una volta resosi indipendente dalla programmazione del suo produttore, verrebbe a costituire una «*causa sopravvenuta da sola sufficiente a determinare l'evento lesivo versificatosi in concreto (art. 41, co. 2, c.p.)*»[73], tale da interrompere, *ex abrupto*, il nesso di causalità che li lega al produttore.
Le problematiche sottese all'accoglimento di questa tesi, però, avrebbero certamente un impatto di risonanza tale da attrarre nella voragine di un vuoto normativo parte di questa disciplina.
Ciò che infatti si rischia è un *responsability gap*: se, allo stato attuale, risulta impossibile imputare direttamente i sistemi di *A.I.*, il risvolto della medaglia implica altresì una deresponsabilizzazione di coloro che li progettano, sviluppano e producono. Tale deresponsabilizzazione appare evidente anche laddove si consideri come opaca non solo la fase decisoria ma anche quella esecutiva, all'interno della quale il sistema di *A.I.* raccoglie dati, computa, analizza ed esegue la funzione per la quale è stato creato. Proprio in quest'ottica ci si allontana maggiormente dall'apparato delle regole cautelari a cui devono conformarsi gli operatori[74].
Onde evitare pericolose forme di responsabilità oggettiva (*versari in re illicita)* mascherate dalla previsione di inarrivabili standard cautelari di presunta prevedibilità, un tentativo di ricostruzione di un modello di responsabilità è rinvenibile all'interno dell'ambito profilo societario.
Un ancoraggio alla disciplina societaria, che presta attenzione ai soggetti operanti al suo interno, riguarda l'ipotesi della responsabilità per danno da prodotto difettoso. Il paradigma della responsabilità per danno da prodotto difettoso si innesta nel magmatico rapporto intercorrente tra il diritto penale e la c.d. società del rischio.
La normativa di carattere penale trae evidentemente alcuni spunti dalla disciplina civilistica della responsabilità oggettiva per danno da prodotto difettoso, che impone a «*chi inocula un rischio*» di «*risentire delle conseguenze che ha provocato sul versante della riallocazione delle risorse economiche*»[75]: il produttore è tenuto, dunque, a risarcire il danno provocato da un proprio prodotto difettoso ad un consumatore. Tale modello di responsabilità oggettiva, però, è in contrasto con i

[72] CAPPELLINI A., *Machina delinquere non potest*? *Brevi appunti su intelligenza Artificiale e responsabilità penale*, in *Discrimen*, 2019, pp. 1 – 23, p. 5 e ss.
[73] SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale, cit.*, p.107.
[74] PANATTONI B.*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Il diritto dell'informazione e dell'informatica,* cit., p.351.
[75] PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in *Rivista italiana di diritto e procedura penal*e, cit., p. 1753.

principi costituzionali che allocano personalmente e causalmente la responsabilità a colui che ha commesso il fatto tipico inquadrabile in una norma penale.
Sul piano concettuale è possibile evidenziare alcune prospettive della responsabilità per danno da prodotto difettoso: una strutturale ed una eziologica. La prima distingue la responsabilità «*per tipo*» di produzione, che specifica le tecniche per la costruzione qualitativa di un prodotto, certificandone le pericolosità annesse, non imbrigliabili all'interno di misure cautelari; quella eziologica, relativa al «modo» di produzione, è finalizzata invece alla neutralizzazione del rischio di danno generato dal prodotto che, laddove munito dei «*prescritti corredi informativi per i consumatori, non esterna profili residuali di elevata pericolosità*[76]».
Spostandosi sul collegato piano eziologico, è importante distinguere i profili della responsabilità per difetto di costruzione, endemico nella filiera produttiva ed in grado di duplicarsi, come un germe portatore di discordia, all'interno del prodotto commercializzato; per difetti di fabbricazione, che involgono uno o più elementi di una serie, per il resto esente da vizi (vizi dovuti ad errori statisticamente calcolabili); per difetti di informazione, laddove il consumatore non viene reso edotto delle corrette modalità d'utilizzo del prodotto; per difetti da rischio di sviluppo, ovvero per quei rischi non conosciuti o conoscibili dal produttore al momento della circolazione del prodotto[77].
L'illustrazione di queste tipologie di danno non è, però, in grado di fagocitare la complessità dei temi di rilevanza penale, evidenziandone le lacune relative all'accertamento eziologico del nesso di causalità e, ancor più, all'individuazione delle singole figure responsabili all'interno delle organizzazioni produttrici. Emerge il problema della responsabilità distribuita[78] ovvero la difficoltà, a livello di ricostruzione eziologica, dell'attribuzione dell'errore fatale fonte del difetto, in quei processi di fabbricazione in cui vi è una collaborazione tra più soggetti che, anche a livelli diversi, hanno partecipato alla creazione del prodotto. Nelle auto a conduzione autonoma, il problema potrebbe abbracciare tanto l'ambito del difetto di progettazione, quanto quelli di programmazione e costruzione, facendo emergere le difficoltà probatorie appena evidenziate data la molteplicità di attori differenti coinvolti nella programmazione delle fasi di guida. Tale ventaglio di attori recitanti il loro ruolo da protagonista nel settore produttivo dei sistemi di *A.I.* esprime l'inadeguatezza del modello personalistico, qualora non fosse possibile compartire ed isolare la sorgente del difetto.
Un secondo aspetto critico involge la struttura stessa del tipico reato omissivo improprio (o reato commissivo mediante omissione) ovvero di quel reato nel quale la legge incrimina il mancato compimento di un'azione giuridicamente doverosa, imposta per impedire il verificarsi di un evento: in questo caso l'evento è elemento costitutivo del fatto tipico. Secondo il principio *cuius commoda, eius et incommoda*, si individua nella figura del produttore il soggetto tenuto ad una posizione di garanzia, presupposto stesso per una responsabilità a titolo di colpa. Il modello privilegiato è quello della posizione di «*garanzia c.d. da ingerenza*»[79], nel quale la responsabilità commissiva per omissione deriva da un fatto precedentemente compiuto dal produttore: la scelta

[76] *Ibid*., p. 1751-1752.
[77] *Ibid.*
[78] MAGRO M.B., *Decisione umana e decisione robotica: un'ipotesi di responsabilità da procreazione robotica*, cit., p. 3.
[79] PIERGALLINI C., *La responsabilità del produttore: una nuova frontiera del diritto penale*? In *Diritto penale e processo*, n. 9/2007, Milano, pp. 1125 – 1130, p. 1126.

della commercializzazione del bene. La prevedibilità di possibili estrinsecazioni pericolose del bene impone genericamente l'obbligo al produttore di tracciarne e monitorarne gli sviluppi.
Un terzo elemento critico in questa riflessione riguarda le forme tipiche di colpevolezza cui la giurisprudenza tende: una sorta di «*pendolarismo tra colpa e dolo eventuale*»[80].
In questa materia così particolarmente complessa, laddove la sistematica intricata della rete algoritmica dei sistemi di *A.I.* incontra la difficoltà di individuare il soggetto responsabile del difetto che riconduca al danno, emerge altresì l'elevata difficoltà a mappare, nella sua completezza, il rischio prevedibile riconducibile alle derive degli *outputs* dei sistemi intelligenti. La capacità di apprendimento autonomo dei sistemi artificiali riflette un'ermeneutica sintomaticità delle situazioni dannose che consente, solo in parte, una prevedibile pericolosità del prodotto: saranno le divergenze nelle realtà, ad es. dei sinistri stradali, che consentiranno al produttore una reazione costruttiva atta a compartimentare il problema e risolverne le derive socialmente inaccettabili. Individuata la difficoltà nella delimitazione solo potenziale dei confini del rischio, non accompagnata dalla capacità di sapersi razionalmente orientare sul versante preventivo, ne emerge un profilo di incapacità a reperire modelli di evitabilità dell'evento dannoso.
È dal punto di vista giurisprudenziale che il tipo d'imputazione appare di così emblematica ricostruzione, oscillando ora sulla colpa cosciente, all'insorgenza dei primi casi critici, ora sul dolo eventuale, qualora il produttore scegliesse di permanere nella situazione di rischio e continuare nella commercializzazione del sistema, nonostante la manifestazione dei suddetti eventi dannosi. La giurisprudenza, di fatto, «*depennando l'evento, issa il rischio a perno della fattispecie*» che si tramuta in un reato d'obbligo, incapace di rendere un «*corredo nomologico di copertura, sfuggendo ad una qualsivoglia pretesa di determinazione*»[81].
Quello che di certo permane nella ricostruzione effettuata è la riconducibilità del danno al prodotto (c.d. causalità negativa), che fa emergere in modo interessante la possibilità di imputare direttamente all'ente la responsabilità per il reato-presupposto, onde evitare pericolosi vuoti di tutela di diritti ed interessi penalmente rilevanti, come la salute, l'integrità e la vita.
Il punto di sutura che lega la responsabilità del danno da prodotto difettoso all'imputazione della società costruttrice può rinvenirsi nell'art. 8 del d.lgs. 231: la disposizione imputa all'ente le conseguenze del reato presupposto anche qualora divenisse impossibile individuare l'autore del fatto tipico. L'omessa individuazione, però, dovrebbe essere accompagnata da una violazione degli standard di diligenza, dai quali derivi l'anomalia del prodotto.
Nel caso della circolazione stradale, affinché sia ipotizzabile una colpevolezza dell'ente, sarebbe necessaria una «modifica de *lege ferenda*, vale a dire l'inclusione dei reati di omicidio e lesioni colpose derivanti da difetti di produzione nel catalogo degli illeciti presupposto della responsabilità dell'ente[82]».
La mancata individuazione della persona fisica può dipendere o dall'assenza di un modello organizzativo dell'ente, incapace di identificare i soggetti adibiti alla filiera produttiva; oppure da un difettoso assetto organizzativo, incapace di contenere il rischio-reato. Onde evitare, però, che l'imputazione di rimpiazzo all'ente si trasformi in un gravoso automatismo d'ascrizione

[80] *Ibid*., p. 1127.
[81] *Ibid.*
[82]Il rischio nell'imputazione è l'uso di un modello circolare: l'inadeguatezza del modello organizzativo è la fonte dell'incapacità di individuare l'autore persona fisica, cfr. PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, in *Rivista italiana di diritto e procedura penal*e, cit., p. 1754.

