Diritto e politica dei trasporti

Rivista semestrale *open access* di dottrina, giurisprudenza e documentazione

Fascicolo 1/2025

Con i contributi di

Fernando Elorza Guerrero, Manuel Guillermo Sarmiento García, Emilio Romualdi, Christina Zournatzi, Lucrezia Magli, Nicola Pierpaolo Barbuzzi, Gino Fontana, Martina Baltuzzi, Vincenzo Palo, Paolo Felix Iurich, Marco Di Giugno, Paolo Sabra Piazza, Francesca Di Monaco, Emma Maresca

ISSN 2612-5056

LUISS

La Rivista è promossa dall'Osservatorio sul Trasporto Aereo "Antonio Catricalà" Luiss G. Carli, anno 8, n. 14 (I-2025), ed è registrata presso il Tribunale di Roma al n. 150/2018 del 19 settembre 2018.
The Journal is published by the Air Transport Observatory "Antonio Catricalà" at Luiss G. Carli, and it is registered at the Court of Rome under No. 150/2018 on 19 September 2018.
Direttore responsabile/Editor-in-Chief: Prof. Francesco Gaspari, Università degli Studi "G. Marconi" di Roma e Osservatorio sul Trasporto Aereo "Antonio Catricalà" Luiss G. Carli
http://www.dirittoepoliticadeitrasporti.it/
La rivista è promossa dall'Osservatorio sul Trasporto Aereo "Antonio Catricalà" Luiss G. Carli, anno 7, n. 12 (I-2024)

ISSN 2612-5056
Luiss University Press

Diritto e politica dei trasporti è una Rivista online e open-access, classificata dall'Anvur tra le riviste di classe A nell'area disciplinare 12 (Scienze giuridiche), indicizzata da DOAJ – Directory of Open Access Journals (https://doaj.org/) e da ERIH PLUS – European Reference Index for the Humanities and Social Sciences (https://kanalregister.hkdir.no).
Diritto e politica dei trasporti is an online,open-access, Anvur class A Journal, subject area 12 (Law). It is indexed in DOAJ – Directory of Open Access Journals (https://doaj.org/) and in ERIH PLUS – European Reference Index for the Humanities and Social Sciences (https://kanalregister.hkdir.no).

Grafica e impaginazione: Ente Nazionale Aviazione Civile e Luiss University Press
Pubblicato nel mese di ottobre 2025

Modalità di invio dei contributi
Chiunque può inviare il suo scritto in file ".doc" alla direzione della Rivista (direzione@dirittoepoliticadeitrasporti.it) o alla Segreteria editoriale (redazione@dirittoepoliticadeitrasporti.it) unitamente alle seguenti informazioni:
1) i dati personali dell'Autore, la qualifica accademica e/o professionale, nonché i recapiti;
2) un abstract in lingua inglese e uno in lingua italiana, che non deve superare le 1.000 battute ciascuno (spazi inclusi), 5 parole chiave;
3) l'autorizzazione al trattamento dei dati personali forniti dall'Autore alla Rivista, ai sensi del Regolamento UE 679/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016 (Regolamento Generale sulla Protezione dei Dati), nonché del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);
4) una formale richiesta di pubblicazione, che si intende implicitamente inclusiva delle seguenti dichiarazioni da parte dell'Autore:
a) che il lavoro sia esclusivo frutto dell'Autore e sia stato redatto nel rispetto delle norme del diritto d'autore e della riservatezza delle informazioni anche con riferimento alle fonti utilizzate;
b) che l'Autore non ha già pubblicato ovvero non ha chiesto la pubblicazione dello scritto ad altra rivista, salvo espresso consenso del Direttore o del Comitato di direzione;
c) che le posizioni espresse impegnano l'Autore e non la Rivista;
d) che l'Autore esonera la Rivista da ogni responsabilità con riguardo alla scelta di pubblicare lo scritto, non pubblicarlo o di rimuoverlo dalla rivista in caso di violazione di norme di legge o nei casi previsti dal Codice etico adottato dalla Rivista;
e) che l'Autore rispetta tutte le altre indicazioni contenute nel Codice etico della Rivista.
Il Direttore o il Comitato di direzione si riserva di non pubblicare i contributi che non rispettino le caratteristiche editoriali richieste. Gli autori sono gli unici responsabili dei contenuti dei loro scritti. Non si accettano scritti anonimi.
Tutti i contributi sono pubblicati in formato PDF. Si possono stampare gli "estratti" con le indicazioni tipografiche della Rivista e con la data di pubblicazione.
I criteri redazionali sono indicati nell'apposita sezione della Rivista.

Submission of contributions
Manuscripts are sent in ".doc" format to the Journal's Executive Editors (direzione@dirittoepoliticadeitrasporti.it) or to the Editorial Staff (redazione@dirittoepoliticadeitrasporti.it). The e-mail includes the following information:
1) Author's personal data, academic and/or professional qualifications, contacts;
2) an abstract in Italian language and an abstract in English of not more than 1.000 characters each (including spaces), 5 key words;
3) authorization to process personal data provided by the Author to the Journal in accordance with Regulation EU 679/2016 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), and Legislative Decree 30 June 2003, No. 196 (Italian Personal Data Protection Code);
4) request to publish the manuscript, which implicitly includes the following declarations by the Author:

a) that the manuscript is the result of research activity conducted by the Author and that it complies with the rules on intellectual property rights and on confidentiality of information, also with regards to the sources used;
b) that the manuscript has not been already published nor has been submitted for publication to another Journal, except for express consent by the Editor-in-Chief or the Executive Editors;
c) that the views expressed in the publication are the sole responsibility of the Author and do not reflect the views of the Journal;
d) that the Author explicitly exonerates the Journal of all responsibility with regards to the choice to publish the manuscript, not to publish it, as well as to remove it from the Journal in the event of a breach of any legal provisions or in the cases laid down in the Code of Ethics adopted by the Journal.
e) that the Author abides by all other provisions of the Journal's Code of Ethics.
The Editor-in-Chief and the Executive Editors reserve the right not to publish contributions that do not comply with the editorial criteria. Authors only are exclusively responsible for the contents of their writings. Anonymous writings are not accepted.
All contributions are published in PDF format. Off-prints may be downloaded and printed.
Editorial criteria are available online, in the relevant section of the Journal.

Diritto e politica dei trasporti

Fascicolo 1/2025 anno 8, n. 14

Cybersecurity e privacy in movimento: verso una nuova epistemologia dei dati e della responsabilità nella *smart mobility**

Nicola Pierpaolo Barbuzzi

Docente a contratto di Diritto privato presso l'Universitas Mercatorum di Roma, avvocato, PhD's

Gino Fontana

Avvocato, PhD

Abstract

Cybersecuity and privacy in motion: towards a new epistemology of data governance and responsibility in smart mobility ecosystem.

In the context of the pervasive digital transformation within the automotive industry, the issue of privacy and cybersecurity emerges as a complex, multifaceted challenge that converges legal and technical dimensions into an integrated framework. This evolving scenario necessitates a critical reassessment of traditional regulatory paradigms, prompting an ontological inquiry into the nature of data and its intrinsic value. From a legal perspective, blockchain technology presents itself as a pivotal epistemic tool capable of ensuring transparency, immutability, and trust within digital systems, thereby serving as a mechanism that bridges the gap between technological advancement and the safeguarding of individual autonomy, a cornerstone of human rights. Furthermore, the interconnection of digital mobility systems demands an interdisciplinary approach that reconciles the imperative for innovation with the need for flexible governance structures. In this regard, blockchain, in conjunction with evolving regulatory strategies, emerges as a paradigmatic solution, offering a balanced approach that protects privacy while fostering technological development. This framework lays the foundation for a secure and sustainable digital mobility ecosystem, where legal safeguards are aligned with technological progress.

* Sottoposto a referaggio. Nicola Pierpaolo Barbuzzi è autore dei paragrafi 1, 2, 4, 5 del presente scritto; Gino Fontana è autore del paragrafo 3.

Nel contesto dell'incessante permeazione digitale nell'industria automobilistica, la problematica della privacy e della cybersicurezza si rivela come una sfida polimorfica in cui confluiscono dimensioni giuridiche e tecnico-informatiche in un intreccio sincretico. Tale scenario impone una decostruzione critica dei tradizionali paradigmi normativi richiamando una riflessione ontologica sulla natura dei dati e sul loro valore intrinseco. In quest'ottica, la tecnologia blockchain *si propone quale strumento epistemico, capace di infondere trasparenza, immutabilità e fiducia nei sistemi digitali, fungendo da ponte fra il divenire tecnologico e la preservazione dell'autonomia individuale, fondamento di ogni diritto. L'interconnessione dei sistemi di mobilità digitale, infine, esige un approccio interdisciplinare che sappia armonizzare l'impulso innovativo con una* governance *flessibile, delineando così nuovi orizzonti di sicurezza in cui la* blockchain*, in sinergia con strategie normative rinnovate, rappresenta la risposta paradigmatica per il connubio tra sviluppo tecnologico e protezione della sfera privata, aprendo la via ad una mobilità digitale sostenibile e sicura.*

Keywords: smart mobility, privacy, cybersecurity, blockchain, IoT.

Parole chiave: mobilità intelligente, privacy, cybersecurity, blockchain, IoT.

1. Introduzione

L'ibridazione della dimensione umana con quella tecnologica non poteva non coinvolgere l'automobile, dono di un ben noto spirito maligno[1], in un'epoca in cui veicoli connessi, cooperanti e a guida autonoma iniziano a guadagnare sempre maggiori fette di mercato, ridefinendo la cornice concettuale della mobilità. Se in una prima fase la rivoluzione tecnologica è stata in grado di trasformare i sapiens in "sapiens digitalis"[2], ora anche gli strumenti tecnologici in uso al *sapiens* diventano "intelligenti", acquisendo capacità cognitive autonome, evolvendo in sistemi cyber-fisici in grado di interagire con l'ambiente esterno e con gli esseri umani in modo dinamico, contestuale

1. "Ma ricordate, anche se il dono è meraviglioso e rende migliore la vita di quasi tutti (eccetto, con il senno di poi, di quelli che vengono scelti come vittime), che se qualcuno rifiuta il dono e la maggior parte delle persone lo accetta, la vita di questa persona sarebbe molto peggiore di quella che era prima che il dono venisse offerto!", G. CALABRESI, *Il dono dello spirito maligno. Gli ideali, le convinzioni, i modi di pensare nei loro rapporti col diritto* (a cura di), trad. di C. Rodotà, Milano, 1985.
2. P. BENANTI, *La necessità di una algoretica*, 2021, https://www.osservatoreromano.va/it/news/2021-12/quo-289/la-necessita-di-una-algoretica.html (ultimo accesso 04/04/2025).

ed adattivo. Tale trasformazione segna, tuttavia, una frattura epistemologica con il paradigma classico della tecnologia, quale mero prolungamento della volontà umana, configurando un nuovo assetto ontologico in cui l'intelligenza artificiale, qualora applicata agli autoveicoli, attraverso processi di *machine learning*[3] e *deep learning*[4], consente a questi di apprendere dall'esperienza di guida e modificare i propri schemi operativi senza un intervento diretto del programmatore. Nel suo impianto originario, era l'etimologia stessa del termine macchina, dal greco *μηχανή* – mēkhanē, ad indicare la strumentalità dell'invenzione asservita alle necessità umane, padroneggiata da quest'ultimo attraverso la *τέχνη* – téchne; all'attualità la macchina *sapiens* pur restando, almeno per il momento, concettualmente vincolata ad un sistema di controllo e responsabilità umana, è in grado di emanciparsi nel perimetro etico e giuridico imposto, proponendosi come uno strumento intelligente in grado di aggiornarsi automaticamente *over the air*, autoregolarsi, evolversi apprendendo dai dati raccolti e risolvere problemi complessi come nel caso dei veicoli a guida autonoma, manifestando, al tempo stesso, capacità predittive e decisionali che, di fatto, ridefiniscono il concetto stesso di *liability* nel contesto della *smart mobility* ed ancora più in generale in quello delle *smart city*. Gli autoveicoli, immersi nell'infosfera, attesa la progressiva virtualizzazione della fisicità, saranno in grado di cooperare con oggetti privati della loro connotazione fisica, iniziando ad essere concettualmente "concepiti indipendentemente dal loro supporto materiale"[5]. Sul piano sistemico, allargando la lente analitica, ciò che sta mutando è il processo di validazione dei comportamenti, quel meccanismo di fiducia che classicamente

3. Il *machine learning* è una disciplina dell'intelligenza artificiale che si occupa dello sviluppo di algoritmi capaci di apprendere automaticamente dai dati, migliorando progressivamente le proprie prestazioni senza essere esplicitamente programmati per ogni singolo compito. Alla base di questo approccio vi è l'idea che i sistemi informatici possano identificare schemi, correlazioni e regolarità all'interno di grandi insiemi di informazioni, affinando la propria capacità decisionale attraverso l'esperienza.
4. Il *deep learning* è un ambito dell'intelligenza artificiale che si sviluppa all'interno dell'apprendimento automatico, e si concentra sull'addestramento di reti neurali artificiali per risolvere compiti complessi. Questo approccio prende ispirazione dal cervello umano, cercando di replicarne in forma semplificata il funzionamento: così come i neuroni biologici lavorano insieme per elaborare informazioni, anche le reti neurali artificiali sono composte da nodi interconnessi che collaborano per analizzare e interpretare i dati. A rendere il *deep learning* particolarmente potente è la sua capacità di apprendere in modo autonomo rappresentazioni astratte e stratificate dei dati. Questo avviene grazie alla struttura multilivello delle reti, dove ogni strato successivo elabora informazioni sempre più complesse. Il processo di apprendimento si basa in genere su grandi quantità di dati etichettati; durante l'addestramento, il sistema cerca di minimizzare l'errore tra le sue previsioni e le risposte corrette, modificando progressivamente i parametri interni – come pesi e *bias* – attraverso un meccanismo noto come *backpropagation*, che consente di correggere gli errori in modo efficiente. Tuttavia, il *deep learning* non si limita solo all'apprendimento supervisionato. Esistono anche tecniche che permettono alla rete di imparare da dati non etichettati, scoprendo autonomamente strutture o regolarità nei dati. È il caso, ad esempio, degli *autoencoder* o delle reti generative avversarie (GAN), utilizzate per compressione, generazione o rilevamento di anomalie.
5. Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

veniva deputato ad organi di controllo statuali, che oggi, attraverso i sistemi di controllo distribuiti, come nel caso della *blockchain*, consentono di trasformare l'autovettura connessa o autonoma da mero mezzo meccanico di trasporto ad un entità computazionale distribuita, parte di una rete neurale globale che raccoglie elabora e condivide dati in tempo reale, anche biometrici del conducente, dialogando e cooperando con altre infrastrutture intelligenti e con altri veicoli, in un orizzonte di *vehicle-to-evertyting* (V2X). In una prospettiva del genere è evidente come l'autovettura da mero strumento asservito alle umane necessità si trasformi in un partner cognitivo algoritmico, in grado di prendere decisioni in situazioni di emergenza, anche predittivamente, in tempi decisamente più performanti, rispetto ai classici tempi di reazione umana.