(oggettiva) della responsabilità, è necessario che ci si trovi di fronte ad un fatto tipico, soggettivamente ed oggettivamente antigiuridico, rispetto al quale si possa identificare un nesso di correlazione funzionale tra la carente organizzazione ed il reato presupposto[83].
A fronte delle difficoltà mostrate, alcune considerazioni sorgono come necessarie.
Le lucide analisi operate in questa materia mostrano come un certo margine di imprevedibilità, sebbene ridotto, potrebbe far vacillare alcuni principi ordinamentali.
Un bilanciamento di interessi appare quantomai necessario: la disciplina societaria necessita di un'implementazione atta a ricomprendere alcune nuove previsioni giuridiche che squarcino il velo che cela i nuovi profili di responsabilità penale. Un regime coerente, chiaro e trasparente dev'essere costituito per quei soggetti (come i programmatori e gli sviluppatori) addetti alla sperimentazione, ideazione e programmazione dei sistemi di *A.I.,* in modo che possano essere isolate e compartite le fonti di rischio. Al legislatore è demandato il compito di operare un bilanciamento di interessi che ricomprenda la tutela dei beni giuridici che potrebbero divenire potenziale bersaglio dei sistemi di *A.I.*, garantendo, altresì, lo sviluppo delle tecnologie di *deep learning, neural network* e *cloud computing,* tasselli, questi, necessari per le vetture a conduzione autonoma.

4.3 L'*A.I.* SUL BANCO DEGLI IMPUTATI? IPOTESI DI IMPUTAZIONE DIRETTA DEI SISTEMI ARTIFICIALI

Un profilo d'imputazione particolare che interseca la materia, solo lambendola allo stato attuale, è l'imputazione diretta dei sistemi di *A.I.*: tale si presenta come la terza direttiva d'analisi sui nuovi profili di responsabilità emergenti, che questa trattazione intende prospettare.
Immaginare un sistema di *A.I.* antropomorfizzato, a cui vengano formalmente attribuiti diritti e doveri, posizioni giuridiche ed interessi appare largamente prospettabile nel mondo del futuro: è forse possibile che un giorno robot ed umani possono calcare indistintamente le stesse strade, possano svolgere i medesimi lavori ed attenersi alle medesime regole.
A fronte delle lacune e dei vuoti di tutela previamente ipotizzabili, senza trascurare il tema del *responsability gap,* un profilo d'imputazione diretta dei sistemi potrebbe essere analizzato per chiudere il cerchio dell'attribuzione di responsabilità nell'ambito della guida autonoma.
Il modello del diritto penale, classificatorio ed ascrittivo dei regimi di responsabilità, tradisce una difficoltà ontologica nell'aprire le porte ad una disciplina tanto delicata quanto dirompente, per via di quei principi costituzionali e di tenuta ordinamentale che sorreggono l'intera impalcatura giuridica dello stato di diritto. Il principio di personalità della pena, il principio di colpevolezza, il valore preventivo e rieducativo della pena sono i pilastri del nostro ordinamento che, a meno di torsioni innaturali, difficilmente si adeguerebbero alla figura della «*personalità elettronica giuridicamente rilevante*»[84] attribuibile ai sistemi di *A.I.*
In primis, appare necessario individuare il centro d'imputazione: *l'A.I.* c.d. forte, ovvero quella in grado di apprendere ed imparare computando i dati dell'esperienza e di emettere decisioni coerenti.
In secundis, è necessario ricostruire un complesso giuridico tale da individuare delle disposizioni capaci di adeguarsi perfettamente ai nuovi modelli d'imputazione.

---

[83] *Ibid.*
[84] PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato,* in *Rivista italiana di diritto e procedura penal*e, cit., 1762.

Esclusi da questa trattazione sono i casi in cui i sistemi intelligenti agiscano come meri strumenti sotto il dominio dell'utilizzatore[85], in quanto questi è personalmente responsabile dell'operato del sistema, sia che realizzi il fatto così come rappresentato *ex ante*, sia che l'intervento imprevedibile del sistema muti il decorso causale (c.d. *aberratio causae)* od il suo oggetto (c.d. *aberratio ictus).* Così come permane il dolo d'esecuzione del reato, qualora dovesse mutare il decorso causale, allo stesso modo permane nella pur contraria ipotesi in cui la deviazione imprevedibile del sistema non comporti la verificazione dell'evento voluto dall'utilizzatore, ma uno diverso (c.d. *aberractio delicti*). In quest'ipotesi, non potrà individuarsi la figura del reato perfetto, ma a nulla osta la configurabilità del delitto nella sua forma tentata, qualora l'agire umano detenga i generali canoni di idoneità e inequivocità degli atti[86] e l'eventuale imputazione colposa dell'evento diverso.
La difficoltà maggiore nel riconoscere una personalità giuridica a questi sistemi, allo stato attuale, è l'impossibilità a livello cognitivo, di attribuir loro una volontà profonda, una capacità d'arbitrio libera e cosciente, con la conseguenza che l'assenza della quale non consente la piena configurabilità dell'elemento soggettivo del reato, condizione necessaria, questa, per l'attribuzione personale di una condotta delittuosa.
Dal punto di vista materiale, l'attribuzione di un fatto, penalmente rilevante, appare riconducibile alla figura dei sistemi di *A.I.*.[87] Chiarificatrice appare la posizione di un sistema di *A.I.* che governi e conduca la vettura nel traffico: qualora si verificasse un investimento imputabile ad un suo errore, non potrebbe non sostenersi che la macchina avesse commesso azioni penalmente rilevanti. Allo stesso modo, persino un'omissione sarebbe astrattamente imputabile al sistema di *A.I.*, in quanto se un agire è imposto alla macchina e questa dovesse scegliere, sulla base dei meccanismi di *deep* o *machine learning*, di non compiere l'atto necessario, in quel caso potrebbe essergli attribuita la commissione mediante omissione[88].
Ma come precedentemente evidenziato, di più difficile configurazione appare la colpevolezza dell'agente artificiale: complessa appare la ricostruzione dell'elemento soggettivo in capo al sistema intelligente, al quale difficilmente la «*negligence*» o l'«*intent*», la volontà e la consapevolezza, potrebbero essere ascritti. Il sistema deve dimostrare non solo la rappresentazione psicologica del suo operato, ma anche la volontà precisa di perpetrarne gli esiti.
Chi sostiene l'imputazione diretta, ritiene che le macchine possano essere create al fine specifico di portare a compimento determinati obiettivi. Un sistema informatico specifico, una volta ricevuto l*'input*, potrà essere programmato per realizzare, secondo le proprie capacità, il compito assegnato. Il sistema intelligente, in questo caso, ha una specifica «volizione» di realizzare il fatto, grazie alla rappresentazione che di questo offrono i suoi *database* di archiviazione. Questa «volizione» al raggiungimento di un determinato obiettivo, cui il sistema si prodiga in ogni modo, è da alcuni ritenuta equiparabile al dolo.
Attribuita al sistema la capacità di rappresentazione volitiva diretta alla commissione del reato, potrebbero immaginarsi delle ipotesi di non punibilità, qualora dovesse essere corrotto il suo

[85] CAPPELLINI A., *Machina delinquere non potest*? *Brevi appunti su intelligenza Artificiale e responsabilità penale*, in *Discrimen*, cit., p.6.
[86] *Ibid*., p. 7, Così anche HALLEVY G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*," in *Akron Intellectual Property Journal,* Vol. 4: Iss. 2, article 1, 2010, consultabile alla pagina web: < https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/ >, p.185.
[87] HALLEVY G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*," in *Akron Intellectual Property Journal*, *cit*.
[88] *Ibid*., p. 187.

funzionamento a causa dell'installazione di un *trojan horse,* un *worm,* un *virus* o in generale un *malware* in grado di neutralizzarne le capacità computative[89].
Con riguardo, invece, alla colpa, ben potrebbe identificarsi uno standard di comportamento di un «sistema modello» su cui parametrare l'operato degli agenti artificiali: stabiliti gli standard di prudenza, perizia e diligenza nello svolgimento di una determinata attività, la violazione di tali prescrizioni potrebbe fondare il rimprovero penale. É evidente come questo potrebbe configurarsi come un falso problema in quei sistemi tipicamente ideati per svolgere determinate attività pericolose, laddove sono richiesti elevati standard di sicurezza e di prudenza: i sistemi stessi non potrebbero contravvenire alle specifiche regole innestate dai propri sviluppatori.
Dal punto di vista strettamente giuridico emergono altresì le persuasive considerazioni svolte rispetto al paradigma sanzionatorio-afflittivo: i sistemi di *A.I.,* ritenuti colpevoli di condotte sussumibili in fattispecie delittuose, potranno essere considerati destinatari della pena stabilita per quel reato, a seguito di un equo processo.
Così come la pena capitale rappresenta l'alienazione dal contratto sociale per un cittadino, caposaldo della società di diritto, a seguito della commissione di un reato grave potrà essere, per i sistemi di *A.I.*, i robot antropomorfizzati, sancita una formattazione o soppressione complessiva delle loro funzionalità. Con tale operazione, l'agente intelligente potrà essere espunto dal contesto sociale, riprogrammato ed epurato potrà essere rimesso in circolazione[90].
A specchio dei paesi che individuano la libertà, intesa come capacità di agire senza vincoli all'interno del compendio normativo civile, come il bene più importante per la vita dell'uomo, la sospensione del sistema per un certo periodo di tempo può essere una sanzione che riproduce le finalità della carcerazione. Questa, infatti, aliena dalla società chi non è in grado di attenersi ai modelli o chi non riesce a rispettarne le prescrizioni: molteplici sono gli spunti che emergono dal Beccaria, nel suo «Dei delitti e delle pene», nel quale sottolinea con lucidità come la privazione della libertà sia per l'uomo fonte di tormento ed insegnamento maggiore rispetto la pena di morte. Un uomo che viene estromesso dalla vita sociale, per il tramite della pena limitativa della libertà, sopporterà le conseguenze delle sue azioni, bramando di riavere quella libertà tanto agognatamente desiderata.
Per i sistemi di *A.I.,* accanto alla carcerazione può essere prospettata l'attività socialmente utile, un lavoro che possa ricucire lo strappo commesso rispetto alla collettività. Persino le pene pecuniarie, come in specie la multa, potranno essere attribuite ai sistemi di *A.I.*: il valore della loro attività lavorativa produce un vantaggio monetizzabile per il privato, in termini di risparmio dei costi o di produzione di ricchezza.
Ma il modello di responsabilità diretta dei sistemi di *A.I.* non avrebbe come conseguenza la deresponsabilizzazione *de relato* dei programmatori. Per converso, programmatori, sviluppatori e ideatori manterrebbero un regime d'imputazione nei loro confronti, qualora il sistema intelligente venisse utilizzato come mero elemento strumentale attuativo della condotta, ovvero qualora l'errore che ha cagionato il danno dipendesse direttamente da un difetto a lui imputabile.
Uno degli argomenti maggiormente spesi per sostenere il modello di responsabilità giuridica diretta dei sistemi di *A.I.* è il forte parallelismo con la responsabilità penale della persona giuridica. Il diritto penale, quando è stato chiamato a normare le fattispecie di reato commesse dagli enti, ha

[89] *Ibid., p.191.*
[90] *Ibid.,* p.196.

implementato il modello originale con una *fictio iuris*, creando cioè un nuovo soggetto (appunto l'ente) chiamato a rispondere per un fatto tipico altrui connesso alla sua attività d'impresa. In questo senso, la modifica normativa celava la necessità di replicare ai nuovi e crescenti pericoli che accompagnavano il fenomeno criminale societario. I sistemi di *A.I.*, così come le società, non hanno una materialità composita, un corpo destinatario della pena: nonostante ciò, però, alcuni reati sono stati già, da questi o attraverso questi, commessi.

L'esigenza di una regolamentazione penale diretta, allo stato attuale, è attenuata poiché smorzato è l'impatto di questi sistemi nella realtà quotidiana. Così com'è stata necessaria l'introduzione della disciplina sulla responsabilità penale degli enti, così sarà necessaria l'attribuzione di profili di responsabilità diretta per i sistemi di *A.I.* Dopotutto: «*Models of criminal liability exist as general paths to impose punishment. What else is needed*?»[91].

A fronte di quanto espresso, a fronte delle considerazioni fin qui presentate, è davvero possibile configurare dei profili di responsabilità penale per i sistemi di intelligenza artificiale? La dottrina maggioritaria, sebbene non abbia mai davvero dato credibilità alla ricostruzione di questa disciplina, è coerente e coesa nel ritenerne, allo stato attuale, non configurabile l'ipotesi di responsabilità diretta.

Le principali motivazioni di questa negazione muovono su tre profili cardine: l'attribuzione dell'elemento soggettivo, il valore della pena ed il parallelismo normativo con le società.

In primo luogo, quando si parla di elemento soggettivo non può che emergere il principio di colpevolezza: il ricorso alla pena da parte del legislatore si legittima a fronte di offese recate colpevolmente, ovvero offese personalmente rimproverabili al loro autore (art. 27 co. 1 Cost.).

Sebbene alla macchina intelligente possa essere imputato un fatto materiale, l'ascrizione soggettiva d'uno stato cosciente appare insormontabile. Il sistema, infatti, ricostruisce la realtà, analizza le circostanze ed emette *output* decisionali adattandosi alla realtà: si parla, come tale, di robot (re)agenti[92].

Anche se astrattamente si può ritenere che la scelta sia operata dal sistema finalisticamente in modo intelligente, ricomprendere in questa capacità anche l'elemento doloso si presenta come una torsione incompatibile coi canoni ordinariamente previsti. Il dolo, per configurarsi nella sua completezza, deve necessariamente ricomprendere non solo la rappresentazione psicologica del fatto nella sua tipicità antigiuridica, ma deve ricomprenderne altresì la volontà effettiva di realizzazione di tutti gli elementi rilevanti del fatto concreto, tramite l'azione tipica. Com'è evidente, però, questa volontà consapevole è concepibile solamente in quei soggetti «*dotati della capacità di autodeterminazione*»[93], ovvero della capacità di scegliere autonomamente il proprio agire. I sistemi intelligenti non sono in grado di avere una così profonda capacità di scelta, non c'è etica, non c'è emotività, in una locuzione: non c'è coscienza o intenzionalità delle proprie azioni[94].

La volontà di questi sistemi, dunque, non può considerarsi piena in quanto è assente la capacità di comprensione della realtà, che appare priva della profondità del libero arbitrio, necessario per cogliere le sfaccettature della realtà e decidere di conseguenza, poiché tali macchine sono

[91] *Ibid*., p. 201.

[92] PAGALLO S., *Saggio sui robot e il diritto penale* in *Scritti in memoria di Giuliano Marini*, in VINCIGUERRA S., DASSANO F. (a cura di), Napoli, 2010, in specie pp. 595 – 607, p. 601.

[93] CAPPELLINI A., *Machina delinquere non potest*? *Brevi appunti su intelligenza Artificiale e responsabilità penale*, in *Discrimen*, cit., p.14.

[94] PAGALLO U., *Saggio sui robot e il diritto penale* in *Scritti in memoria di Giuliano Marini*, in VINCIGUERRA S., DASSANO F. (a cura di), cit., p. 600.

«*automatiche, non autonome*»[95] in quanto si muovono da sole, ma non detengono le capacità di governarsi o regolarsi da sé. Sebbene i sistemi, anche i più evoluti, n quanto si muovono da sole, ma non detengono le capacità di governarsi o regolarsi da sé. Sebbene i sistemi, anche i più evoluti, possono esternare capacità di comprensione e rielaborazione ottimale degli *input* innestati, la capacità di autodeterminarsi è ontologicamente riconducibile all'uomo[96]. Emblematica è la figura del programmatore che progetta e prospetta l'impalcatura algoritmica, la stringa di codici che permette alla macchina di animarsi. È l'algoritmo che produce schemi logici di *decision making* che, però, discendono necessariamente da previsioni informatiche operate dal soggetto umano.

Ciò che manca, ontologicamente, ai sistemi di *A.I.*, è la capacità critica e cosciente di agire liberamente: manca la capacità di comprendere il peso sociale e giuridico delle proprie scelte. I sistemi agiscono come se fossero intelligenti, riproducono un'intelligenza umana, ma questo non significa che tale riproduzione sia di per sé un'intelligenza.

In definitiva, appare chiaro come, nei confronti di questi sistemi, non possa essere mosso il rimprovero penale poiché è assente l'imputazione dell'elemento soggettivo della colpevolezza.

Un ulteriore punto di rottura, verso chi sostiene la configurabilità di una responsabilità diretta, emerge qualora si tratti il sistema sanzionatorio applicabile: in questo caso crolla l'intera costruzione finalistica del modello di prevenzione, generale e speciale, nonché il riferimento primo della pena, ovvero la retribuzione.

Per quanto attiene al carattere della retribuzione, difficilmente l'*A.I.* appare, infatti, come un soggetto suscettibile di un rimprovero penale che, possa, specificamente, scontare una pena atta a riequilibrare lo squarcio sociale commesso con la propria azione.

Non si comprende, altresì, come possano attuarsi le finalità di prevenzione generale o speciale. Dal punto di vista della funzione di prevenzione speciale, o rieducativa, il sistema dovrebbe essere un soggetto in grado di apprendere il disvalore commesso, valutarne le conseguenze negative per il tramite della sanzione commissionata. Il problema si acuisce con i sistemi intelligenti che, salvo una riprogrammazione specifica, che altro non fa che sostituirne i *chip* o *software* «difettosi», non sono in grado di apprendere le motivazioni che hanno condotto il giudice a commisurare una pena.