2. La transizione tecnologica degli autoveicoli e dei sistemi di connessione e raccolta dei dati

L'evoluzione del grado di autonomia dei veicoli è stato oggetto di approfondite analisi e classificazioni scientifiche, configurandosi come un tema di notevole interesse teorico e applicativo. Inizialmente, le indagini si sono concentrate sull'impiego del "locus of control" e sull'esame delle modalità mediante le quali le informazioni raccolte venivano trasmesse al conducente, stabilendo una scala progressiva che, partendo da un livello 1 in cui l'intero carico operativo della guida è demandato all'essere umano, culmina in un ipotetico livello 10, ove il sistema informatico si fa carico di tutte le operazioni, comprendendo la facoltà di comunicare le decisioni adottate[6]. Successivamente, il filone di studi si è orientato verso una definizione dell'automazione in termini di relazione tra il grado di intelligenza e l'autonomia all'interno del complesso sistema uomo-macchina[7], per evolversi in una trattazione che classifica il livello di autonomia sulla base dell'efficacia del controllo in tempo reale del veicolo. In questo contesto, si evidenzia il passaggio da un livello 0 "manual control", nel quale il conducente non solo esegue ogni operazione – dal monitoraggio dello stato sistemico alla formulazione e selezione di specifiche opzioni prestazionali, fino alla loro concreta implementazione – a un grado di "full automation", ove il sistema operativo realizza autonomamente l'intera sequenza di azioni, escludendo ogni possibile intervento dell'utente[8]. Il legislatore italiano, pur in presenza di una più graduale tassonomia, ha privilegiato una classificazione ridotta in due ampie categorie, distinguendo nettamente i veicoli a guida autonoma da quelli a guida assistita. Nel dettaglio, il primo tipo è definito come "dotato di tecnologie capaci di adottare e attuare comportamenti di guida senza l'intervento attivo del guidatore, in determinati ambiti stradali e condizioni esterne", mentre il

6. Cfr. T.B. SHERIDAN, W.L. VERPLANK, *Human and computer control of undersea teleoperators*, Arlington, 1978.
7. Cfr. V. RILEY, *A general model of mixed-initiative human-machine systems*, 1989, https://doi.org/10.1177/154193128903300227 (ultimo accesso 06/04/2025).
8. Cfr. M.R. ENDSLEY, D.B. KABER, *Level of automation effects on performance, situation awareness and workload in a dynamic control task*, in *Ergonomics*, 1999, v. 42(3), p. 462 ss.

secondo è descritto come "dotato di uno o più sistemi di assistenza alla guida, che vengono attivati da un guidatore al solo scopo di attuare comportamenti di guida da egli stesso decisi e che comunque necessitano di una continua partecipazione attiva da parte del conducente alla attività di guida"[9]. Di conseguenza, come ampiamente indicato dalla letteratura scientifica, nel caso dei veicoli a guida assistita, il conducente dovrà mantenere un monitoraggio costante del sistema e garantire, attraverso un controllo sia laterale che longitudinale, la disponibilità ad assumere il pieno controllo del veicolo in ogni istante, qualora se ne renda necessaria l'interruzione del circuito automatizzato[10].

Tuttavia, l'automazione sia essa completa o solo quale guida assistita, necessita per poter funzionare di una infrastruttura che consenta al veicolo di dialogare con altri veicoli o con la casa produttrice. Tanto si è reso molto più praticabile a partire dal 2018, anno che segna il passaggio alla connettività a bassa latenza e banda larga del 5G; grazie a tale infrastruttura i veicoli, dotati di sistemi di raccolta dati connessi alla rete, sono in grado di coadiuvare in maniera più performante il conducente nell'esperienza di guida, ma anche la casa produttrice di parametri utili alla verifica del funzionamento dell'autoveicolo ai fini della manutenzione, presentandosi così come una delle più promettenti applicazione pratiche dell'IoT (*Internet of Things*) ossia di quella nuova generazione di dispositivi connessi alla rete Internet in grado di scambiarsi ed elaborare dati[11]. Sarà, pertanto, possibile definire "connesso" quel veicolo in grado di utilizzare un insieme di tecnologie di comunicazione per scambiare informazioni direttamente con altri veicoli mediante una infrastruttura dedicata o mediante servizi *cloud*. Ad oggi, non esiste una vera e propria classificazione delle connessioni per i veicoli, essendo distinte solamente sulla scorta delle caratteristiche funzionali: l'interoperabilità, l'adeguatezza ad applicazioni di sicurezza attiva nella guida, l'interazione generalizzata con il veicolo. Nel dettaglio, l'interoperabilità attiene alla capacità assunta dal veicolo di poter dialogare con altri interlocutori in diversi contesti attraverso un unico linguaggio e per la stessa applicazione, come nel caso di veicoli di diverse case produttrici in grado di dialogare – senza soluzione di continuità – con sistemi a bordo strada. Il secondo requisito dell'adeguatezza attiene alla capacità della tipologia di connessione di rispondere agli standard imposti dalle applicazioni (reti dedicate con bande di frequenza dedicate), mentre il terzo requisito attiene la capacità della connessione di prelevare e fornire dati ad applicazioni e

9. D.M. n. 70 del 28/02/2018 (Smart Road).
10. Cfr. T.M. GASSER, D. WESTHOFF, *BASt-study: Definitions of automation and legal issues in Germany, in Human Factors Evaluation of Level 2 And Level 3 Automated Driving Concepts*, U.S. Department of Transportation of National Highway Traffic Safety Administration, 2014, https://www.nhtsa.gov/sites/nhtsa.gov/files/812043_hfevaluationlevel2andlevel3automateddrivingconceptsv2.pdf (ultimo accesso 16/10/2025).
11. Cfr. M.B.M. NOOR, W.H. HASSAN, *Current research on Internet of Things (IoT) security: A survey, in Comput. Netw.*, 2019, https://doi.org/10.1016/j.comnet.2018.11.025 (ultimo accesso 05/04/2025); cfr. G. PIGNATARO, *Self-driving cars, gestione del rischio e accountability: la funzione preventiva della responsabilità civile nella legislazione europea*, *questa Rivista*, 2024.

strumentazione del veicolo stesso, includendo anche la capacità di modificare il settaggio degli applicativi e aggiornare il *software* in modalità protetta[12]. Potremo quindi, sulla scorta della diversa tipologia di connessione, distinguere in servizi tradizionali (livello C-0, quali connessione ad Internet, assistenza al traffico, scatole nere in cui lo scambio di dati è regolato dalle condizioni contrattuali tra l'utilizzatore ed il fornitore del servizio), servizi di pubblico interesse (livello C-1, i quali rispondendo al requisito della interoperabilità e senza la necessità dell'utilizzo di reti dedicate, generano benefici al guidatore come nel caso del *Public Safety Answering Point*), servizi legati alla sicurezza (livello C-2, in cui i veicoli cooperano tra di loro scambiandosi dati dinamici come nel caso dei V2V o V2l, *vehicle to infrastructure*), servizi generalizzati integrati con il veicolo (livello C-3, in cui vi è una connessione costante del veicolo con il *cloud*). Chiarito il concetto di connessione, appare necessario individuare quali siano gli strumenti necessari alla raccolta dei dati. La letteratura individua due macro categorie di sensori in base al tipo di informazione raccolta: da un lato i sensori extroceptivi, progettati per raccogliere dati dall'ambiente esterno al veicolo e sensori proprioceptivi che monitorano lo stato interno del veicolo. Nella prima categoria a titolo esemplificativo possiamo individuare sia le telecamere ad alta risoluzione, in grado di interpretare i segnali stradali, che i radar e LiDar utilizzati, i primi, per determinare la distanza e la velocità degli oggetti attraverso l'emissione di onde radio, mentre i secondi per costruire mappe tridimensionali attraverso l'utilizzo di impulsi laser[13]. A questi si aggiungono i sensori ultrasonici, impiegati per le operazioni a corto raggio, come nel caso dei parcheggi. Diverso è l'impiego dei sensori proprioceptivi come quelli integrati nel motore e nelle componenti meccaniche, utilizzati nell'ambito della diagnostica predittiva e alla manutenzione proattiva o i sensori TPMS avanzati che monitorano pressione, temperatura ed usura degli pneumatici. Discorso a parte meritano i sensori integrati nell'abitacolo e nei sedili che monitorano la postura del conducente e dei passeggeri, consentendo l'attivazione ottimale degli airbag in caso di collisione, nonché quelli del *Driver Monitoring System* (sensori di monitoraggio del conducente) i quali attraverso telecamere a infrarossi e sensori posizionati sul volante o integrati nei sedili, analizzano il comportamento facciale e biometrico del guidatore, identificando segnali precoci di affaticamento o distrazione, attivando avvisi visivi, sonori o vibrazionali per richiamare l'attenzione. Ulteriore classificazione, attiene il principio operativo dei sensori, potendosi distinguere tra dispositivi attivi che emettono un segnale e ne misurano il ritorno (radar e LiDar) e dispositivi passivi come ad esempio le telecamere che si limitano a rilevare le informazioni presenti nell'ambiente. I dati raccolti dai sensori possono, a seconda della tecnologia veicolare, essere inseriti in sistemi complessi di analisi come

12. AA.VV., *Automatica. Il futuro prossimo dell'auto: connettività e automazione*, Centro studi Fondazione Filippo Caracciolo, 2017, https://fondazionecaracciolo.aci.it/app/uploads/2022/05/Studio_Auto_Autonoma_web.pdf (ultimo accesso 6/04/2025).
13. Cfr. B. LANDONI, *Utilizzo del LiDAR per il rilevamento della profondità in applicazioni automotive*, 2021, https://eipro.futuranet.it/2021/09/18/utilizzo-del-lidar-per-il-rilevamento-della-profondita-in-applicazioni-automotive/ (ultimo accesso 04/04/2025).

quelli dell'*Adaptive Cruise Control* (ACC) ed il *Lane-Keeping Assist* (LKA). Questi due sistemi rappresentano i pilastri della guida assistita[14], integrando tecnologie sofisticate che convergono in un sistema dinamico di percezione, elaborazione e intervento in tempo reale, incarnando una simbiosi tra *hardware* e algoritmi di intelligenza artificiale, rendendo la macchina un agente proattivo nell'ecosistema della mobilità. Nel caso dell'*Adaptive Cruise Control*, il funzionamento si fonda sulla raccolta e sull'elaborazione dei dati provenienti da una pluralità di sensori attivi e passivi, tra cui radar, LiDAR e telecamere ad alta risoluzione. Il radar, emettendo onde radio e analizzando il segnale riflesso, misura la distanza e la velocità del veicolo che precede, mentre le telecamere, affiancate da algoritmi di visione artificiale, forniscono informazioni complementari per l'identificazione degli oggetti e la lettura della segnaletica stradale. In alcuni sistemi avanzati, il LiDAR integra questi dati creando una mappa tridimensionale estremamente dettagliata dell'ambiente circostante. I dati acquisiti vengono quindi fusi tramite algoritmi di *sensor fusion*[15], che consentono di ottenere una rappresentazione accurata e robusta dello scenario in tempo reale. Sulla base di questa mappa digitale, il sistema stabilisce un ciclo continuo di *feedback*, modulando la potenza del motore e la frenata in modo da mantenere una distanza di sicurezza preimpostata, adattando progressivamente la velocità in risposta alle variazioni del traffico. L'intero processo, gestito da centraline elettroniche (ECU) dotate di capacità di *edge computing*, permette una risposta rapida e precisa, minimizzando il ritardo tra la percezione dell'ambiente e l'intervento sul veicolo[16]. Parallelamente, il *Lane-Keeping Assist* sfrutta una sofisticata combinazione di sensori ottici, prevalentemente telecamere frontali, e sensori inerziali. Le telecamere acquisiscono costantemente immagini della carreggiata e, mediante algoritmi di elaborazione delle immagini che impiegano tecniche di *deep learning* e trasformate di Hough[17], rilevano le