L'applicazione di una pena come la sospensione temporanea, identificata da Hallevy, mal potrebbe realizzare il ruolo medicinale della pena privativa della libertà personale, poiché assente, nel momento di sospensione, la capacità di rielaborazione e autoriflessione del sistema.

Infine, non è attuabile nei confronti dei sistemi intelligenti la funzione general-preventiva: i consociati robot, infatti, non sarebbero in grado di cogliere la funzione deterrente della punizione, in quanto incapaci di provare emozioni come paura o timore[97].

Nemmeno i più sofisticati sistemi di *machine learning* appaiono in grado di veicolare il messaggio dissuasivo diretto a non realizzare tali condotte poiché assente, a monte, risulta la capacità critica di comprenderne il disvalore causato, altro non trasformandosi che in una conseguenza, prevista, della propria azione da ascrivere al disegno criminoso realizzato. Per quanto concerne, invece,

---

[95] CAPPELLINI A., *Machina delinquere non potest*? *Brevi appunti su intelligenza Artificiale e responsabilità penale*, in *Discrimen,* cit., p. 5.

[96] LIMA D., *Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law*, in *South Carolina L. Rev.*, cit., p. 693 e ss.

[97] CAPPELLINI A., *Machina delinquere non potest*? *Brevi appunti su intelligenza Artificiale e responsabilità penale*, in *Discrimen,* cit., p. 16.

l'argomento più persuasivo utilizzato dai sostenitori della responsabilità diretta dei sistemi di *A.I.*, interessante appare il parallelismo operato con le persone giuridiche.
Per il riconoscimento di un modello imputativo penale per l'ente, il dibattito filosofico-giuridico si è a lungo interrogato sulla possibilità di attribuire materialità ad un conglobato che materialità non possiede, cioè una struttura sociale capace di detenere un ruolo economico. Il riconoscimento di una materialità a questi enti passò per la creazione di una *fictio iuris* che attribuì loro «*realtà*» nel mondo giuridico e sociale. Il parallelismo operato tra la *societas* e l'*A.I.,* però, è un parallelo erroneo in quanto la prima ha, al suo interno, una personalità fisica fatta di soggetti, di uomini che davvero esistono nel mondo fisico, destinatari delle previsioni normative, che orientano la creazione dei modelli di organizzazione sociale e financo ne colpiscono con la pena il portafoglio[98].
Il parallelismo seguito viene definito «*malfermo*»: la *societas* esiste nella realtà giuridica attraverso uomini che «*naturalisticamente e spiritualmente, le danno vita*».
L'attante, il sistema di *A.I.*, invece, è indipendente da un soggetto che ne muova le fila dopo la progettazione e l'addestramento. Il sistema di *A.I.* sarà in grado di scegliere autonomamente, ma solo all'interno degli schemi di riconoscimento programmati dal suo produttore, il cui distacco viene evidenziata dal fatto che l'eventuale sanzione, a questo attribuita, non sarebbe in grado di intaccare gli interessi di alcuna persona alle sue spalle. L'*A.I.* appare capace di autodeterminarsi: diviene un prodotto soggettivizzato dotato di fisicità, in grado di interagire con l'uomo, invocando di essere «*libera, di una libertà che le è stata elargita dal proprio creatore*»[99].
Da questa breve disamina, appare chiaro come, allo stato attuale, sia prematuro poter parlare di personalità giuridica e responsabilità penale diretta per i sistemi di *A.I.*
Prematuro appare il discorso quantomeno per due ordini di ragioni: la prima è di ordine tecnologico, mentre la seconda di ordine giuridico. Allo stato attuale, lo sviluppo tecnologico consente di creare sistemi solo in grado di apparire intelligenti: questi sono, infatti, in grado unicamente di replicare il ragionamento logico umano, comportandosi come se lo fossero, ma inevitabilmente ancora non lo sono. La capacità di replica e di adattamento delle macchine potrà essere il motore che consentirà a questi strumenti di apprendere ed imparare ad apparire umani, ma la strada per una soggettività per questi sistemi appare ancora lunga.
Allo stesso modo, richiedere al diritto di normare un fenomeno in evoluzione così incerta nel suo perimetro, rischia due derive i cui effetti sono entrambi potenzialmente dannosi. La prima deriva potrebbe essere rappresentata da una normazione troppo generica sulla materia, una normazione generalmente inclusiva di molteplici implicazioni giuridiche, a maglie molto larghe, ma con il rischio di essere incapace di gestire correttamente il fenomeno. La seconda deriva, diametralmente opposta, potrebbe portare ad emanare una regolamentazione capillare, a maglie molto stringenti che, però, rischierebbero di imbrigliare un fenomeno le cui evoluzioni dirompenti ugualmente, infine, mostrerebbero l'incapacità di gestire gli sviluppi.

5. UN CROCEVIA NECESSARIO: LA *CYBERSECURITY* NEI VEICOLI AUTONOMI

[98] *Ibid*., p.18.
[99] CAPPELLINI A., *Machina delinquere non potest*? *Brevi appunti su intelligenza Artificiale e responsabilità penale*, in *Discrimen*, cit., p. 18.

Un aspetto che non può essere sottovalutato, nell'ecosistema connesso delle *self-driving cars*, è certamente il tema della *cybersecurity*: l'autovettura, così come un sistema informatico o telematico, può divenire mezzo, strumento o bersaglio di attacchi malevoli. Le crescenti sfide della mobilità connessa impongono riflessioni sui possibili rischi derivanti da utilizzi non conformi o attacchi informatici nei confronti di queste vetture.
I primi moniti del rapporto «*Authority*» di *E.N.I.S.A.* sottolineano come troppo spesso il settore della sicurezza cibernetica venga trascurato, per la mancanza di competenze o l'incapacità di creare progetti adatti a prevenire i rischi. In controtendenza a questo, invece, rispetto l'ambito di applicazione delle vetture a conduzione autonoma, la necessità di ideare sistemi robusti, sicuri ed affidabili appare una pietra miliare per il loro sviluppo.
Pilastro fondamentale che deve accompagnare lo sviluppo di questi sistemi è la c.d. *security by design*[100]*:* la sicurezza, l'affidabilità e la robustezza si ergono come punto di partenza del progetto di produzione del veicolo.
Gli attacchi, astrattamente configurabili, appaiono di molteplici tipologie: bersaglio può essere il sistema di *machine learning*, il quale può subire una distorsione del suo meccanismo di riconoscimento biometrico per il tramite di false somministrazioni di dati che hanno l'effetto, ad esempio, di impedire il riconoscimento corretto di un cartello, aumentando i rischi per la sicurezza stradale. Ulteriore attacco ipotizzabile potrebbe colpire i sistemi di rilevamento delle aggressioni informatiche, con la conseguenza che i *malware*, penetrando nel *core* della vettura, possano agire indisturbati al suo interno.
Aspetto molto critico rappresentano gli aggiornamenti di sistema: qualora *l'update* fraudolento, inviato da un *hacker* tramite un'interfaccia di *phishing* ai sistemi della vettura, venisse installato dal proprietario, la conseguenza potrebbe essere l'apertura di una *back door* capace di garantire un accesso indisturbato, all'attaccante da remoto, all'intero funzionamento informatico.
Da queste brevi considerazioni emerge come il settore della *cybersecurity* si identifichi come un tassello imprescindibile nello sviluppo dei progetti delle *autonomous cars.*
Il trattamento degli innumerevoli dati utilizzati dai sistemi, in conformità con il *G.D.P.R.*, appare altresì elemento di rilevante interesse giuridico: nei veicoli a conduzione autonoma devono essere salvaguardati i diritti fondamentali, nonché le libertà, in modo da garantire un utilizzo improntato alla non discriminazione dei soggetti coinvolti. La raccolta dei dati deve avvenire previa adeguata informativa al titolare, che deve prestarne consenso libero, cosciente, specifico ed inequivocabile. Forti appaiono le criticità in senso probatorio circa la conoscenza e la consapevolezza del loro utilizzo, la prova dei quali non appare certo semplice da fornire.
Dal punto di vista penale, la riflessione conduce ad analizzare criticamente i fenomeni, di fatto verificando se i disposti delle normative vigenti possano adeguarvisi ovvero se, al contrario, ne sia necessaria una revisione. Considerato come a livello attuale la riflessione riguardi fattispecie astratte, è importante individuarne alcune implicazioni concrete, senza pretesa d'esaustività.
Un primo fenomeno ipotizzabile potrebbe essere quello del c.d. veicolo autonomo vettore di sostanze stupefacenti o di altri prodotti illeciti[101]: tale uso consentirebbe alle organizzazioni

[100] COLAROCCO V., *Cybersecurity e intelligenza artificiale: la sfida della guida autonoma e l'intervento dell'ENISA*, in *Diritto di internet*, 2021, consultabile alla pagina web: < https://dirittodiinternet.it/cybersecurity-intelligenza-artificiale-la-sfida-della-guida-autonoma-lintervento-dellenisa/>.
[101] CAPPELLINI A., *Profili penalistici delle self-driving cars*, in *Diritto penale contemporaneo - rivista trimestrale*, cit., p. 344.