14. Cfr. M.C. GAETA, *Automazione e responsabilità civile automobilistica*, in *Resp. civ. prev.*, 2016, V, p. 1725 ss.
15. Cfr. J. KOCIC, N. JOVICIC; V. DRNDAREVIC, *Sensor and Sensor Fusion in autonomous vehicles*, in *26th Telecommunications Forum*, 2018, https://doi.org/10.1109/TELFOR.2018.8612054 (ultimo accesso 04/04/2025).
16. BOSCH, *Smart driver assistance systems*, 2020, https://www.bosch-mobility-solutions.com (ultimo accesso 18/03/2025); Cfr. S.F. VAROTTO; C. MONS, J.H. HOGEMA, M. CHRISTOPH, N. VAN NES; M.H. MARTENS, *Do adaptive cruise control and lane keeping systems make the longitudinal vehicle control safer? Insights into speeding and time gaps shorter than one second from a naturalistic driving study with SAE Level 2 automation*, in *Transportation Research Part C: Emerging Technologies*, 2022, https://www.sciencedirect.com/science/article/pii/S0968090X22001899?via%3Dihub (ultimo accesso 16/10/2025); Cfr. K.K. AKIYAMA, R. SHINKUMA, C. YAMAMOTO, M. SAITO, T. ITO, K. NIHEI, *Edge computing system with multi-LIDAR sensor network for robustness of autonomous personal-mobility, 2022*, in *IEEE 42nd International Conference on Distributed Computing Systems Workshops* (ICDCSW), Bologna, Italy, 2022, https://ieexplore.ieee.org/document/9951373 (ultimo accesso 16/10/2025), p. 290 ss.
17. La trasformata di Hough è un metodo computazionale per il riconoscimento di forme geometriche in immagini digitali, in particolare rette, cerchi ed ellissi. Il principio fondamentale consiste nella trasformazione dallo spazio cartesiano allo spazio dei parametri, dove una retta, invece di essere rappresentata nella forma $y = mx + q$, viene espressa come $\rho = x \cos\theta + y \sin\theta$, con ρ e θ che definiscono la distanza dall'origine e l'orientazione della retta. L'algoritmo procede accumulando evidenze nello spazio parametrico, dove ogni punto dell'immagine contribuisce a

linee di demarcazione delle corsie e analizzano la geometria della strada. Questi algoritmi, affinati da reti neurali convoluzionali (CNN)[18], sono in grado di distinguere in maniera affidabile le corsie, anche in presenza di condizioni di scarsa luminosità o deterioramento della segnaletica. Qualora il sistema individui una deviazione non intenzionale della corsia – ad esempio, a causa di una distrazione del conducente – il LKA attiva un protocollo di intervento: può emettere avvisi visivi sul cruscotto, segnali acustici o, nei modelli più avanzati, applicare correzioni automatiche all'angolo di sterzata per riportare il veicolo all'interno del limite di corsia. L'integrazione dei dati provenienti da sensori inerziali e giroscopi che monitorano la dinamica del veicolo, rafforza ulteriormente la precisione del sistema, garantendo una stabilità e una sicurezza ottimale in fase di correzione[19]. Ulteriormente, la letteratura scientifica sottolinea l'importanza l'utilizzo di strutture modulari e di architetture di controllo gerarchico in grado di separare la percezione dai livelli decisionali[20]. In questo contesto, i dati raccolti dai sensori vengono inizialmente processati in moduli di percezione, i quali generano una rappresentazione vettoriale dello scenario; successivamente, moduli di pianificazione e controllo elaborano strategie di intervento, determinando

molteplici rette candidate. Cfr. J.- Q. ZHANG; H.-B. DUAN; J.L. CHEN, A. SHAMIR, M. WANG, *HoughLaneNet: Lane detection with deep hough transform and dynamic convolution*, in *Computer & Graphics*, 2023, v. 116, https://doi.org/10.1016/j.cag.2023.08.012 (ultimo accesso 15/04/2025), p. 82 ss.; M. KARTHIKEYAN, S. SATHIAMOORTHY, V. MARUGANANDAM, *Lane Keep Assist System for an Autonomous Vehicle Using Support Vector Machine Learning Algorithm*, in *Innovative Data Communication Technologies and Application*, 2020, https://link.springer.com/chapter/10.1007/978-3-030-38040-3_11 (ultimo accesso 16/10/2025).

18. Le reti neurali convoluzionali (CNN) rappresentano una classe avanzata di modelli di apprendimento automatico progettati per elaborare dati strutturati spazialmente, come le immagini, attraverso un'architettura ispirata al funzionamento della corteccia visiva biologica. La loro struttura è caratterizzata da strati convoluzionali, che applicano filtri appresi per estrarre caratteristiche gerarchiche dai dati, riducendo la dimensionalità e preservando le informazioni spaziali rilevanti, seguiti da strati di pooling, che comprimono l'informazione migliorando l'invarianza alle trasformazioni. Tale approccio ha rivoluzionato il campo della computer vision, rendendo le CNN il paradigma dominante in molteplici settori, dalla guida autonoma alla diagnostica per immagini. Cfr. M. SAHAL, Z. HIDAYAT, R.A. PUTRA, M.A. RIZQUIFADHIILAH, F.D. SAPUTRA, *Lane Keeping System using Convolutional Neural Network for Autonomous Car*, 2023, in *14th International Conference on Information & Communication Technology and System (ICTS)*, https://ieeexplore.ieee.org/document/10330834 (ultimo accesso 16/10/2025).
19. Continental AG, *Autonomus mobility, automated driving*, 2020, https://www.continental.com (ultimo accesso in data 18/03/2025); J. JANAI, F. GÜNEY, A. ROSER, *Computer Vision for Autonomous Vehicles: Problems, Datasets and State-of-the-Art*, 2021, https://doi.org/10.48550/arXiv.1704.05519 (ultimo accesso 04/04/2025).
20. W. XUE-FANG; J. JINGJING, *A hierarchical control framework for autonomous decision-making systems: Integrating HMDP and MPC*, 2024, https://doi.org/10.48550/arXiv.2401.06833 (ultimo accesso 03/04/2025); cfr. E. ZHANG, J. HAUNG, Y. GAO, Y. LIU, Y. DENG, *A hierarchical perception decision-making framework for autonomous driving*, 2021, https://ideas.repec.org/a/taf/tcybxx/v8y2022i3p192-209.html (ultimo accesso 03/04/2025); cfr. D. KIM, R.R.L. MENDOZA, K.F.R. CHUA, M.A.A. CHAVEZ, R.S. CONCEPCION, R.R.P. VICERRA, *A Systematic Analysis on the Trends and Challenges in Autonomous Vehicles and the Proposed Solutions for Level 5 Automation*, 2021, https://ieeexplore.ieee.org/document/9731982 (ultimo accesso 03/04/2025).

la migliore traiettoria o il corretto intervento sui sistemi attuatori. Questo approccio a strati, incorporando meccanismi di *feedback* a breve e lungo termine, permette ai sistemi ACC e LKA di operare in maniera robusta anche in scenari complessi e dinamici, dove la rapidità di decisione è cruciale per la sicurezza. L'innovazione di questi sistemi risiede non solo nella capacità di integrare e analizzare dati in tempo reale, ma anche nell'adattamento continuo degli algoritmi, che attraverso tecniche di *machine learning* apprendono dalle esperienze operative. Ciò consente una progressiva ottimizzazione delle prestazioni, rendendo il veicolo sempre più capace di anticipare e rispondere alle variabili ambientali.

3. Tipologie di dati personali, *asset* digitali e *blockchain*

All'attualità, l'automobile da semplice mezzo di trasporto ha assunto sempre più i tratti di una entità capace di osservare, registrare e interpretare ogni gesto del conducente e dei passeggeri, generando un flusso ininterrotto di dati che vanno ben oltre la geolocalizzazione o la velocità media: di fatti, come anticipato, sensori di pressione sui sedili rilevano il peso dei passeggeri e quindi il numero degli individui presenti nell'abitacolo, microfoni integrati, spesso attivati da comandi vocali apparentemente innocui, sono in grado di captare conversazioni private, telecamere a infrarossi monitorano il livello di attenzione del guidatore attraverso il tracciamento oculare, mentre i sistemi di *infotainment* memorizzano cronologie di ricerca, *playlist* musicali e persino le preferenze dei ristoranti presso i quali ci si è fermati, costruendo un ritratto digitale intimo e pervasivo che alimenta un'"economia della sorveglianza" in cui il valore commerciale dei dati sovrasta il diritto alla riservatezza[21]. La raccolta sistematica e capillare dei dati all'interno e all'esterno dell'autovettura, molto spesso giustificata dalla necessità di migliorare l'esperienza di guida o garantire una maggiore sicurezza stradale, nasconde dinamiche di potere asimmetriche, laddove i produttori automobilistici, le compagnie assicurative o terze parti (dai fornitori di mappe alle agenzie pubblicitarie) potrebbero accedere ai *dataset* che includono, ad esempio, orari abituali di spostamento, percorsi preferiti, stili di frenata e addirittura gli stati emotivi (rilevati dall'analisi del tono vocale). In alcuni casi, come per i Model 3 e Y di Tesla, la *cabin camera* posizionata sopra lo specchietto retrovisore e funzionale al rilevamento dei segni di stanchezza del conducente (occhi chiusi, uso dell'apparecchio cellulare) è stata utilizzata per condividere nelle *chat* dei dipendenti della casa produttrice le immagini del conducente e dei trasportati senza un preventivo consenso[22]. I dati resi accessibili a soggetti terzi, non sufficientemente anonimizzati e nella loro

21. Cfr. T. ZARSKY, *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making*, in *Science, Technology, & Human Values, Special Issue: Governing algorithms*, 2016, p. 118 ss.

22. Cfr. S. STECKLOW, W. CUNNINGHAM, H. JIN, *Tesla workers shared sensitive images recorded by customer cars*, 2023, www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06 (ultimo accesso 13/04/2025); cfr. G.H. RUFFO, *Tesla Files: Huge Data Leak Shows Issues with Data*

forma non aggregata, contenenti metadati relativi al *timestamp* o alle coordinate GPS, potrebbero consentire di identificare sia i volti, le voci nonché i dettagli interni delle autovetture, violando il precetto contenuto nell'articolo 9 del Regolamento EU n. 679 del 2016 (*General Data Protection Regulation* - GDPR) il quale vieta espressamente il trattamento dei dati biometrici senza un consenso specifico dei soggetti interessati. La normativa europea in tema di privacy tenta di scongiurare l'avverarsi di scenari simili, attraverso l'imposizione di principi generali come quello della minimizzazione dei dati *ex* articolo 5 del GDPR. Tuttavia, il rigoroso impianto normativo comunitario si scontra con realtà applicative in cui il consenso dell'utente è spesso ridotto a una spunta verde cliccata frettolosamente su schermi *touchscreen* e sepolto in pagine e pagine di termini d'uso, scritti in un linguaggio giuridico inaccessibile[23]. Tanto accade, molto spesso, mentre i sistemi di *connected car* continuano a operare in modalità silenziosa, raccogliendo informazioni anche quando il veicolo è spento[24]. Di fatti, i veicoli connessi hanno sviluppato una sorta di doppia vita: quella ufficiale, fatta di comandi vocali e schermi luminosi, ed una segreta, fatta di registrazioni e rilevamento di dati che continuano a scorrere ininterrottamente. Lo spegnimento è solo apparente in quanto i sensori ed i sistemi telematici continuano a mantenere un'attenzione vigile, raccogliendo informazioni che vanno ben oltre la semplice manutenzione. In tale contesto l'utente è sempre più invisibile e la tecnologia che lo osserva si fa sempre più opaca, dovendosi considerare questa modalità silenziosa di funzionamento degli autoveicoli non come un dettaglio tecnico, ma una scelta progettuale *by design* che riflette un preciso rapporto di potere in cui l'opacità, progettata per eludere il diritto, non è un *bug* ma una *feature* dei sistemi di *data capitalism*, anzi meglio di *surveillance capitalism* che si appropria dell'esperienza umana e la usa come "materia prima da trasformare in dati sui comportamenti"[25]. Se alla modalità silenziosa si aggiungono la complessità dei sistemi tecnologici ed una frammentazione tale delle responsabilità tra produttori, fornitori di *software* e gestori di *cloud* tale da rendere quasi impossibile l'attribuzione di violazioni

Protection, SUA, Autopilot, and FSD, 2023, https://www.autoevolution.com/news/tesla-files-huge-data-leak-shows-issues-with-data-protection-sua-autopilot-and-fsd-215571.html (ultimo accesso 13/04/2025); cfr. J. MÖKANDER, J. MORLEY, M. TADDEO, L. FLORIDI, *Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitation*, in *Sci. Eng. Ethics*, 2021, https://doi.org/10.1007/s11948-021-00319-4 (ultimo accesso 16/10/2025); European Commission: Directorate-General for Research and Innovation, *Ethics of connected and automated vehicles – Recommendations on road safety, privacy, fairness, explainability and responsibility*, Publications Office, 2020, https://data.europa.eu/doi/10.2777/035239 (ultimo accesso 16/10/2025).

23. European Commission: Directorate-General for Research and Innovation, *Ethics of connected and automated vehicles – Recommendations on road safety, privacy, fairness, explainability and responsibility*, Publications Office, 2020, cit.
24. Cfr. U. PAGALLO, *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, 2017, https://edpl.lexxion.eu/article/EDPL/2017/1/7 (ultimo accesso 16/10/2025).
25. Cfr. S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019, p. 17 ss.

specifiche, emerge in tutta la sua drammaticità un vuoto di *accountability*, terreno di coltura delle partiche opache di cui ci stiamo occupando.
Anche il nodo della proprietà dei dati raccolti resta insoluto, acuendosi su questo tema lo scontro tra utenti e case automobilistiche. Da un lato, gli utenti, quali generatori primari delle informazioni, rivendicano un diritto di controllo sul proprio capitale digitale, dall'altro le case automobilistiche se ne attribuiscono la titolarità in quanto proprietà intellettuale derivante dall'ottimizzazione tecnologica. I veicoli connessi si trasformano in piattaforme di estrazione dati in grado di alimentare modelli produttivi basati sulla vendita di *insights* a terze parti, come nel caso della *partnership* tra Ford e Google, dove i dati aggregati di guida potranno essere utilizzati per affinare gli algoritmi predittivi del traffico (t*raffic prediction*) o per personalizzare la pubblicità in base alla geolocalizzazione[26]. Il modello europeo definito dal Regolamento UE n. 868 del 2022 (*Data Governance Act*) si muove nella direzione della promozione dell'"altruismo digitale" incoraggiando la condivisione volontaria di dati per il pubblico interesse[27] (ad esempio, la ricerca su incidenti stradali), ma senza intaccare i modelli di monetizzazione esistenti, lasciando senza risposta un'altra domanda fondamentale: chi dovrebbe beneficiare economicamente dei dati generati da un'auto connessa? Una possibile soluzione potrebbe emergere dall'utilizzo di tecnologie decentralizzate come la *blockchain* che permetterebbe agli utenti di certificare la proprietà dei dati attraverso *smart contract* e di decidere, in tempo reale, chi possa accedervi e per quali scopi in un più ampio orizzonte di "economia dei dati democratica" in cui ogni utente diventa il custode del proprio patrimonio informativo[28]. Difatti, la tecnologia *blockchain*, per la sua capacità di assicurare l'integrità, la sicurezza e la resistenza alle alterazioni dei dati in essa contenuti, si sta progressivamente affermando come strumento chiave nella tutela dei veicoli connessi. Recenti studi hanno dimostrato come l'implementazione di protocolli decentralizzati, esemplificata da soluzioni come il sistema VChain[29], possano neutralizzare minacce

26. https://corporate.ford.com/articles/products/ford-and-google-to-accelerate-auto-innovation.html (ultimo accesso 05/04/2025): "Ford and Google to accelerate auto innovation, reinvent connected vehicle experience. Ford and Google come together in first of its kind partnership to create unique services and capabilities for Ford and Lincoln customers".
27. Art. 2, n. 16, reg. UE n. 868 del 2022.
28. Cfr. K. EL FELLAH, I. EL AZAMI, A. EL MAKRANI, H. BOUIJIJ, O. EL AZZOUZY, *Revolutionizing Automotive Security: Connected Vehicle Security Blockchain Solutions for Enhancing Physical Flow in the Automotive Supply Chain*, in *Computer Systems Science and Engineerin*g, 2025, https://doi.org/10.32604/csse.2024.057754 (ultimo accesso 02/04/2025).
29. VeChain è una piattaforma *blockchain* progettata per migliorare la gestione della *supply chain* e dei processi aziendali, offrendo soluzioni per la tracciabilità dei prodotti e la prevenzione della contraffazione. Fondata nel 2015, VeChain utilizza una blockchain pubblica chiamata VeChainThor, che supporta *smart contract* e applicazioni decentralizzate. La piattaforma impiega un modello a doppio *token*: VET, utilizzato per trasferire valore sulla rete, e VTHO, impiegato per pagare le transazioni e alimentare le operazioni sulla *blockchain*. Grazie all'integrazione con dispositivi IoT, VeChain consente alle aziende di monitorare in tempo reale la produzione, la logistica e la distribuzione dei loro prodotti, garantendo trasparenza e autenticità lungo l'intera catena di approvvigionamento.

informatiche e garantire trasmissioni sicure, anche in condizioni di rete variabili[30]. La *blockchain*, grazie all'impiego di chiavi crittografiche univoche, consente di certificare l'origine dei dati e di salvaguardare la privacy, instaurando un meccanismo di autenticazione sofisticato in grado di garantire il controllo accurato di ogni transazione. Le attuali sperimentazioni si basano, da un lato, su meccanismi di consenso come il *Proof of Work* (PoW) e il *Proof of Elapsed Time* (PoET), i quali, supportati da hardware affidabili e sistemi di comunicazione dedicati (*Dedicated Short-Range Communication* - DSRC o reti cellulari), assicurano trasmissioni sicure anche in ambienti di rete complessi[31]; dall'altro, l'integrazione della *blockchain* con gli *smart contract* permette il rafforzamento dell'integrità delle catene di approvvigionamento, agevolando processi quali il leasing e la manutenzione[32]. La sicurezza dei dati sarebbe garantita dall'adozione di algoritmi avanzati come gli RSA (Rivest-Shamir-Adleman)[33]. Di fatti, mentre gli algoritmi simmetrici, quali AES, RC6 o *Blowfish*, si distinguono per la rapidità di esecuzione, le soluzioni asimmetriche come RSA offrono un livello di sicurezza superiore, sebbene a fronte di maggiori requisiti computazionali. Inoltre, l'adozione di tecniche emergenti come la crittografia a curva ellittica e quella post-quantistica, come dimostrato dalla letteratura scientifica[34], promette ulteriori progressi nella protezione dei dati senza compromettere l'efficienza operativa[35]. È di tutta evidenza come l'utilizzo della *blockchain* nei sistemi di veicoli connessi favorisca un rilevamento tempestivo delle minacce, contrastando efficacemente attacchi *zero-day*[36] e garantendo la continuità operativa, in quanto è proprio la natura decentralizzata del sistema ad eliminare i tradizionali punti

30. Cfr. A. KUMAR, A.S. YADAV, D.S. KUSHWAHA, *VChain: Efficient blockchain based vehicular communication protocol*, 2020, https://ieeexplore.ieee.org/document/9057801 (ultimo accesso 16/10/2025).
31. Cfr. F. AZAM, A. BIRADAR, N. PRIYADARSHI, S. KUMARI, S. TANGADE, *A review of blockchain based approach for secured communication in internet of vehicle (IoV) Scenario*, in *Second Int. Conf. Smart Technol. Comput., Elect. Electr. (ICSTCEE)*, 2021, https://ieeexplore.ieee.org/document/9708555 (ultimo accesso 16/10/2025), p. 1 ss.
32. Cfr. P. DUTTA, T-M. CHOI, S. SOMANI, R. BUTALA, *Blockchain technology in supply chain operations: Applications, challenges and research opportunities*, in *Transport. Res. Part E: Logist. Transport. Rev.*, 2020, https://www.sciencedirect.com/science/article/pii/S1366554520307183?via%3Dihub (ultimo accesso 16/10/2025).
33. Cfr. C. SILVA, V.A. CUNHA, P. BARRACA JÃO, R.L. AGUIAR, *Analysis of the cryptographic algorithms in IoT communications*, in *Inf. Syst. Front.*, 2023, https://link.springer.com/article/10.1007/s10796-023-10383-9 (ultimo accesso 16/10/2025), p. 1243 ss.
34. Cfr. H. GHARAVI, J. GRANJAL, E. MONTEIRO, *Post-quantum blockchain security for the internet of things: Survey and research directions*, in *IEEE Commun. Surv. Tutorials*, 2024, https://doi.org/10.1109/COMST.2024.3355222 (ultimo accesso 17/04/2025), p. 1748 ss.
35. : Cfr. S. ULLAH, J. ZHENG, N. DIN, M.T. HUSSAIN, F. ULLAH, M. YOUSAF, *Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey*, in *Comput. Sci. Rev.*, 2023,https://www.sciencedirect.com/science/article/abs/pii/S1574013722000648?via%3Dihub (ultimo accesso 16/10/2025).
36. Gli attacchi *zero-day* rappresentano una delle minacce più insidiose nel panorama della sicurezza informatica, poiché sfruttano vulnerabilità sconosciute nei *software*, nei sistemi operativi o nelle infrastrutture digitali prima che gli sviluppatori abbiano la possibilità di rilasciare una *patch* correttiva. Il termine "zero-day" sottolinea l'assenza di un preavviso o di un periodo di difesa da parte delle aziende e degli utenti, i quali si trovano esposti a un rischio immediato non appena la falla viene scoperta e sfruttata dai cybercriminali.

di vulnerabilità, assicurando al contempo la scalabilità necessaria per gestire flussi informativi complessi[37]. In questo contesto, i proprietari dei dati mantengono il controllo esclusivo delle proprie informazioni, riducendo il rischio di falsificazioni e di intercettazioni non autorizzate[38]. Parallelamente, l'adozione della blockchain all'interno della catena di approvvigionamento automobilistico potrebbe rappresentare una svolta in termini di trasparenza e affidabilità[39]. La registrazione immutabile delle transazioni e la gestione sicura delle identità dei veicoli hanno il beneficio di rafforzare la fiducia tra le varie entità, facilitando lo scambio di informazioni critiche e il monitoraggio dei flussi fisici di componenti e prodotti. Questa tecnologia si dimostra particolarmente efficace nell'assicurare la tracciabilità e la certificazione digitale dei beni, elementi fondamentali in un contesto economico caratterizzato da una rapida evoluzione e da dinamiche di mercato sempre più complesse[40]. Tuttavia, nonostante i molteplici vantaggi, l'adozione diffusa della *blockchain* nel settore automobilistico si confronta con sfide rilevanti in quanto, la trasparenza, intrinseca al sistema decentralizzato, può scontrarsi con la necessità di mantenere segrete informazioni strategiche, creando tensioni tra condivisione e riservatezza[41]. Inoltre, l'incremento della complessità nelle reti di approvvigionamento impone la definizione di standard comuni e la gestione di flussi dati sempre più consistenti, elementi imprescindibili per garantire un sistema sicuro e interoperabile[42]. Concludendo, la *blockchain*, applicata al sistema dei veicoli connessi, si configura come una proposta rivoluzionaria in grado di elevare la sicurezza e l'efficienza dei nuovi veicoli e delle relative catene di approvvigionamento, a patto che si affrontino con rigore sistematico le criticità legate alla standardizzazione, alla gestione della privacy e alla scalabilità in contesti in continuo mutamento[43]. Tuttavia, il suo impiego, pur ricco di potenzialità, rischia

37. Cfr. T. ZAIDI, S. GARAI, *Emerging trends in cybersecurity: A holistic view on current threats, assessing solutions, and pioneering new frontiers*, in *Blockch. Heal. Tod.*, 2024, https://blockchainhealthcaretoday.com/index.php/journal/article/view/302 (ultimo accesso 16/10/2025).
38. Cfr. G. ABDELKADER, K. ELGAZZAR, A. KHAMIS, *Connected vehicles: Technology review, state of the art, challenges and opportunities*, in *Sensors*, 2021, https://www.mdpi.com/1424-8220/21/22/7712 (ultimo accesso in data 16/10/2025).
39. Cfr. P. FRAGA-LAMAS, T.M. FERNANDEZ-CARAMES, *A review on blockchain technologies for an advanced and cyber-resilient automotive industry*, in *IEEE Access*, 2019, https://ieeexplore.ieee.org/document/8626103 (ultimo accesso 16/10/2025).
40. Cfr. V. MALIK, R. MITTAL, D. MAVALURU, B.R. NARAPUREDDY, S.B. GOYAL, R.J. MARTIN, *Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks*, in *IEEE Access*, 2023, https://ieeexplore.ieee.org/document/10177172 (ultimo accesso 16/10/2025).
41. Cfr. S. ZAFAR, S.F.U. HASSAN, A.S. MOHAMMAD, A.A. AL-AHMADI, N. ULLAH, *Implementation of a distributed framework for permissioned blockchain-based secure automotive supply chain management*, in *Sensors*, 2022, https://www.mdpi.com/1424-8220/22/19/7367 (ultimo accesso 16/10/2025).
42. Cfr. A.O. OKOMANYI, A.R. SHERWOOD, E. SHITTU, *Exploring effective strategies against cyberattacks: The case of the automotive industry*, in *Environ. Syst. Decis.*, 2024, https://link.springer.com/article/10.1007/s10669-024-09971-0 (ultimo accesso 16/10/2025).
43. Cfr. M.D.S. FERDOUS, M.J.M. CHOWDHURY, K. BISWAS, N. CHOWDHURY, V. MUTHUKKUMARASAMY; *Immutable autobiography of smart cars leveraging blockchain technology*, in *Knowl. Eng. Rev.*, 2020, https://www.cambridge.org/core/journals/knowledge-engineering-review/article/abs/immutable-autobio-

di rimanere incompleto in assenza di un solido supporto normativo che regoli i diritti di proprietà sui dati e introduca licenze d'uso dinamiche. Tale mancanza normativa impedisce di superare la complessa dicotomia che vede i dati veicolari come entità con una duplice natura: da un lato, risorsa personale e, dall'altro, elemento infrastrutturale fondamentale.
Senza un intervento legislativo mirato, il contrasto tra il proprietario del veicolo e quello dei dati resta irrisolto, compromettendo la capacità della *blockchain* di fornire una soluzione definitiva a questo problema strutturale.