criminali di sostituire la figura umana del corriere, di fatto eliminando la principale pedina da cui far partire le indagini in materia di traffico di sostanze stupefacenti.
L'utilizzo di queste vetture potrebbe essere indirizzato, altresì, a commettere attentati, come nell'ipotesi in cui fossero riempite di esplosivo e lasciate vicino luoghi affollati. Tale utilizzo, c.d. *kamikaze* della vettura, potrebbe racchiudere in sé il pericolo per l'incolumità pubblica senza la necessaria opera di immolazione dell'autore.
Vagliando approfonditamente il fenomeno, potrebbe essere punita l'opera di chi crea un pericolo per l'incolumità pubblica, servendosi di vetture a guida autonoma: alterati i sistemi di sicurezza in modo che venga superato il *firewall* che impone il rispetto del codice della strada, le vetture potrebbero essere lanciate ad elevata velocità contro un centro pedonale. Qualora si ipotizzasse, poi, una comunicazione telematica *vehicle-to-vehicle,* il *worm* infettante un sistema potrebbe veicolarsi in un'area circoscritta di veicoli, di fatto creando una flotta di armi mobili da lanciare, in un centro cittadino, allo scopo di attentare alla vita dei passanti. Configurabile, in questo esempio, potrebbe essere il reato di strage, *ex* art. 422 c.p., che punisce con l'ergastolo chiunque, col dolo d'uccidere, compia atti tali da porre in pericolo l'incolumità pubblica, se dal fatto derivi la morte di più persone.
A rigor d'analisi, però, queste fattispecie ricalcano in modo abbastanza puntuale le discipline previste nel Codice penale, dovendo al più essere ampliate le modalità d'esecuzione di tali reati.

5.1 L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO: L'ART. 615-*TER* C.P.

Una delle preoccupazioni più marcate, infatti, legate all'utilizzo di questi modelli, paragonabili a veri e propri sistemi informatici e telematici, è lo scenario nel quale un soggetto terzo, ad es. un *hacker,* si introduca nel sistema e prenda i comandi, da remoto, della vettura. La minaccia prospettata da chi, con fini fraudolenti, si sostituisce nel controllo del mezzo, impone l'adozione di sistemi difensivi idonei a compartire e perimetrare le possibili conseguenze negative derivanti dal tentativo di accesso abusivo operato dall'esterno.
L'*hacker,* in questo caso, per il tramite di una forzatura delle vulnerabilità dei *software* può ottenere le chiavi d'accesso al sistema di *A.I.* che governa la vettura ed utilizzarla, da remoto, come stesse utilizzando un'automobile radiocomandata[102]. L'ingresso nel sistema di un *malware,* inoculato tramite una rete di *phishing,* che sfrutta la debolezza insita al fattore umano, ovvero installato forzando le contromisure di sicurezza, attribuisce il potere al criminale di controllare la vettura.
L'art. 615-*ter* c.p., che nel nostro ordinamento punisce chiunque si introduca abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza o vi si mantenga contro la volontà di chi abbia il diritto di escluderlo, appare riconducibile alla condotta di intrusione dell'*hacker,* persona fisica, che assuma abusivamente il controllo dei sistemi di conduzione della vettura autonoma. Tale fattispecie è, inoltre, uno dei reati presupposto per configurare un'ipotesi di responsabilità penale dell'ente, *ex* art. 24-*bis* d.lgs. 231 dell'8 giugno 2001, qualora fosse imputabile a questo l'accesso non autorizzato.
Tale reato, introdotto dal legislatore nel 1993 con la legge 547, rappresenta un cardine della disciplina in materia di reati informatici. Tale fattispecie è stata costruita e ricalcata sul modello

[102] CAPPELLINI A., *Profili penalistici delle self-driving cars*, in *Diritto penale contemporaneo - rivista trimestrale,* cit., p. 345.

della violazione di domicilio, esteso giuridicamente al concetto di domicilio informatico. La collocazione sistematica dell'art. 615-*ter* c.p. nel titolo XII, sezione IV dei delitti contro l'inviolabilità del domicilio, evidenzia il bene oggetto di tutela, rappresentato dal domicilio che, in questa materia, necessiterebbe di una interessante estensione interpretativa. Tale concetto, inteso come spazio cibernetico di pertinenza della persona, dovrà altresì ricomprendere lo *smart vehicle* nell'area di tutela. Il sistema della vettura intelligente, strumento d'estrinsecazione del domicilio informatico, diviene perimetro nei confronti del quale circoscrivere lo *ius excludendi alios* detenuto dal proprietario. L'estensione giuridica di questo concetto anche alla vettura autonoma, però, dev'essere vagliato dalla più critica dottrina, in quanto evanescente è, in questo caso, il concetto di un domicilio informatico.
La fattispecie, già ampiamente criticata per via delle scelte lessicali che evidenziano le condotte «fisiche» sottostanti le scelte normative («si introduce» e «si mantiene»), trova la sua consumazione già nel momento in cui un terzo non autorizzato instaura un «dialogo logico-informatico» con la vettura: un tentativo di introduzione nel sistema di *A.I.*, operato tramite un ingaggio con il sistema bersaglio, integra di per sé il reato descritto.
Nonostante gli investimenti in materia di cybersicurezza rappresentino un tema centrale per garantire l'affidabilità dei sistemi delle vetture a conduzione autonoma, al fine della configurabilità del reato di accesso abusivo ad un sistema informatico o telematico non è richiesta né la forzatura delle misure di sicurezza, né l'adeguatezza a prevenirne gli attacchi. Tale requisito si erge piuttosto come elemento di esternazione della *voluntas excludendi alios* del proprietario, sottolineata e rimarcata dall'avverbio «*abusivamente*», che rappresenta una condizione di illiceità speciale. L'avverbio palesa l'assenza di un titolo autorizzativo per l'operato dell'agente, che instaura un contatto sensibile con il sistema, rispetto alla volontà di riservatezza e di esclusione che il proprietario intende esercitare sulla vettura.
Ipotizzabile in concorso con l'accesso abusivo, come sottolineato in giurisprudenza mentre negato in dottrina, è la detenzione, diffusione ed installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico punito dall'art. 615-*quinquies* c.p. Tale fattispecie, prodromica alla realizzazione del reato di accesso abusivo e ricondotta al tema delle *self-driving cars*, potrebbe già punire la condotta di chi installa abusivamente un *malware* all'interno delle vetture, allo scopo di danneggiarne i sistemi di *A.I.*, i dati, le informazioni o interromperne il loro corretto funzionamento. È lo scopo, qui, il fine specifico del dolo della condotta: l'installazione o la detenzione è direttamente volta ad eseguire un *malware* idoneo a creare un danno, ovvero ad interromperne un servizio. Il dolo specifico del danno impernia tale fattispecie e la differenzia da quella stabilita nell'art. 615-*quater* c.p., laddove il dolo specifico è, invece, diretto a procurare profitto a sé o ad altri.

5.2 I DANNEGGIAMENTI DI SISTEMI INFORMATICI: GLI ART. 635-*QUATER* E *QUINQUIES* C.P.

Nell'alveo delle fattispecie riconducibili alle *self-driving cars* si trovano, altresì, i reati di danneggiamento di sistemi informatici o telematici.
Tali previsioni normative sono collocate sistematicamente nel titolo XIII dei delitti contro il patrimonio, capo I ovvero quelli commessi mediante violenza alle cose o alle persone.
Il legislatore, nella fattispecie dell'art. 635-*quater* c.p. punisce la condotta di chiunque distrugga, danneggi, renda inservibili od ostacoli gravemente l'utilizzo di sistemi informatici o telematici.

Ipotizzabile, in questo caso, l'attacco ad un sistema informatico di una vettura autonoma, che abbia l'obiettivo di danneggiarne l'impianto frenante, gli strumenti di localizzazione e posizionamento ovvero, in modo potenzialmente più pericoloso, «gli occhi e le orecchie della vettura»: i sensori *lidar* e radar adibiti alla circolazione. Il danneggiamento o anche solamente l'interruzione dell'ordinaria funzionalità di questi sensori può comportare conseguenze gravi per gli utenti della strada.

Il bacino di condotte punibili appare assai flessibile, lasciando all'interprete l'analisi dei profili attinenti alla distruzione, al danneggiamento, al rendere inservibile o all'ostacolare il funzionamento, fermo restando che l'accesso, qui, è solo prodromico, in quanto è la finalità specifica del danno che impernia la fattispecie. Il danneggiamento, in questo caso, non avviene in modo fisico, ma ad essere colpiti sono i programmi, i *software* che animano e conducono la vettura autonoma: bersaglio prediletto possono essere i sistemi di *machine learning*, che altera le capacità di riconoscimento dei segnali stradali.

Il danneggiamento può avere a bersaglio, altresì, i sensori, inibendone o alterandone il corretto funzionamento ovvero colpire i canali di ricezione, analisi e riproduzione degli *inputs* dati dai segnali stradali.

Rappresentando un punto di connessione imprescindibile per la viabilità del futuro, criticità particolari emergono qualora dovessero considerarsi i problemi di cybersicurezza legati all'infrastruttura stradale intelligente. L'infrastruttura digitale, nella quale si inseriranno le vetture a conduzione autonoma, dovrà essere progettata per gestire quantità considerevoli di traffico di dati gestionali derivanti dai loro sistemi. Il collegamento dovrà gestire in tempo reale non solo le apparecchiature di smistamento e coordinazione del traffico, ma anche i rapporti sulla viabilità inviati dalle vetture ai server delle case automobilistiche.