4. *Cybersecurity* e privacy: il quadro normativo e regolamentare

Il legislatore europeo è intervenuto a partire dal 2015 nel settore *automotive*, attraverso direttive e regolamenti atti a colmare il vuoto normativo degli Stati membri[44]. Un primo esempio è il Regolamento UE n. 758 del 2015 che disciplina l'implementazione obbligatoria, sui veicoli di nuova produzione, del sistema denominato *eCall*, ideato per attivare automaticamente o manualmente una chiamata d'emergenza al numero unico europeo 112[45]. Tale segnalazione viene instradata attraverso centri di raccolta appositamente predisposti (*Public Safety Answering Points* – PSAP), gestiti da enti pubblici o da soggetti privati autorizzati. L'obiettivo primario di questa tecnologia è la tempestiva attivazione dei soccorsi, con la conseguente riduzione della mortalità e della gravità delle lesioni derivanti da incidenti stradali. Il Regolamento, inoltre, ammette la coesistenza di sistemi privati analoghi (*Third Party Service eCall* – TPS *eCall*), già in uso prima della normativa, purché non sostituiscano il servizio pubblico, il cui impianto è obbligatorio per tutti i veicoli omologati a partire dal 31 marzo 2018, stabilendo, altresì, che le due tipologie di sistemi operino in maniera indipendente, senza possibilità di condivisione o interscambio di dati[46]. Altro esempio è quello del Regolamento UE n. 2144 del 2019, il quale rappresenta una svolta nell'ambito della sicurezza dei trasporti, imponendo a partire dal 2022 l'adozione obbligatoria, su tutte le nuove immatricolazioni, di sofisticati sistemi di assistenza alla guida (*Advanced Driver Assistance Systems* - ADAS) come l'adattamento intelligente della velocità, rilevamento in retromarcia con telecamera o sensori, avviso in caso di disattenzione del conducente dovuta a stanchezza o distrazione, registratori di dati di evento (scatola nera - RDE) e segnalazione di arresto di emergenza e l'interfaccia di installazione di dispositivi di tipo *alcolock*, tutti spesso integrati con altri dispositivi di sicurezza del veicolo come ABS (*anti-lock braking system*), EBD (*Electronic Brake-Force Distribution*) o ESP (*Electronic Stability Control*). I sistemi avanzati di assistenza alla guida rappresentano una vera e propria evoluzione tecnologica nel mondo automobilistico, trasformando i veicoli in piattaforme

graphy-of-smart-cars-leveraging-blockchain-technology/A9C2C31B80091A409ABF05C7671FD331 (ultimo 16/10/2025).

44. Cfr. M. MORELLI, Il processo di digitalizzazione del settore automobilistico. Quando il progresso tecnologico deve sempre essere supportato da norme, regole di condotta e buone pratiche, in Sociologia del diritto, Vol. 51, N. 2, 2024, p. 105 ss.

45. Art. 4, reg. UE n. 758 del 2015.

46. Art. 6, n.11, reg. UE n. 758 del 2015.

intelligenti capaci di analizzare il contesto stradale e reagire in tempo reale[47]. Questi sistemi, simili per certi aspetti a computer integrati nel mezzo, si basano su un sofisticato equilibrio tra componenti *hardware* e *software* che consente loro di raccogliere informazioni dall'ambiente circostante, elaborarle e tradurle in azioni concrete[48]. Il cuore del loro funzionamento risiede in una rete di sensori altamente specializzati, progettati per percepire dettagli fondamentali come la velocità, la distanza dagli ostacoli e le condizioni della strada. I dati raccolti vengono poi inviati a una potente unità di elaborazione, che li analizza in frazioni di secondo per generare risposte adeguate alla situazione, rese ancora più efficaci grazie all'adozione di tecnologie *by-wire*[49], che sostituiscono i tradizionali comandi meccanici con segnali elettrici, assicurando una maggiore precisione e riducendo i tempi di reazione. Risulta tuttavia cruciale, nell'analisi dei sistemi di guida assistita e autonoma, coglierne la duplice natura ontologica, che riflette una distinzione sostanziale tra l'automazione come supporto e l'automazione come sostituzione dell'uomo nella guida. Un chiarimento normativo in tal senso è offerto dalla Convenzione di Vienna, come modificata il 14 dicembre 2020 ed entrata in vigore il 14 luglio 2022 (RU 2022 51), la quale, all'articolo 1, lettera a), qualifica come sistema di guida autonoma quell'apparato costituito da componenti *hardware* e *software* capaci di esercitare in modo continuativo il controllo dinamico del veicolo. A sua volta, l'articolo 1, lettera ab), definisce tale controllo dinamico come l'insieme delle funzioni operative e strategiche eseguite in tempo reale, necessarie per la conduzione del veicolo, comprendendo tra esse il controllo della traiettoria sia laterale che longitudinale, il monitoraggio delle condizioni stradali, la reazione agli eventi di traffico e la gestione delle manovre, tanto in fase di preparazione

47. Considerando n. 10), reg. UE n. 2144 del 2019.

48. Art. 1, lett. g) del d.m. 28 febbraio 2018; cfr. D. CERINI, A. PISANI TEDESCO (a cura di), *Smart mobility, smart cars e intelligenza artificiale: responsabilità e prospettive*, Torino, 2019; cfr. P. MANCINO, *Auto connesse e rischi sulla privacy, le criticità sono anche tra le righe della normativa*, 2023, in https://www.federprivacy.org/informazione/primo-piano/auto-connesse-e-rischi-sulla-privacy-le-criticita-sono-anche-tra-le-righe-della-normativa (ultimo accesso in data 02/04/2025); cfr. S. PELLEGATTA, *I sistemi hardware installati sui "veicoli intelligenti": complementarità e ridondanza come strumenti tecnici per consentire il passaggio del controllo legale del mezzo dalla persona fisica alla macchina. (Radar, Lidar, Drive by Wire)*, su *Diritto di Internet*, 2022, https://dirittodiinternet.it/i-sistemi-hardware-installati-sui-veicoli-intelligenti-complementarita-e-ridondanza-come-strumenti-tecnici-per-consentire-il-passaggio-del-controllo-legale-del-mezzo-dalla-persona-f/ (ultimo accesso 02/04/2025).

49. La tecnologia *by-wire* sta trasformando profondamente la risposta dei veicoli ai comandi del conducente, sostituendo i tradizionali collegamenti meccanici con segnali elettronici. Questo approccio, già applicato al controllo di freni e sterzo, consente di eliminare componenti fisici come il piantone, affidando la gestione della direzione e della frenata a impulsi digitali interpretati da centraline elettroniche. Anche il *feedback* percepito dal conducente, come la resistenza del pedale del freno, viene riprodotto artificialmente. Oltre a semplificare la progettazione e ridurre i guasti, questa evoluzione tecnologica accresce la sicurezza, diminuendo il numero di elementi meccanici potenzialmente pericolosi in caso di urto. Cfr. S. *PELLEGATTA, I sistemi hardware installati sui "veicoli intelligenti": complementarità e ridondanza come strumenti tecnici per consentire il passaggio del controllo legale del mezzo dalla persona fisica alla macchina*, cit.

quanto nella loro segnalazione. Una simile articolazione concettuale è recepita anche nell'ordinamento interno, in particolare nel decreto 20 febbraio 2018, noto come "Smart Road", il quale, all'articolo 1, lettere f) e g), opera una distinzione analoga tra veicoli dotati di sistemi di guida autonoma e quelli muniti di tecnologie di assistenza alla guida.
Chiariti questi aspetti tecnici, è evidente come le disposizioni contenute in entrambi i Regolamenti abbiano evidenti ricadute sulla privacy dell'utente, sia esso inteso quale conducente che trasportato. All'uopo, l'articolo 6 del Regolamento UE relativo al sistema *eCall* stabilisce che quest'ultimo debba essere progettato (privacy *by design*) in modo da conservare esclusivamente le ultime tre coordinate GPS del veicolo, limitandone l'archiviazione al tempo strettamente necessario per determinare la sua geolocalizzazione esatta e la direzione di marcia al momento dell'evento. Inoltre, è previsto che i produttori di autoveicoli forniscano agli utenti un manuale di istruzioni chiaro ed esaustivo, nel quale siano dettagliate le modalità di trattamento dei dati personali e i diritti esercitabili dagli interessati. Per quanto attiene eventuali sistemi privati installati dalle case automobilistiche parallelamente a quello pubblico, il loro impiego può andare oltre la semplice sicurezza stradale e trasformarsi in uno strumento per la raccolta di dati, successivamente utilizzati dai centri di elaborazione privati per offrire servizi complementari, come la prenotazione di ristoranti o altre funzioni commerciali. Diversamente, il Regolamento UE n. 2144 del 2019 introducendo ulteriori dispositivi di rilevazione pone diverse questioni in materia di protezione dei dati personali. Tra questi, i più problematici dal punto di vista della privacy, sono il sistema di monitoraggio della disattenzione e della stanchezza del conducente, i cui dati devono essere immediatamente cancellati una volta concluso il trattamento[50], nonché il Registratore di Eventi per l'Automobile (RDE). Quest'ultimo, simile alla cosiddetta *black box* (scatola nera) già impiegata da tempo nel settore automobilistico, è progettato per registrare e conservare parametri critici nei momenti immediatamente precedenti, contestuali e successivi a una collisione. Tra i dati acquisiti rientrano la velocità, l'azionamento dei freni, la posizione e l'inclinazione del veicolo, lo stato e la frequenza di attivazione dei dispositivi di sicurezza, nonché il funzionamento del sistema *eCall* e di altri meccanismi di prevenzione degli incidenti, il tutto nel rispetto del GDPR. Sul piano della gestione dei dati raccolti, l'articolo 6 del Regolamento UE n. 2144 del 2019, prescrive che il RDE debba operare all'interno di un sistema a circuito chiuso che garantisca l'anonimizzazione delle informazioni, prevenendone manipolazioni e utilizzi impropri. A tale scopo, l'articolo 6.5 vieta espressamente l'archiviazione delle ultime quattro cifre del codice VIS (*Vehicle Indicator Section*) del numero di identificazione del veicolo (VIN)[51], nonché di qualsiasi altro elemento che possa consentire l'individuazione del mezzo o del suo proprietario. In ordine all'accesso ai dati raccolti, gli articoli 6.3 e 6.4 lett. d) del Regolamento UE n. 2144 del 2019, nel rendere indisponibili i dati raccolti dai sistemi di avviso della disattenzione e della stanchezza del conducente e di avviso avanzato della distrazione del conducente ("non sono in alcun momento accessibili o messi a disposizione di terzi e

50. Art. 6.3, reg. UE n. 2144 del 2019.
51. Art. 6.5 reg. UE n. 2144 del 2019.

sono immediatamente cancellati dopo il trattamento"), riserva, nel caso dei dati raccolti dal sistema RDE, l'accesso alle sole autorità nazionali, tramite un'interfaccia standardizzata e nel rispetto delle disposizioni legislative nazionali o dell'Unione, limitatamente alle finalità di ricerca e analisi sugli incidenti stradali, comprese eventuali indagini giudiziarie. Tuttavia, la previsione di anonimizzazione solleva alcune perplessità, poiché le informazioni registrate dal dispositivo si riferiscono inevitabilmente a un veicolo specifico, che potrebbe essere utilizzato da conducenti diversi, come nel caso di auto in *sharing*[52] o noleggiate con copertura assicurativa aziendale. Se, però, i dati venissero aggregati per individuare tendenze sugli incidenti e sviluppare strategie di prevenzione, l'anonimizzazione acquisirebbe un senso compiuto.

Al di là di questi primi aspetti legati alla privacy, le problematiche relative all'applicazione delle nuove tecnologie agli autoveicoli aprono anche ad una necessaria riflessione sulla *cybersecurity* dei singoli dispositivi installati e del veicolo nella sua interezza, in quanto, l'espansione dei fenomeni cybercriminali organizzati (*cybergang* come *LockBit*) fa si che in un prossimo futuro si discuterà più di autoveicoli *hackerati* (il *ransomware*[53] quale rivisitazione in chiave tecnologica del "cavallo di ritorno"), che rubati[54]. Emblematico, sul punto, è l'esperimento condotto nel 2015 due esperti statunitensi di sicurezza informatica i quali hanno dimostrato in modo eclatante le vulnerabilità dei sistemi digitali dei veicoli moderni, riuscendo a prendere il controllo remoto di una Jeep Cherokee tramite il sistema *Uconnect*. Questa piattaforma, che gestisce funzioni come navigazione, *infotainment* e connettività, esponeva il veicolo a rischi informatici in quanto identificabile *online* attraverso un indirizzo IP. Durante il test, condotto con un giornalista a bordo, i

52. European Commission: Directorate-General for Research and Innovation, *Ethics of connected and automated vehicles – Recommendations on road safety, privacy, fairness, explainability and responsibility*, Publications Office, 2020, cit.: "Significant data collection is necessary for the safe and efficient functioning of CAVs. The vehicle-to vehicle (V2V), vehicle-to-infrastructure (V2I) or vehicle-to- everything (V2X) communication channels include the potential for a multitude of separate actors vying for general and specific personal data controlled by drivers, in real time or near-real time. One particular challenge that arises in this context is the privacy protection of multiple concerned individuals (e.g. driver, pedestrian, passenger or other drivers). The use of CAVs can include sharing of rides from similar origins and destinations, between different passengers. In such situations, all passengers sharing the same vehicle, as well as pedestrians and other road users in the vehicle's vicinity could, in principle, be identified. This can occur without the awareness of those affected. The European data protection rules require any such processing to rely on a valid legal basis and on transparent information about the processing being provided to all individuals concerned.".

53. Il *ransomware* è una tipologia di *software* malevolo (*malware*) progettato per compromettere dispositivi digitali mediante la cifratura o il blocco selettivo dei dati in essi contenuti. Una volta attivato, il programma impedisce l'accesso a tali informazioni e richiede il pagamento di una somma di denaro (*ransom*) quale condizione per il ripristino della piena disponibilità dei contenuti digitali.

54. Cfr. M. CARRÀ, *I rischi 'nascosti' dell'auto a guida autonoma e il pericolo dell'hackeraggio*, 2021, *Forbes*, https://forbes.it/2021/02/18/i-rischi-nascosti-dellauto-a-guida-autonoma-e-il-pericolo-dellhackeraggio (ultimo accesso 16/10/2025).

ricercatori hanno inizialmente eseguito azioni minori – come l'accensione forzata dell'aria condizionata e della radio – per poi dimostrare la possibilità di azioni ben più gravi: hanno spento il motore mentre l'auto era in autostrada e, in un secondo momento, in un ambiente controllato, hanno manipolato anche sterzo e freni, evidenziando la pericolosità concreta di simili attacchi.
In un orizzonte così composito il tema della *cyberscurity* e della privacy diventano un *must*, due aspetti della medesima problematica. Sul punto le Nazioni Unite sono intervenute con due Regolamenti, UNECE *Cybersecurity* n. 155 del 2021 che si riferisce al nuovo standard ISO/SAE 21434 (*Road Vehicle Cyber Security Engineering*) e UNECE *Software Updating* n. 156 del 2021, in vigore dal 2024 per le omologazioni e dal 2026 per le nuove immatricolazioni, i quali si pongono come il punto di partenza di un più ampio quadro relativo alla *cybersecurity* e all'aggiornamento dei dati in movimento. L'attuazione di tali normative ha segnato l'inizio di una nuova era nel settore automobilistico, imponendo standard rigorosi per la sicurezza dei sistemi informatici e per la gestione degli aggiornamenti software. In particolare, il Regolamento UNECE *Cybersecurity* n. 155, "risk based", impattando sull'intero ciclo di vita del veicolo (dal *concept* alla produzione sino alla rottamazione coinvolgendo l'intera *supply chain*) richiede agli OEM (*Original Equipment Manufacturer* ovvero i costruttori e produttori di componentistica) di fornire prove documentali relative ai processi di sviluppo dei componenti *software* e *hardware*, affinché i veicoli possano ottenere la certificazione necessaria per l'immatricolazione, in un contesto generale di *secure by design*. Contestualmente, il Regolamento UNECE n. 155 impone di individuare e valutare criticamente le aree di maggior rischio in termini di *cybersecurity*, prevedendo misure adeguate atte a mitigare le potenziali vulnerabilità e a garantire un monitoraggio costante, da rendere note annualmente all'ente certificatore. L'architettura del Regolamento UNECE n. 155 si sviluppa su due direttrici strettamente interconnesse: la prima impone l'adozione di un sistema di gestione della sicurezza informatica (CSMS) all'interno dell'organizzazione, il quale deve coprire l'intero ciclo operativo, dalla definizione delle politiche interne fino alla gestione degli incidenti legati a potenziali attacchi digitali, assicurando che ogni componente, anche quelle sviluppate da terzi, siano soggetto a procedure certificate. In tale prospettiva, il costruttore dei veicoli impone ai propri fornitori di componenti di essere *compliant* agli aspetti normativi in ambito cyber (ISO 26262, ISO 21434), dimostrando, così, la loro compliance relativamente a tutto il *vehicle life-cycle*. La seconda direttrice si concentra sulla protezione del prodotto, delineando un quadro in cui il veicolo debba essere messo in sicurezza rispetto a specifiche classi di rischio, lasciando però la scelta delle soluzioni tecniche a carico del costruttore e dei suoi fornitori. In quest'ottica, è prevista l'adozione di un processo di analisi delle minacce e dei rischi (TARA) che consenta di identificare, valutare e quantificare i possibili danni in termini di sicurezza, operatività, impatto economico e tutela della privacy, proteggendo così informazioni sensibili come i dati sullo stile di guida, le destinazioni e i contatti personali. Diversamente dal Regolamento UNECE n. 155 il Regolamento UNECE *Software Updating* n. 156 pone l'accento sugli aggiornamenti *software* e del sistema di gestione degli aggiornamenti (*smart update management system* - SUMS), stabilendo come ogni intervento *software* debba essere eseguito in condizioni di sicurezza, con un'informativa trasparente rivolta al

consumatore finale. Una volta che il veicolo prende vita su strada, la piattaforma SUMS diventa il partner indispensabile per le officine di riparazione e manutenzione, potendovi accedere ai dati di bordo del veicolo, intervenire sulle unità di controllo elettronico (ECU) e tracciare con precisione ogni operazione eseguita. Allo stesso tempo, il costruttore del veicolo può inviare aggiornamenti *software* e miglioramenti delle configurazioni, che vengono scaricati e implementati direttamente tramite SUMS *over the air*, assicurando non solo la sicurezza e l'efficienza dei veicoli, ma garantendo anche la totale trasparenza e tracciabilità degli interventi. La crescente integrazione di componenti elettronici e *software* richiede un continuo aggiornamento degli standard di conformità, tanto che oggi si fa riferimento a nuove linee guida internazionali, come lo standard ISO/SAE 21434, che si dedica specificamente all'ingegneria della *cybersecurity* per i veicoli, affiancato dalla ISO 26262, incentrata sulla sicurezza funzionale degli utenti e delle vetture.
Tuttavia, i Regolamenti ONU in esame nulla dicono in ordine alla tutela della privacy in caso di sua violazione, attraverso i sistemi integrati nell'autovettura o di trattamento oltre il consenso accordato. È di tutta evidenza come le grandi opportunità economiche che derivano dal rilevamento dei dati degli autoveicoli spingono le case automobilistiche verso una massimizzazione del processo di trattamento dei dati, portandole a ripensare al loro modello imprenditoriale in un sistema di condivisione con i partner dei loro ecosistemi aziendali[55], al fine della realizzazione di un vantaggio competitivo[56]. In un simile scenario il modello normativo europeo in tema di protezione dei dati personali (Direttiva *ePrivacy*, GDPR e *Data Act*) si frappone tra le mire, a volte spregiudicate, delle case automobilistiche e la tutela dei diritti fondamentali dei cittadini dell'Unione. Nel 2021, il Comitato Europeo per la Protezione dei Dati (EDPB), con la partecipazione attiva dell'Autorità Garante italiana, ha elaborato linee guida EDPB (Linee Guida 1/2020 *on processing personal data in the context of connected vehicles and mobility related applications*) mirate a regolamentare l'uso delle tecnologie di largo impiego, fornendo indicazioni specifiche ai produttori e agli utilizzatori. A distanza di un anno dall'inizio dei lavori, l'EDPB, consapevole delle criticità dei veicoli connessi e delle conseguenze disastrose di una intrusione su tali sistemi[57], ha adottato in via definitiva le linee guida riguardanti le automobili connesse, sollecitando i costruttori automobilistici e le aziende operanti nel settore delle automobili *smart* a conformarsi ai principi di privacy *by design* e privacy *by default* (articolo 25 del GDPR) affinché i sistemi installati limitino la raccolta e la trasmissione di dati personali ai soli scopi strettamente necessari, in conformità con i principi di cui al GDPR[58]. L'elaborazione dei dati, in questo contesto, deve poggiare su basi giuridiche solide, prevalentemente fondate sul consenso esplicito degli interessati[59] e sul criterio della necessità,

55. Cfr. Y. CHEN, J. KREULEN, M. CAMPBELL, C. ABRAMS, *Analytics ecosystem transformation: A force for business model innovation*, 2111, http://dx.doi.org/10.1109/SRII.2011.12 (ultimo accesso 03/04/2025).
56. Cfr. D. BILGERI, H. GEBAUER, E. FLEISCH, F. WORTMANN, *Driving process innovation with IoT field data*, in *MIS Quarterly Executive*, 2019, http://dx.doi.org/10.17705/2msqe.00016 (ultimo accesso 03/04/2025).
57. Par. 1.5.5., punto 59 EDPB 2021.
58. Par. 1.5.4., punto 57 EDPB 2021.
59. Par. 1.5.1., punto 46 EDPB 2021.

come nel caso di funzionalità per l'assistenza alla guida, la sicurezza stradale o i servizi assicurativi basati sull'uso del veicolo (*pay-as-you-drive*)[60]. Per questi ultimi, inoltre, le compagnie assicurative devono offrire agli automobilisti un'opzione alternativa che non implichi l'installazione di dispositivi di monitoraggio continuo (*black box*) o la tracciabilità dei loro spostamenti. La trasparenza, insieme a quello del consenso, è l'altro principio cardine: i soggetti presenti a bordo dell'auto devono ricevere informazioni chiare, fornite nella loro lingua, sulle modalità di trattamento dei dati e avere la possibilità di esercitare agevolmente i diritti previsti dalla Direttiva UE n. 58 del 2002 (*ePrivacy*) e dal GDPR. Inoltre, per garantire maggiore tutela, gli utenti dovrebbero poter attivare o disattivare con semplicità determinati servizi tramite un'interfaccia intuitiva (*user friendly*). Laddove tecnicamente realizzabile, i dati – in particolare quelli invasivi[61] relativi alla geolocalizzazione – dovrebbero essere trattati direttamente all'interno del veicolo, evitando il trasferimento a server remoti. Le misure di protezione individuate dai Garanti includono la pseudonimizzazione o l'anonimizzazione delle informazioni, oltre all'impiego di sistemi crittografici che ne assicurino l'integrità e impediscano accessi non autorizzati. L'EDPB ha inoltre approvato la versione iniziale delle linee guida relative agli assistenti vocali digitali (*Virtual Voice Assistants* – VVA), dispositivi presenti in smartphone, smart TV, automobili connesse e altoparlanti intelligenti ampiamente diffusi nelle abitazioni. Uno degli aspetti più critici emersi attiene la complessità e la varietà dei dati trattati da questi assistenti in grado di eseguire ordini, rispondere a domande, controllare dispositivi domotici, fornire assistenza clienti o rimanere semplicemente in ascolto, in attesa di un comando. I trattamenti possono riguardare sia utenti specificamente identificabili, ad esempio tramite riconoscimento biometrico della voce, sia gruppi indefiniti di persone, come membri di una stessa famiglia. Per mitigare i rischi e migliorare le tutele, i Garanti hanno richiesto ai produttori che gli assistenti vocali siano progettati in modo da garantire la massima trasparenza e riservatezza fin dalla fase di sviluppo (*by design*), attraverso configurazioni predefinite orientate alla protezione dei dati (*by default*). È fondamentale che l'utente possa comprendere con chiarezza lo stato del dispositivo – se in ascolto (*passive listening*) o in esecuzione di un comando – e che vi sia una definizione esplicita della titolarità del trattamento dei dati, anche nei casi in cui intervengano fornitori di servizi terzi. Infine, devono essere ben distinte le finalità per cui i dati vengono elaborati, con un consenso esplicito e separato per specifici trattamenti, come quelli legati a operazioni di marketing, profilazione o apprendimento automatico (*machine learning*) degli algoritmi di intelligenza artificiale[62]. Tra le misure di sicurezza raccomandate rientrano l'adozione di meccanismi di autenticazione robusti, l'impiego di tecniche di pseudonimizzazione e l'applicazione di specifiche garanzie per i dati biometrici, come l'elaborazione del riconoscimento vocale direttamente sul dispositivo anziché attraverso server remoti.

60. Newsletter del Garante della Privacy del 29/03/2021, https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9568537 (ultimo accesso 15/04/2025).
61. Par. 1.5, punto 45 EDPB 2021.
62. Par. 1.5.4, punto 58 EDPB 2021.