A fronte della gestione di questa mole esponenziale di dati di traffico, il rischio di subire un attacco cibernetico appare quantomai evidente. Ipotizzabile è il *DDoS attack*: *distributed denial of service,* traducibile in italiano come interruzione distribuita del servizio.

L'architettura stradale, caratterizzata da un sistema di *cloud computing*, potrà essere esposta ad un attacco cibernetico capace di paralizzarne l'intero corretto funzionamento: un «bombardamento» simultaneo di tentativi di accesso ai *server* adibiti al coordinamento dei dati, inibisce la capacità di gestione del traffico e, infine, ne provoca l'interruzione. Ogni *online website,* infatti, detiene una limitata capacità di processazione delle richieste di accesso che, qualora forzata, ha la conseguenza di interromperne il servizio offerto. Il fenomeno è espressione della capacità di un *master* di orchestrare un attacco congiunto da molteplici sistemi, definiti *zombie*, infettati da un precedente *malware,* installato sfruttando, ad es., tecniche di *phishing,* in grado di essere risvegliati e di rivolgere il loro attacco al bersaglio designato. In questo caso di parla di *BotNet.*

Le finalità che muovono questi attacchi possono essere molteplici: colpire società ed istituti di credito per ottenere vantaggi finanziari, ottenere una rivincita di fronte ad un'ingiustizia, motivi ideologici o, ipotizzabile, la *cyberwarfare*[103]. L'evoluzione del *battlefield* segue necessariamente gli sviluppi legati alle nuove armi ed ai nuovi sistemi tecnologici: se nel Novecento le guerre di combattevano solamente con lo scontro di armate fisiche (terrestri, aeree o navali), la modernità ha riservato un nuovo campo di battaglia, non fisico, ma cibernetico: chiara, in questo caso, è la

[103] ZARGAR S. T., JOSHI J., TIPPER D., *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*, in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, Fourth Quarter 2013.

situazione della guerra in Ucraina, laddove molteplici sono stati i tentativi, da ambo le parti, di rendere inservibili ed inutilizzabili i diversi portali governativi nazionali, le reti telefoniche e quelle di telecomunicazione.

5.3 LE INTERCETTAZIONI ILLECITE DELLE COMUNICAZIONI INFORMATICHE O TELEMATICHE: L'ART. 617-*QUATER C.P.*

Ulteriore fattispecie, che bersaglia l'insieme del traffico dati intercorrente nell'ambito delle autovetture a conduzione autonoma, che può configurarsi è l'intercettazione illecita delle comunicazioni informatiche o telematiche, prevista dall'art. 617-*quater* c.p.

Tale previsione normativa è collocata sistematicamente nel titolo XII, dei delitti contro la persona, alla sezione V, ovvero quella dedicata alla tutela dell'inviolabilità dei segreti. La condotta ipotizzabile, in questo caso, è quella di un *hacker* che, per fini prestabiliti, carpisce ed intercetta le comunicazioni che intercorrono tra i sistemi informatici ed i *server* della società produttrice dell'autovettura autonoma. L'elemento costitutivo che caratterizza questa fattispecie, ricalcata sul modello delle intercettazioni di comunicazioni tra persone, è che qui ad essere carpito è il flusso intercorrente tra due sistemi. L'intercettazione qui captata non è più, dunque, un flusso comunicativo tra persone, così come previsto nel Codice di procedura penale, ma si tramuta in flusso comunicativo tra sistemi, il cui dialogo logico viene intercettato o impedito dal terzo soggetto agente. Tutelata, in questo caso, nella sezione V del Codice penale, è l'inviolabilità dei segreti, anche se in questo caso non è più la comunicazione umana il bersaglio della condotta dell'agente.

Prodromica alla realizzazione di questo reato, può ipotizzarsi l'installazione di apparecchiature o programmi atti ad intercettare la comunicazione tra i sistemi: l'art. 617-*quinquies* c.p. punisce proprio chiunque, al fine di intercettare (con il previsto dolo specifico), dispone apparecchiature adibite a questa finalità.

6. CONCLUSIONI

Il progresso tecnologico rappresenta la chiave del futuro dell'umanità, sotto ogni punto di vista: scienza, sanità, economia ed ambiente ne rappresentano i punti cardinali.
Futuro e progresso rappresentano due binari che corrono paralleli, quattro ruote motrici che percorrono la carreggiata, verso un traguardo, mai come adesso, tanto bramato.

Il futuro della mobilità stradale passa attraverso il presente dell'*A.I.*: un sistema di algoritmi computativi in grado di analizzare i dati dell'esperienza, rielaborandoli in un *output* che possa definirsi razionale. Il tentativo di indirizzare, finalisticamente, i processi cognitivi all'interno di meccanismi come il *machine learning* o il *deep learning*, però, in alcune circostanze, viene frustrato dalla strabiliante capacità di questi sistemi, di emettere *output* decisionali inaspettati per il proprio programmatore.

La necessità di prevedere un quadro giuridico coerente per i sistemi di *A.I.*, ha spinto l'Unione europea ad adottare diverse comunicazioni, che sono poi state recepite all'interno della proposta di Regolamento (COM 2021), denominato *A.I. Act*, che definisce aree tematiche di rischio per classificare gli utilizzi dei sistemi intelligenti. Tali vengono distinti, in base all'impatto che possono avere sui diritti e sulle libertà dell'uomo, in rischio basso o minimo, elevato ed inaccettabile. Gli estremi della classificazione appaiono poco rilevanti in quanto se da un lato il

rischio minimo è trascurabile, il rischio inaccettabile, invece, impone rigorosamente il divieto d'utilizzo di questi sistemi, qualora il loro uso, la loro messa in servizio o la loro l'immissione nel mercato siano rivolti ad arrecare discriminazione, sorvegliare e vigilare, sfruttare le vulnerabilità o attribuire punteggi sociali alla popolazione civile. Unica deroga consentita è prevista nell'utilizzo dei sistemi di identificazione biometrica, da remoto, in tempo reale ed in spazi aperti al pubblico, qualora sia coinvolto un interesse di natura pubblica e sia necessario l'intervento delle forze dell'ordine. I sistemi ad alto rischio, invece, sono l'estrinsecazione del bilanciamento di interessi operato dall'Unione: un bilanciamento che consenta lo sviluppo e la crescita trasparente di questi apparati, nel rispetto dei diritti fondamentali.

I settori nei quali l'utilizzo della tecnologia di *A.I.* può apportare significative modifiche sono molteplici: è possibile immaginare il settore della medicina, con l'uso di sistemi intelligenti in grado di coadiuvare i chirurghi nelle operazioni più complesse; il settore aviatorio, dove il pilota automatico stabilizza l'operato del velivolo; il settore della logistica; il manufatturiero-industriale; ma soprattutto il settore *automotive.* È in questo settore, infatti, che i sistemi di *A.I.* mostrano, in misura esplosiva, le loro capacità di innovazione: grazie a sensori intelligenti, radar e lidar, gli algoritmi gestiscono i comandi longitudinali e trasversali della vettura, determinandone la direzione tramite mappe di geolocalizzazione. Immaginare una mobilità che non coinvolga attivamente il conducente, non è un esercizio complesso solo dal punto di vista tecnologico, ma anche sociale e giuridico, in quanto, fin dall'origine dei primi modelli di automobile, la figura dell'uomo era considerata punto nevralgico di partenza, tramutato in accordo certificato dagli Stati firmatari della Convenzione di Vienna del 1968. Inizialmente, dunque, l'automobile era considerata qualsiasi veicolo in movimento dotato di un conducente.

Il primato dell'uomo sul governo della macchina sta, però, scomparendo, per garantire una maggiore sicurezza sulle strade: gli studi effettuati dall'Unione mostrano, infatti, come l'errore umano rappresenti il 90% delle cause da cui derivano i sinistri stradali, un dato preoccupante che ha spinto il legislatore ad investire nell'aumento degli standard di sicurezza di guida. L'entrata in vigore del Regolamento 2019/2144 nel luglio 2022 impone l'adozione immediata di precisi sistemi di sicurezza, nelle vetture di nuova omologazione, in materia di adattamento intelligente della velocità, sistemi di frenatura di emergenza, assistenza al mantenimento di corsia, nonché dei veri e propri sistemi di supporto che monitorino l'attenzione e la freschezza del conducente.

Nonostante le basi per la regolamentazione della mobilità automatizzata fossero state ipotizzate con questo Regolamento, l'emendamento alla Convenzione di Vienna del 1978, entrato in vigore anch'esso nel luglio 2022, ha aperto definitivamente le strade pubbliche alle vetture autonome, equiparando la figura del conducente a quella di un sistema intelligente capace di gestire, in autonomia, le funzionalità di guida. Per classificare i livelli di conduzione autonoma della vettura, l'intervento della S.A.E. è stato illuminante: tale classificazione ha previsto una suddivisione crescente in sei livelli di guida, laddove l'autonomia dei sistemi cresce in modo inversamente proporzionale al potere di controllo della vettura da parte dell'uomo. Se l'autonomia dei sistemi al livello zero è minima, in quanto massimo è il controllo del conducente; al contrario, al livello cinque, l'autonomia dei sistemi è massima, tanto che totalmente assente è il governo della vettura da parte dell'uomo.