L'applicabilità del *Data Act*, destinato a integrarsi con il GDPR per rafforzare il controllo di cittadini e imprese sui dati, siano essi personali o non personali, generati dall'interazione con prodotti e servizi, ha avuto impatto immediato sul settore automobilistico, ampliando il diritto alla portabilità dei dati, che, disciplinato dall'art. 20 del GDPR, viene esteso a qualsiasi informazione prodotta attraverso l'uso di dispositivi e macchinari in un evidente cambio di prospettiva che pone al centro l'utente e la sua protezione (*user-centric approach*). Pur non risolvendo esplicitamente la questione relativa alla proprietà dei dati, essendo questi prodotti dal veicolo, ma intrinsecamente connessi all'utente (*my car, my data*), quest'ultimi, attraverso il sistema di regole dettate dagli articoli 3-5 del *Data Act*, diventano i custodi dei dati e potranno accedere ai dati grezzi da loro co-generati e pre-elaborati, compresi i metadati associati, in modo semplice e sicuro, potendone disporne liberamente e senza costi, anche per trasferirli ad un altro operatore economico. L'integrazione dei metadati tra i dati messi a disposizione dell'utente è fondamentale al fine di una contestualizzazione dei dati raccolti, utile alla loro comprensione. Tuttavia restano esclusi i dati derivati o altamente arricchiti da processi complessi o da algoritmi di proprietà di terzi. La portata innovativa del *Data Act* è evidente, rafforzando anche la trasparenza, garantendo agli interessati la possibilità di conoscere se le informazioni vengano raccolte in tempo reale, quali dati siano effettivamente generati dall'utilizzo di un determinato prodotto o servizio e quali modalità di accesso siano previste, imponendo ai costruttori/fornitori di esplicitare se e con quali finalità i dati verranno utilizzati dal fornitore o condivisi con soggetti terzi. Tuttavia, la trasversalità del *Data Act* e la non specificità dello stesso per il settore automobilistico, rientrando nel suo ambito di applicazione per via analogica attraverso il tema della connessione e della produzione di dati, lasciano in ombra aspetti dirimenti come quello della proprietà dei dati che potrebbe essere risolta esclusivamente da una normativa *ad hoc*.

5. Conclusioni

Le sfide lanciate dalle *disruptive technological innovations* nell'ambito dei veicoli connessi e dei CAVs (*connected and automated vehicle*s), riflettono, in linea di massima, quelle che la massiva applicazione delle tecnologie basate sulla raccolta dei dati hanno rappresentato sia per la consolidata architettura interpretativa giuridica che per gli assetti societari e per la sostenibilità, estensivamente intesa. Come più volte sottolineato, l'approccio non può che essere multidimensionale, coinvolgendo sia i diversi rami del sapere e della conoscenza che, al loro interno, in una prospettiva analitica multilivello, i differenti segmenti che lo compongono. La *cybersecurity* come la privacy, quest'ultima proiettata sempre più in una dimensione collettiva[63], riveste un ruolo ambivalente, sia come prospettiva di sviluppo che di freno, atteso il rigoroso sistema di tutele e

63. Cfr. G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto Pubblico*, n.1, 2019, p. 89 ss.; M. DE TULLIO, U*guaglianza sostanziale e nuove dimensioni della partecipazione politica*, *Tesi in Diritti Umani. Teoria, storia e prassi – XXXI ciclo*, Napoli, 2018, cap. 3, par. 4.

sanzioni imposte dal legislatore comunitario. Si rende quindi necessario conciliare sinergicamente la tutela dei diritti fondamentali degli utenti-cittadini, in cui la privacy e la *cybersecurity* rientrano a pieno in una dimensione di complementarità e non di opzione binaria[64], con le opportunità di sviluppo che possono derivare dal trattamento dei dati acquisiti, come nel caso in analisi, da dispositivi installati in un autoveicolo. Il primo passo per avvicinare e fondere la tutela dei diritti con un sostenibile sviluppo è quello di raccogliere la fiducia dell'utente. Il tema della fiducia, all'indomani dell'adozione di sistemi di validazione decentrata come quelli della *blockchain*, riveste un ruolo di primaria importanza ed è una delle direttrici su cui muoversi. L'introduzione di una "user-centered perspective"[65] rappresenta la fase iniziale di un rinnovato modello relazionale tra utilizzatore e produttore, in cui l'utente, fidelizzato mediante l'integrazione tra la propria esperienza d'uso e il patrimonio reputazionale legato al *brand*, presta un consenso libero, specifico e informato (*opt-in*)[66] alla raccolta e all'impiego dei propri dati personali. In tale prospettiva, la fiducia dell'interessato si configurerà come manifestazione del cambiamento paradigmatico delle *policy* aziendali, a condizione che il produttore/fornitore del servizio sia in grado di fornire evidenza oggettiva, supportata da metriche *data-driven*, anche dell'implementazione di un sistema continuativo di formazione (*life long learning*), finalizzato a garantire livelli adeguati di *accountability* in materia di sicurezza informatica e di gestione dei rischi correlati a trattamenti non conformi al quadro normativo vigente in materia di protezione dei dati personali[67]. La previsione della *security awareness* all'interno dei programmi di formazione continua aziendali, qualora integrato con una strategia di *Corporate Social Responsibility* (CSR) ispirata a principi etici di *risk management*, porterà ad una duplice serie di vantaggi: non solo il potenziamento della capacità di risposta dell'organizzazione agli imprevisti, ma anche il consolidamento del rapporto di fiducia con gli *stakeholder*. Ovviamente la prospettiva utente-centrica va estesa all'intero ecosistema, nel momento in cui viene imposto ai singoli nodi della catena produttiva di essere *compliant*. Sulla base di tali premesse, l'adozione per tutto il ciclo vitale del prodotto di standard certificati funge da *buster*, trasformando le buone pratiche, richieste dal

64. M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Medialaws*, 2018, p. 82 ss.

65. Cfr. F. SCHAFER, H. GEBAUERA, C. GROGER, O. GASSMANN, F. WORTMANNA, *Data-driven business and data privacy: Challenges and measures for product-based companies*, 2023, https://doi.org/10.1016/j.bushor.2022.10.002 (ultimo accesso 08/04/2025).

66. I dati *opt-in*, in cui il consenso è accordato esplicitamente (art. 6 del GDPR) dall'utente, si differenziano dai dati *opt-out* in cui l'utente non ha espresso un consenso al trattamento, ma questo inizia sino a quando il consenso non viene negato (approccio passivo al consenso).

67. La letteratura scientifica ravvisa nell'aumento dei tassi di utilizzo di dati anonimizzati un *trend* di aumento della fiducia degli utenti, essendo per loro stessa natura atti a limitare i rischi derivanti da eventuali violazioni di sicurezza, riducendo l'esposizione complessiva dei dati personali particolari. Cfr. C. UTZ, M. DEGELING, S. FAHL, F. SCHAUB, T. HOLZ, *(Un)informed consent: Studying GDPR consent notices in the field, in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, https://doi.org/10.1145/3319535.3354212 (ultimo accesso 05/04/2025).

legislatore comunitario, in eccellenti pratiche, con una considerevole ricaduta in termini reputazionali oltre che di sicurezza. Tuttavia, nell'attuale scenario di accelerazione tecnologica, la *compliance*, pur rivestendo un ruolo imprescindibile, da sola si configura come strumento insufficiente ad orientare la società verso un futuro migliore. Infatti, se da un lato la regolamentazione digitale definisce i confini tra comportamenti leciti e illeciti, evitando la creazione di zone franche in cui, a causa dell'intrinseca opacità dei processi algoritmici, possano rendersi "di fatto non giustiziabili" le decisioni prese attraverso l'utilizzo di tali sistemi[68], dall'altro non fornisce indicazioni sulle strategie ottimali da adottare all'interno del ventaglio di scelte ammesse, strategie tali da potenziare il benessere collettivo. Coerentemente con quanto sin qui argomentato, spetta sia all'etica digitale, in grado di plasmare i valori e le preferenze morali, sia ad una *governance* digitale efficace, che assicura una gestione oculata delle dinamiche in atto, delineare il cammino verso soluzioni più virtuose[69] e non egoistiche[70], impedendo, tra l'altro, l'applicazione di "standard privati in concorrenza con valori pubblici"[71]. Se il contesto produttivo si connota per una naturale vocazione al progresso e all'innovazione, l'ordinamento giuridico ha storicamente assunto un ruolo eminentemente reattivo nei confronti delle evoluzioni tecnologiche, attendendo il manifestarsi di criticità per poi intervenire con soluzioni normative *ex post*. Risulta inevitabile, dunque, un definitivo mutamento della struttura epistemica: il diritto, da disciplina essenzialmente adattiva, deve evolversi in una dimensione proattiva, capace di anticipare le trasformazioni e predisporre un quadro normativo che non solo disciplini, ma favorisca l'adozione delle innovazioni emergenti[72]. Sul punto, come osservato da autorevole dottrina, il legislatore europeo attraverso provvedimenti quali il *Digital Services Act*, l'*AI Act*, il *Digital Markets Act* ed in ultimo l'*AI Continent Action Plan* dell'aprile 2025, ha inteso percorrere questa nuova direttrice paradigmatica[73].
Nel solco di questa riflessione, la metafora del "demone" che nel concedere all'umanità il beneficio dell'automobile[74] esige quale tributo il sacrificio di innumerevoli vite (rappresentazione plastica e segnica della dimensione di rischio insita nelle logiche tecnologiche che strutturano l'automobilità convenzionale), potrebbe oggi essere sovvertita attraverso lo sviluppo della mobilità intelligente, la quale, mediante l'integrazione tra infrastrutture connesse e sistemi di interazione

68. A. SIMONCINI, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, n. 2, 2023, p. 39.
69. Cfr. L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022, p. 129 ss.
70. Cfr. G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, cit., p. 114.
71. O. POLLICINO, *Costituzionalismo, privacy e meurodiritti*, in *Medialaws*, 2021, p. 11.
72. Cfr. E. AL MUREDEN, *Diritto dell'automotive. Dalla fabbrica alla strada: tra regole, mercato, tecnologia e società*, Bologna, 2024.
73. Cfr. G. BORGES, *New Liability Concepts: The Potenzial of Insurance and Compensation Funds*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, p. 126 ss.; cfr. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla Proposta di Regolamento dell'UE in materia di intelligenza artificiale*, in *BioLaw Journal. Rivista di BioDiritto*, 2021, n.3, p. 426 ss.
74. *Infra*, introduzione.

veicolo-uomo, promette di ridurre drasticamente il verificarsi di eventi lesivi, ridefinendo lo schema di riferimento della sicurezza stradale. In origine, nel nostro ordinamento, l'introduzione della circolazione veicolare di massa ha portato alla necessità di strutturare un sistema di responsabilità giuridica, inizialmente formalizzato dal solo articolo 2054 del Codice Civile e successivamente integrato dall'istituzione dell'obbligo assicurativo con la Legge n. 990 del 1969, a fronte della crescente diffusione degli autoveicoli e del rischio che proprietario e conducente inserivano nel sistema[75]. Ad oggi, la disciplina della responsabilità per danni derivanti dalla circolazione dei veicoli a motore si fonda su una logica di tutela rafforzata del terzo danneggiato, discostandosi in modo significativo dall'impianto codicistico ottocentesco. La vigente formulazione dell'articolo 2054 c.c., infatti, non si limita a ribadire il principio generale della responsabilità civile, ma introduce una deroga alla regola della responsabilità fondata sulla colpa[76], invertendo così l'onere della prova a favore della parte lesa. Tale opzione normativa, ispirata da finalità solidaristiche e di protezione degli interessi deboli, trova fondamento in un'evoluzione già in atto nel diritto positivo, anticipata da interventi legislativi speciali risalenti ai primi decenni del Novecento. È del 1912, infatti, una delle prime discipline settoriali dedicate ai sinistri stradali, segno della crescente attenzione per i rischi connessi alla diffusione della mobilità meccanizzata. La norma codicistica del 1942 si innesta dunque su un terreno normativo già tracciato, e trae ispirazione diretta dal codice della strada allora vigente; non è un caso che l'articolo 2054 c.c. riproduca, con minime modifiche, il contenuto dell'articolo 120 del R.D. 8 dicembre 1933 n. 1740[77], da cui eredita l'impianto sostanziale, introducendo solo lievi correttivi relativi all'identificazione dei soggetti su cui ricade la responsabilità risarcitoria[78].

Il consolidato sistema di tutele appena descritto, potrebbe essere messo in discussione dall'attuale transizione verso la mobilità *smart*, potenzialmente in grado di equilibrare due poli tradizionalmente in tensione: la circolazione e l'esigenza di sicurezza. I veicoli connessi e cooperativi, di fatti, introducono una prospettiva inedita, in quanto in grado di ridurre sensibilmente, se non azzerare,

75. Cfr. G. CALABRESI, E. AL MUREDEN, *Driverless car. Intelligenza artificiale e futuro della mobilità*, Bologna, 2021.

76. Cfr. M. FRANZONI, *L'illecito*, in M. FRANZONI, *Trattato della responsabilità civile*, Milano, 2004; ID., *Dei fatti illeciti*, in F. GALGANO (a cura di) *Commentario del codice civile Scialoja-Branca, Fatti illeciti, supplemento artt. 2043-2056-2059*, Bologna-Roma, 1993.

77. Art. 120 del r.d. 8 dicembre 1933 n. 1740, abrogato dal d.P.R. 13 dicembre 2010 n. 248: "Responsabilità del conducente e del proprietario dei veicoli. Il danno prodotto a persone o cose dalla circolazione di un veicolo si presume dovuto a colpa del conducente. La presunzione è esclusa solo quando questi provi che da parte sua si è avuta ogni cura, per evitare che il danno si verificasse. Non possono in alcun caso considerarsi come danni derivanti da forza maggiore quelli cagionati da difetti di costruzione o di manutenzione del veicolo. Il proprietario del veicolo è obbligato solidalmente col conducente a meno che provi che la circolazione del veicolo sia avvenuta contro la sua volontà, salva la responsabilità che a lui possa incombere secondo i principi generali del Codice civile",

78. C.M. BIANCA, *Diritto civile, La responsabilità*, V, Milano, 1994, p. 747; cfr. F. PECCENINI, *La responsabilità civile per la circolazione dei veicoli*, in P. CENDON (a cura di), *La responsabilità civile*, XIII, Torino, 1998.

l'incidenza del fattore umano quale principale causa dei sinistri stradali, garantendo al contempo una maggiore sostenibilità ambientale. Se da un lato si profilano interrogativi di ordine etico connessi ("moral dilemmas") all'autonomia delle scelte algoritmiche che tali sistemi sono chiamati a compiere in situazioni di emergenza (*trolley problem*)[79], dall'altro l'attuale impianto giuridico fa già ricorso alla categoria dello stato di necessità[80], consentendo di arrecare pregiudizio a un terzo per scongiurare un danno più grave al bene vita del conducente e dei trasportati[81].
Di fatti, la norma dell'articolo 2054 c.c. rispecchia quasi integralmente il contenuto dell'articolo 54, comma 1°, del codice penale, mantenendo inalterati i presupposti costitutivi pur manifestando una declinazione differente degli effetti: mentre, nell'ambito penale, lo stato di necessità opera da esclusione della punibilità dell'agente, nel campo civile esso si configura secondo una logica equitativa, che conferisce al giudice il potere di ridurre il risarcimento ad indennizzo, previa comparazione degli interessi in conflitto. Permane, tuttavia, il dibattito giurisprudenziale e dottrinale, in quanto sussiste il quesito se tale istituto debba essere interpretato come un'esclusione dell'ingiustizia del danno per la sua intrinseca antigiuridicità oggettiva, rientrando così nell'ambito della responsabilità derivante da un atto lecito dannoso, oppure se esso costituisca un illecito, nella cui configurazione la differenza rilevi unicamente nell'ordinamento delle conseguenze giuridiche, traducendosi appunto in un indennizzo in luogo di un pieno risarcimento; alcuni studiosi,

79. Il *Trolley Problem*, nella versione elaborata da Judith Jarvis Thomson, è un celebre esperimento mentale utilizzato per esplorare i principi della responsabilità morale e i limiti del ricorso al criterio utilitarista secondo cui il fine giustifica i mezzi. L'ipotesi riguarda un individuo che può deviare un tram fuori controllo su un binario secondario, salvando cinque persone a costo di provocare intenzionalmente la morte di una sola. Questo scenario solleva questioni profonde, mettendo a confronto le teorie deontologiche, che vietano di trattare l'essere umano come mezzo per un fine, con quelle consequenzialiste, che giustificano il sacrificio del singolo per un beneficio collettivo. In chiave giuridico-filosofica, il problema tocca la legittimità dell'azione lesiva in funzione di un male minore, e apre a interrogativi cruciali sul nesso tra causalità, imputazione soggettiva e il ruolo della dignità umana come argine al calcolo puramente numerico dell'etica. J.J. THOMPSON, T*he Trolley Problem*, in *Yale Law Journal*, 1985, v. 94, https://doi.org/10.2307/796133, p. 1415: "It is plausible to think that the present tense matters because the question for the agent at the time of acting is about the present, viz., "What may I here and now do?" and because that question is the same as the question "Which of the alternatives here and now open to me may I choose?" The alternatives now open to the second surgeon are: kill five or kill one. If killing five is worse than killing one, then perhaps he ought to, but at any rate he may, kill the one",
80. Cfr. M. FRANZONI, *L'illecito*, in *Tratt. Franzoni*, cit.; cfr. M. BRIGUGLIO, *Lo stato di necessità nel diritto civile*, Padova, 1963, p. 146; cfr. B. TROISI, *Lo stato di necessità nel diritto civile*, Napoli, 1988, p. 92.
81. European Commission: Directorate-General for Research and Innovation, *Ethics of connected and automated vehicles – Recommendations on road safety, privacy, fairness, explainability and responsibility*, Publications Office, 2020, cit.: "Consider, as a first topic, the safety of CAVs. An academic and public debate on so-called "moral dilemmas" with automated vehicles has vividly shown that crash avoidance by CAVs is not only a technical challenge but also an ethical and societal one. Dilemma situations are rare accident scenarios in which a highly automated CAV finds itself confronting an unavoidable crash and yet has the possibility of choosing between the road users that will be harmed by the event (e.g. a group of pedestrians, or the CAV's occupant)"; cfr. J.F. BONNEFFON, A. SHARIFF, I. EAHWAN, *The social dilemma of autonomous vehicles*, 2016, https://doi.org/10.1126/science.aaf2654 (ultimo accesso 13/04/2025).

infatti, propongono di inquadrare lo stato di necessità quale fonte tipica di responsabilità civile di natura equitativa, finalizzata a conseguire un bilanciamento puntuale degli interessi in contrapposizione, il che determina, a sua volta, la distinzione tra una responsabilità di carattere oggettivo e un'altra concepita sulla base del criterio dell'imputazione dell'ingiustificato arricchimento[82].

Accanto a queste riflessioni ci si interroga anche sulla effettiva idoneità del sistema codicistico della responsabilità a reggere l'urto delle trasformazioni tecnologiche in corso. L'articolo 2054 c.c., concepito in un'epoca in cui la presenza di un conducente umano rappresentava un presupposto ineludibile, si rivela oggi strutturalmente inadeguato a regolare situazioni in cui la condotta, la colpa, il controllo diretto dell'agente umano viene meno, sostituito da una serie di processi decisionali eterodiretti e affidati a *software* complessi, privi di intenzionalità in senso giuridico. L'ipotesi di colmare questa lacuna attraverso un'inversione dell'onere della prova a carico del presunto danneggiante si rivela insufficiente. Tale soluzione, se applicata rigidamente, presuppone infatti la possibilità di identificare un soggetto che abbia avuto il controllo del mezzo e che sia in grado di fornire una ricostruzione alternativa dei fatti, idonea a escluderne la responsabilità. Nei veicoli a guida automatizzata, però, la funzione di guida non è più esercitata da un soggetto umano, bensì da un sistema tecnologico inaccessibile, il cui funzionamento sfugge alla comprensione tanto dell'utilizzatore quanto dell'eventuale danneggiante. Di conseguenza, l'inversione dell'onere probatorio rischia di diventare uno strumento puramente formale, incapace di garantire una tutela sostanziale. L'utente di un veicolo automatizzato si trova, in effetti, in una condizione di affidamento assoluto: utilizza un prodotto altamente sofisticato, la cui opacità funzionale lo priva della possibilità di intervento, ma anche di difesa. In tale contesto, diventa necessario elaborare un regime giuridico incentrato su una protezione rafforzata, capace di riequilibrare la sproporzione tra chi subisce un danno e chi detiene il potere tecnologico e informativo. Un simile approccio impone il superamento della logica colposa a favore di modelli fondati sulla mera sussistenza del nesso causale tra funzionamento del mezzo e verificazione dell'evento dannoso. La riconduzione di tale responsabilità in capo al produttore, al fornitore di tecnologia o a qualsiasi altro soggetto che tragga profitto dall'immissione sul mercato di tali sistemi, appare non solo giuridicamente coerente, ma anche socialmente necessaria nella

82. Sulla funzione surrogatoria, v. Corte di Cassazione, sez. III, 18 novembre 2010 n. 23275, *inedita*: "L'art. 2045 cod. civ., laddove riconosce in favore del danneggiato un'indennità nell'ipotesi in cui chi ha compiuto il fatto dannoso abbia agito in stato di necessità, ha una funzione surrogatoria od integratrice, avendo lo scopo di assicurare al danneggiato un'equa riparazione; ne consegue che non è affetta da violazione di legge la sentenza con cui il giudice d'appello, individuati nel fatto gli estremi dello stato di necessità e corretta in tal senso la motivazione della prima sentenza (che, invece, aveva attribuito al danneggiante la responsabilità risarcitoria ai sensi dell'art. 2043 cod. civ.), esercitando il proprio giudizio equitativo, liquidi in favore del danneggiato, a titolo di indennità, la stessa somma di danaro che il primo giudice aveva liquidato a titolo risarcitorio. (Rigetta, App. Venezia, 25/03/2005)".

prospettiva di una responsabilità distribuita. La guida automatica, lungi dal rappresentare una mera evoluzione meccanica, segna un passaggio epocale nella struttura della responsabilità civile, che non può più fondarsi esclusivamente su categorie novecentesche. L'emergere di entità non umane capaci di determinare autonomamente il corso degli eventi impone l'adozione di una nuova grammatica giuridica, capace di cogliere l'essenza della vulnerabilità digitale del consumatore e di offrire soluzioni strutturalmente orientate alla tutela effettiva. Soltanto una risposta normativa organica, fondata su criteri di responsabilità distributiva e non meramente soggettiva, può restituire equilibrio a un rapporto in cui il potere tecnologico tende a dissolvere la centralità della persona, e con essa, la sua tradizionale posizione giuridica. Appare necessario, al netto di ogni discussione, preservare e rafforzare l'autonomia umana, limitando e rendendo intrinsecamente revocabile l'autonomia conferita alle macchine, soprattutto quando essa rischi di pregiudicare il predominio del giudizio umano. Questo scenario richiama il concetto di meta-autonomia, intesa quale struttura decisionale che regola il processo di delega; in tale ambito, l'essere umano conserva il potere di stabilire quali decisioni debbano essere assunte direttamente e in quali circostanze possa essere lecito cedere parte di tale prerogativa, qualora, per ragioni di efficienza o altre priorità operative, risulti vantaggioso[83]. Nel contesto dei veicoli autonomi, questa prospettiva implica lo sviluppo di sistemi che non si limitino a seguire algoritmi predefiniti, ma siano capaci di apprendere e rivalutare continuamente i propri protocolli decisionali. La meta-autonomia diventa così un meccanismo di auto-riflessione etica, che consente alla macchina di valutare la correttezza delle proprie azioni in un contesto dinamico e imprevedibile[84]. Tuttavia, ogni delega deve essere concepita come una concessione temporanea e rivedibile che non pregiudichi in alcun modo il diritto fondamentale di riprendere il controllo decisionale, garantendo all'agente umano di poter decidere nuovamente[85].

Concludendo, è ineludibile come il diritto e l'etica non possano più limitarsi a rincorrere il progresso, sopraggiungendo solo quando siano state compiute scelte sbagliate, nel tentativo di recuperare errori, ma devono assumere un ruolo centrale nella sua *governance*, trasformandosi, nel solco indicato dal legislatore europeo, da mero regolatore *ex post* a strumento di orientamento e indirizzo *ex ante* delle innovazioni tecnologiche[86]. La mobilità intelligente non è solo una frontiera ingegneristica, ma anche una sfida etica e giuridica che impone un ripensamento strutturale

83. Cfr. L. FLORIDI, J. COWLS, M. BELTRAMETTI, R. CHATILA, *AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, p. 689 ss., https://doi.org/10.1007/s11023-018-9482-5 (ultimo accesso 03/06/2025); Cfr. S.C. MATTEUCCI, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. Pubbl.*, n.1, 2019, p. 5 ss., https://doi.org/10.1438/93718 (ultimo accesso 03/06/2025).

84. Cfr. L. FLORIDI, *The Logic of Information: A Theory of Philosophy as Conceptual Design*, 2019, OUP Oxford.

85. Cfr. L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., p. 98.

86. Cfr. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivisita di BioDiritto*, n.1, 2019, p. 63 ss.

delle categorie della responsabilità e della tutela dei diritti fondamentali, anche prevedendo sistemi di *liability* in discontinuità con i modelli tradizionali[87], affinché l'evoluzione tecnologica non si traduca nell'ennesimo vuoto normativo, ma, *de iure condendo*, in un equilibrio dinamico tra progresso, sostenibilità e garanzie sociali. In tale cornice concettuale, il progresso tecnologico, superando lo standard di verità provata e obiettiva, si profila come "un sapere motivato da un proposito più esteso, coinvolgente l'intero destino dell'essere umano"[88]. È di tutta evidenza che questa volta, la nottola di Minerva dovrà, per tutti, alzarsi in volo prima che faccia buio e non quando le ombre del crepuscolo hanno già iniziato a riempire il cielo di chiaroscuri[89]!

87. Cfr. K.S. ABRAHAM, R.L. RABIN, *Automated Vehicles and Manufacturer Responsibility for Accidents: a new legal regime for a new era*, in *Va. J. Int'l L.*, n. 105, 2019, https://law.stanford.edu/wp-content/uploads/2018/04/automated-vehicles-article-SSRN-version-pdf-3-28-18.pdf (ultimo accesso 10/04/2025).

88. Cfr. P. ZELLINI, *Il teorema di Pitagora*, Milano, 2023, p. 17, in A. COLAMEDICI, S. ARCAGNI, *L'algoritmo di Babele*, Milano, 2024, p. 128.

89. "Del resto, a dire anche una parola sulla dottrina di come dev'essere il mondo, la filosofia arriva sempre troppo tardi. Come pensiero del mondo, essa appare per la prima volta nel tempo, dopo che la realtà ha compiuto il suo processo di formazione ed è bell'e fatta. Questo, che il concetto insegna, la storia mostra, appunto, necessario: che, cioè, prima l'ideale appare di contro al reale, nella maturità della realtà, e poi esso costruisce questo mondo medesimo, colto nella sostanza di esso, in forma di regno intellettuale. Quando la filosofia dipinge a chiaroscuro, allora un aspetto della vita è invecchiato, e, dal chiaroscuro, esso non si lascia ringiovanire, ma soltanto riconoscere: la nottola di Minerva inizia il suo volo sul far del crepuscolo", G. W. F. HEGEL, *Lineamenti di filosofia del diritto*, Bari, 1965, p. 14 ss.