Il soppianto definitivo del conducente, però, rimane un obiettivo nel lungo periodo, in quanto ancora acerbi sono i sistemi intelligenti, non ancora capaci di gestire le funzionalità di guida che

non si traducono unicamente nel rispetto del codice della strada. Se acerbi sono i sistemi di *A.I.*, in fase di progettazione sono, poi, le infrastrutture «*smart roads*» che dovranno cooperare direttamente con queste vetture per creare l'impalcatura della mobilità connessa.
A latere delle considerazioni fin qui svolte, però, emerge problematico il profilo della responsabilità: in questa fase di transizione, ci si chiede a chi possa essere attribuita l'imputazione penale qualora si verifichi un sinistro stradale con decessi o lesioni gravi. A fronte di una decisione riconducibile ad un sistema di *A.I.*, non prevedibile dal proprio programmatore, come evidenziato dal Consiglio d'Europa, si rischia un *responsability gap*, in quanto i criteri di colpevolezza e di *mens rea* entrano notevolmente in crisi.
Le risposte ipotizzabili a questo interrogativo variano negli Stati.
A livello europeo, due paesi sono emersi per le loro scelte in materia di responsabilità per la guida autonoma: Germania e Francia rappresentano i leader del settore.
La Germania, fin dal 2015, ha avviato un progetto di avvicinamento all'auto a conduzione autonoma, legando saldamente la figura del conducente ai sistemi di *A.I.*, con ciò attribuendogli la responsabilità, in caso sinistro stradale, qualora questi fossero attivi. Civilmente, in concorso con il conducente, rimane obbligato anche il proprietario, salvo il caso in cui questo dimostri che l'uso della vettura era non autorizzato.
In Francia, invece, va menzionata l'ordinanza del 2021 che esonera il conducente dalla responsabilità penale, in caso di evento dannoso, in costanza e conformità dell'uso dei sistemi di guida automatica, quando fosse stato reso edotto delle condizioni corrette di utilizzo dal venditore.
La figura del conducente, diversamente dal modello tedesco, dunque, si slega dall'uomo per attribuirsi ai sistemi di *A.I.*. L'imputazione penale rivolge la sua attenzione alle case produttrici dei modelli autonomi, qualora l'errore sia derivato da un difetto di fabbricazione o malfunzionamento, imputabile alla programmazione del veicolo, salva rimanendo l'ipotesi di una manomissione esterna.
Su questi temi, l'Italia si trova in una situazione arretrata ed immobile, com'è stato evidenziato dall'incapacità di dare seguito alle prospettive di riforma aperte dal D.M. «*Smart Roads*» del 2018, che rimane fonte secondaria deserta e scarsamente applicata.
Le direttive d'analisi che hanno mosso la trattazione hanno portato a considerazione tre tipologie di soggetti molto differenti tra loro: il conducente, l'ente ed il sistema di *A.I.*
La figura del conducente, nei modelli di transizione che condurranno alla completa autonomia dei sistemi di *A.I.*, permane come confortante figura «parafulmine» dell'imputazione penale, a questi attribuita in forza degli obblighi di supervisione e sorveglianza dell'operato della vettura. Raggiunto il livello massimo dell'autonomia, però, laddove tutti i comandi spariscono dall'abitacolo, l'imputazione di questo soggetto non può più essere considerata rilevante e la necessità di evitare preoccupanti vuoti normativi, impone il vaglio dei profili di responsabilità ipotizzabili per l'ente produttore.
In concorso con la figura del conducente o autonomamente, l'ente assume una posizione rilevante per aver immesso nel mercato la vettura autonoma.
I profili imputativi per la società del rischio possono seguire due direttive.
La prima si lega ai profili della colpa di organizzazione rispetto i modelli d'impresa volti ad evitare la commissione di reati. L'adozione di un modello non idoneo a garantire un'adeguata prevenzione rispetto al verificarsi di eventi criminosi, anche qualora non sia identificabile la persona fisica

autrice materiale del reato di connessione, porta ad imputare direttamente la responsabilità all'ente produttore.
Il secondo modello imputativo analizza i rapporti che legano i produttori agli eventi lesivi, derivanti da prodotti difettosi immessi nel mercato. In quest'ottica, fondamentale è la creazione di un'area di rischio permesso, in grado di delimitare cautelarmente l'operato dei programmatori ed evitarne l'imputazione penale qualora abbiano rispettato le disposizioni stabilite dalla legge. Qualora, invece, vengano violate le disposizioni in materia di perimetrazione del rischio, l'attribuzione della responsabilità all'ente, per l'operato dei propri dipendenti, passa necessariamente per una modifica normativa del decreto legislativo n.231 del 2001, dovendosi aggiungere all'elencazione dei reati presupposto commessi dall'ente, l'omicidio e le lesioni colpose derivanti da un prodotto difettoso.
A fronte dell'aumento delle capacità d'autonomia dei sistemi di *A.I.*, l'analisi è stata, infine, orientata a vagliare l'opportunità di estendere l'imputazione penale all'operato autonomo dei sistemi intelligenti. Seppur stimolanti le tesi e la lucidità argomentativa dei paradigmi utilizzati, allo stato attuale non appare riconducibile ai sistemi di *A.I.* una capacità d'arbitrio, libera, profonda e cosciente, l'assenza della quale non consente la configurabilità dell'elemento soggettivo, condizione necessaria per l'attribuzione personale di una condotta delittuosa.
Il problema si pone in termini retorici in questo particolare momento storico, in quanto lo stato della tecnologia consente solamente di immaginare robot antropomorfizzati, capaci di pensare liberamente e svolgere esattamente le funzioni umane.
In un futuro, forse più prossimo che remoto, il legislatore si troverà, però, costretto a legiferare per disciplinare il rapporto dell'uomo con i robot antropomorfizzati, individuando i limiti e confini di questa nuova coesistenza sociale.
Accanto ai modelli imputativi legati alle figure rilevanti del conducente, dell'ente produttore o dell'*A.I.*, una direttiva d'analisi ha vagliato i possibili aspetti legati alla *cybersecurity*: la necessità di trasparenza degli algoritmi delle *A.I.* traspare anche nei sistemi delle vetture a conduzione autonoma, rispetto alle quali appare la necessità di istituire sistemi di sicurezza *by design* e *by default* per contrapporsi, saldamente, alle possibili minacce rivolte contro questi. Tali minacce possono individuarsi nell'accesso abusivo, nei danneggiamenti e nelle intercettazioni abusive di sistemi informatici o telematici, emergendo così la necessità di configurare idonei *software* difensivi che possano garantire una perimetrazione robusta delle funzionalità della vettura.
Un vuoto di tutela allarmante rimane come monito al legislatore del presente, divenendo una sfida concreta per il legislatore del futuro: dell'opacità decisionale dei sistemi di *A.I.*, qualora sia rispettata l'area di rischio permesso, non potendo ad essi imputarsi alcuna responsabilità, a chi potrà essere imputata? Una modifica dei principi costituzionali potrà essere orientata ad introdurre forme di responsabilità oggettiva? La giurisprudenza, poi, come si approccerà a questi temi: rigore garantista o aperture innovative?
Gli interrogativi sono molti; i rischi sentiti, le incertezze affiorano nel campo dell'ordinamento: non resta che la fiducia nelle innovazioni a cui il progresso condurrà.
In un futuro, forse remoto, le tre leggi di Asimov, che fino ad allora rappresenteranno, per alcuni, mera fantascienza, riesumate, potranno rappresentare i principi cardine di un nuovo patto sociale che dovrà essere negoziato, e che, immaginiamo, potrà veder contrapposti, nella nuova Costituzione, i diritti fondamentali dell'uomo, a quelli, altrettanto fondamentali, dei robot.

BIBLIOGRAFIA

BORGOGNO R., *La responsabilità penale nei processi ad elevata automazione* in *Il diritto nell'era digitale,* GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie pp. 727-744.

CAPPELLINI A., *Machina delinquere non potest*? *Brevi appunti su intelligenza Artificiale e responsabilità penale*, in *Discrimen*, 2019, pp. 1-23.

CAPPELLINI A., *Profili penalistici delle self-driving cars*, in *Diritto penale contemporaneo - rivista trimestrale, 2019*, fasc. 2, pp. 325-353.

CASONATO C., MARCHETTI B. *Prime osservazioni sulla proposta di regolamento dell'unione europea in materia di intelligenza artificiale*, in *Biolaw journal - rivista di biodiritto*, n. 3, 2021, pp. 415-437.

COLAROCCO V., *Cybersecurity e intelligenza artificiale: la sfida della guida autonoma e l'intervento dell'ENISA*, in *Diritto di internet,* 2021, consultabile alla pagina web: < https://dirittodiinternet.it/cybersecurity-intelligenza-artificiale-la-sfida-della-guida-autonoma-lintervento-dellenisa/ >.

Commissione europea (a cura di), Comunicazione al Parlamento europeo, al Consiglio europeo, al Consiglio, al comitato economico e sociale europeo e al Comitato delle regioni, *Verso la mobilità automatizzata: una strategia dell'UE per la mobilità del futuro,* COM (2018) 283 final.

Commissione europea (a cura di), Comunicazione al Parlamento europeo, al Consiglio, al comitato economico e sociale europeo e al Comitato delle regioni, *Libro bianco sull'intelligenza artificiale. Un approccio europeo e alla fiducia,* (COM) 65 final.

Consiglio europeo (a cura di), Decisione quadro: 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri - Dichiarazioni di alcuni Stati membri sull'adozione della decisione quadro. Gazzetta ufficiale n. L 190 del 18/07/2002, disponibile alla pagina web: < https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32002F0584 >.

Convenzione di Vienna sulla circolazione stradale, conclusa a Vienna l'8 novembre 1968.

DOUMA F., PALODICHUK S. A., *Criminal liability issues created by autonomous vehicles,* in *Santa Clara Law Review 1157,* n. 4 vol. 52, 2012, consultabile alla pagina web*:* < https://digitalcommons.law.scu.edu/lawreview/vol52/iss4/2 >.

FIORELLA A., VALENZANO A.S., *Colpa dell'ente e accertamento,* Roma, Sapienza Università editrice, 2016, in specie cap. II*, La colpa dell'ente per la "difettosa organizzazione" nel sistema italiano,* in *Colpa dell'ente e accertamento,* pp. 53 – 60,

FIORELLA A., *Responsabilità penale del tutor e dominabilità dell'intelligenza artificiale. Rischio permesso e limiti di autonomia dell'intelligenza artificiale* in *Il diritto nell'era digitale,* GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie pp. 651 – 664.

HALLEVY G., *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*," in *Akron Intellectual Property Journal*: Vol. 4: Iss. 2, article 1, 2010,

consultabile alla pagina web: <https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/ >.

JUHASZ A., *The Legal Framework of Autonomous Driving in Germany*, in *Multi Science - XXXIII. MicroCAD International Multidisciplinary Scientific Conference University of Miskolc*, 23-24 May, 2019, consultabile alla pagina web: < https://www.uni-miskolc.hu/~microcad/cd2019/e1/E_Juhasz_Agnes.pdf >.

LAGIOIA F., *L'intelligenza artificiale in sanità: un'analisi giuridica,* Torino, Giappichelli, 2020.

LIMA D., *Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law*, in *South Carolina L. Rev.*, 69, 2018, pp. 677 – 696.

LOSANO M. *Il progetto di legge tedesco sull'auto a guida automatizzata*. Appendice: il progetto di legge e le relazioni illustrative, in *Diritto dell'informazione e dell'informatica*, xxxiii, 2017, pp. 1-25.

MAGRO M. B., *Decisione umana e decisione robotica: un'ipotesi di responsabilità da procreazione robotica*, in *Legislazione penale* (*Giustizia penale e nuove tecnologie),* 10 maggio 2020, pp. 1-22.

MAROTTA M., *La Francia avvia ufficialmente la legislazione sulla guida autonoma,* in *Diritto di internet*, 2021, consultabile alla pagina web: < https://dirittodiinternet.it/la-francia-avvia-ufficialmente-la-legislazione-sulla-guida-autonoma/ >.

PAGALLO U., *Saggio sui robot e il diritto penale* in *Scritti in memoria di Giuliano Marini*, VINCIGUERRA S., DASSANO F. (a cura di), Napoli, 2010, in specie pp. 595 – 607.

PANATTONI B., *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Il diritto dell'informazione e dell'informatica* - n. 2 – 2021, pp. 317 – 368.

Parlamento europeo e Consiglio (a cura di), Regolamento (UE) 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Parlamento europeo e Consiglio (a cura di), Regolamento Ue 2018/858 del 30 maggio 2018 relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli.

Parlamento europeo e Consiglio (a cura di), Regolamento (UE) 2019/2144 del 27 novembre 2019, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010,(UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011,(UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012,(UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 della Commissione.

Parlamento europeo e Consiglio europeo (a cura di), Proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale e modifica di alcuni atti legislativi dell'unione, COM (2021) 206 final.

Parlamento europeo (a cura di), Risoluzione del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)).

Parlamento europeo (a cura di), Risoluzione del 6 ottobre 2021 sul quadro strategico dell'UE per la sicurezza stradale 2021-2030. Raccomandazioni sulle prossime tappe verso l'obiettivo "zero vittime" (2021/2014(ini)).

Parlamento europeo e Consiglio (a cura di) Regolamento (UE) 2022/2065, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

PELLEGATTA S., *Il valore probatorio della scatola nera installata sui "veicoli connessi" al vaglio della giurisprudenza: verso un regime speciale di responsabilità civile*, in *Diritto di internet*, fascicolo n.1, 2022, pp. 103 – 118.

PICOTTI L., *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, in *Studi in onore di Antonio Fiorella*, vol. I, CATENACCI M., NICO D'ASCOLA V., RAMPIONI R. (a cura di), *Romatre-press*, 2021, in specie pp. 813 – 837.

PICOTTI L., *Veicoli a guida autonoma e responsabilità penale*, in *Veicoli a guida autonoma. Veicoli a impatto zero. Regole, intelligenza artificiale, responsabilità*, CASSANO G., PICOTTI L., (a cura di), Pacini Giuridica, 2023, in specie, pp. 255 – 269.

PICOTTI L., PANATTONI B., *Traditional Criminal Law Categories and AI: Crisis or Palingenesis*? (*International Colloquium Section I*, Siracusa, 15-16 *September* 2022), in *R.I.D.P. - Revue Internationale de Droit Pénal*, Vol. 94, issue 1, 2023.

PIERGALLINI C., *Danno da prodotto e responsabilità penale. Profili dogmatici e politico-criminali,* Milano, Giuffrè, 2004.

PIERGALLINI C., *La responsabilità del produttore: una nuova frontiera del diritto penale*? In *Diritto penale e processo*, n. 9, 2007, Milano, pp. 1125 – 1130.

PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato,* in *Rivista italiana di diritto e procedura penale*, fasc. 4, 2020, pp.1743 – 1772.

PRETE CAPASSO TORRE DI CAPRARA G., *Auto a guida autonoma e regole assicurative* in *Il diritto nell'era digitale,* GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie pp. 315 – 331.

PIERGALLINI S., *La responsabilità penale per eventi generati da sistemi di IA o da processi automatizzati,* in *Il diritto nell'era digitale,* GIORDANO R., PANZAROLA A., POLICE A., PREZIOSI S., PROTO M. (a cura di), Giuffrè, 2022, in specie pp. 712-726.

SAE International, *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, Standard J3016, 2014.

SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Rivista italiana di diritto e procedura penale,* n. 1, 2021, pp. 83 – 118.

SEARLE, J. *(1980). Minds, brains, and programs. Behavioral and Brain Sciences, 3(3),* pp. 417 – 424.

SURDEN H., *Machine Learning and Law*, in *Washington Law Review*, Vol. 89, No. 1, 2014, pp. 87 – 115.

TEDESCO A.P., *Smart mobility e rischi satellitari e informatici: i possibili scenari di allocazione della responsabilità civile*, in *Diritto del commercio internazionale*, n.4, 2019, pp. 801 – 824.

TURING A.M., *Computing Machinery and Intelligence*, 1950, *Mind 4,* pp. 433 – 460**.**

United nation (ed.), ECE/TRANS/WP.29/2020/79: *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.*

United nation (ed.), ECE/TRANS/WP.29/2020/80: *Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system.*

United nation (ed.), ECE/TRANS/WP.29/2020/81: *Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems***.**

United nation (ed.), ECE/TRANS/WP.29/2022/59/Rev.1: *Proposal for the 01 series of amendments to UN Regulation No. 157* (Automated Lane Keeping Systems).

ZARGAR S. T., JOSHI J., TIPPER D., *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*, in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, Fourth Quarter 2013, pp. 2046 – 2069, doi: 10.1109/SURV.2013.031413.00127.

SITOGRAFIA

Ansa, *Auto: è realtà l'Arena del futuro, test ricarica elettriche,* Torino, 2 dicembre 2021, consultabile alla pagina web: <https://www.ansa.it/canale_motori/notizie/attualita/2021/12/02/auto-e-realta-larena-del-futuro-test-ricarica-elettriche_b7f98c8a-1f1a-4862-aea5-b957ccfac0a5.html >,).

BMDV, Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtver- sicherungsgesetzes – Gesetz zum autonomen Fahren, 08 febbraio 2021, consultabile alla pagina web: < https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile >.

MAGNANI A., *Parlamento Ue approva stop a vendita auto a benzina e diesel dal 2035, si spacca maggioranza*, in *Il sole 24 ore,* 9 giugno 2022, consultabile al seguente link: < https://www.ilsole24ore.com/art/salta-riforma-mercato-ue-emissioni-gas-serra-attesa-voto-auto-AEOFiYeB?refresh_ce=1 >.

MCCARTHY J., *What Is Artificial Intelligence*? (Nov. 12, 2007), consultabile alla pagina web: < https://perma.cc/N5YZ-QYS7 > (Ultimo accesso in data 26/08/2022).

Moveo by Telepass,: *Perché l'asfalto che ricarica potrebbe spingere il mercato delle auto elettriche,* 26 luglio 2022, consultabile alla pagina web: <https://moveo.telepass.com/asfalto-ricarica-auto-elettriche/#rb-Asfalto-che-ricarica-la-nuova-tecnologia-al-servizio-dei-veicoli-elettrici >.