AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-7| 2026 Published: |30-07-2026|

FROM HUMAN DRIVER TO ALGORITHM: RETHINKING LEGAL STANDARDS FOR AUTONOMOUS VEHICLES

https://doi.org/10.5281/zenodo.21398792

Raximova Zilola Shuhratjon qizi
3rd-year student, Public Safety University of Uzbekistan Email: rahimovazilola04@gmail.com

Abstract

The rapid development of autonomous vehicle (AV) technologies presents significant legal, ethical, and regulatory challenges that existing legal frameworks are not fully equipped to address. This study examines the necessity of establishing comprehensive liability, cybersecurity, and ethical governance mechanisms for high-level autonomous driving systems (Levels 3–5). It highlights the importance of advanced Event Data Recorders (EDRs) to ensure transparency and accountability by capturing pre-incident sensor data and algorithmic decision-making processes, while also safeguarding user data ownership and privacy rights. Furthermore, the paper explores systemic cybersecurity risks, advocating for the creation of state-backed reinsurance pools to mitigate large-scale damages caused by mass hacking or system failures.

A key focus is placed on algorithmic bias, emphasizing the need for mandatory ethical audits of machine-learning models to prevent discriminatory outcomes in safety-critical environments. The study also proposes a set of forward-looking legal reforms tailored to the Uzbek legal system, including amendments to the Civil, Criminal, and Administrative Codes. These reforms aim to classify autonomous driving systems as sources of increased danger, introduce liability for software manipulation and failure to update safety systems, and establish accountability for fleet operators. Additionally, the paper recommends adopting a “reasonable computer driver” standard, shifting legal evaluation from human-centered benchmarks to technologically feasible industry standards. By integrating these measures, Uzbekistan has the opportunity to develop a coherent and proactive regulatory framework that enhances public safety, fosters innovation, and attracts investment in autonomous mobility.

Keywords

Autonomous Vehicles; Artificial Intelligence; Legal Liability; Cybersecurity; Algorithmic Accountability; Data Governance; Event Data Recorders; Algorithmic

Bias; Machine Learning Ethics; Transport Law; Legal Reform; Emerging Legal Systems.

Introduction

The global transportation sector is undergoing a transformative shift unparalleled since the advent of the internal combustion engine. Autonomous vehicles (AVs), driven by rapid advancements in artificial intelligence (AI), machine learning, and sensor technologies, are transitioning from experimental prototypes to operational systems on public roadways. Once confined to speculative fiction, automated driving systems (ADS) are now embedded in modern vehicles through a continuum of automation levels, ranging from driver assistance to full autonomy. This technological evolution not only promises to redefine mobility but also challenges the foundational principles of legal liability and regulatory governance (Riehl, 2018).

One of the primary motivations behind the development of AVs is the urgent need to enhance road safety. Empirical evidence consistently demonstrates that human error is a contributing factor in approximately 90% to 94% of all traffic accidents (National Highway Traffic Safety Administration [NHTSA], n.d.). In the United States alone, motor vehicle crashes result in an estimated 32,000 to 37,000 fatalities annually, making them one of the leading causes of death, particularly among younger populations (NHTSA, n.d.). Proponents of autonomous driving technologies argue that replacing human drivers—who are susceptible to fatigue, distraction, and impaired judgment—with algorithmic systems capable of real-time data processing could significantly reduce accident rates. Some projections suggest that widespread adoption of AVs could prevent up to 90% of traffic accidents, potentially saving tens of thousands of lives each year (Brookings Institution, 2025).

Despite these promising benefits, the rapid advancement of AV technology has outpaced the evolution of legal frameworks designed to regulate it. Traditional traffic law is inherently human-centric, grounded in negligence principles that assign liability based on a driver's failure to exercise reasonable care. However, as vehicles progress along the Society of Automotive Engineers (SAE) automation spectrum—from Level 0 (no automation) to Level 5 (full automation)—the role of

the human driver diminishes and, in some cases, disappears entirely. At higher levels of automation, particularly Levels 4 and 5, vehicles are capable of performing all driving functions either under specific conditions or universally, raising fundamental questions about who—or what—should be held legally responsible in the event of an accident (Kim, 2020).

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-7| 2026 Published: |30-07-2026|

This shift introduces a paradigm transition from negligence-based liability toward product liability frameworks. In a fully autonomous environment, liability is likely to migrate from individual drivers to manufacturers, software developers, and system designers. Under product liability doctrines, claims may arise from manufacturing defects, design defects, or failures to warn users about potential risks. Unlike negligence, strict liability does not require proof of fault but instead focuses on whether the product itself is defective and unreasonably dangerous (Bose, 2015). This transformation presents significant challenges for courts, as determining causation in accidents involving complex AI systems requires technical expertise and access to proprietary data. A critical factor in resolving such disputes is the emergence of Event Data Recorders (EDRs), often referred to as "black boxes." These devices record crucial data regarding vehicle performance, sensor inputs, and algorithmic decisions in the moments leading up to a collision. EDRs provide an objective basis for reconstructing accidents, enabling investigators to distinguish between human error, system malfunction, and environmental factors. As such, they play an essential role in bridging the evidentiary gap between traditional liability frameworks and technologically driven incidents (Bose, 2015).

Most engineer-respondents to studies by the Institute of Electrical and Electronics Engineers (IEEE) and Information Handling Services (IHS)[22] believe that manufacturers will remove rear-view mirrors, horns, and emergency brakes by 2030—and steering wheels and gas/ brake pedals will be gone by 2035.[23] Some estimate that our fully driverless future will arrive around 2050.24 In the near term, the automated-driving transition will likely be gradual, moving along a spectrum from fully manual to partial assistance to fully automated. This gradation was standardized in 2013, when the international engineering vehicle-standards organization Society of Automotive Engineers (SAE) International25 defined the levels of driving automation.[26] In September 2016, NHTSA— which had in 2013 created its own distinct definitions, using only four levels—adopted the SAE's levels and definitions. By September 2017, federal regulators had evolved the automation-level definitions to the following: L0 No automation. Zero autonomy; the driver performs all driving tasks. L1 Driver assistance. Vehicle is controlled by the driver, but some driving assist features (e.g., steering, speed) may be included in the vehicle design. L2 Partial automation. Vehicle has combined automated functions (e.g., acceleration and steering), but the driver must remain engaged with the driving task and monitor the environment at all times. L3 Conditional automation. Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice. L4 High automation. The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle. L5 Full automation. The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Exhibit 4 — Potential Responsibility for Automated Vehicle Accidents

Automated-driving crashes are inevitable, so courts will likely need to determine the legal and factual standards for determining liability. Depending on the automation level, the legal and factual analyses will likely differ substantially from today's legal analyses. Fully manual Level 0 is the status today, and Level 5 will be our autos' self-driving future. But in the interim, much of the litigation will focus on Levels 1–4. As long as humans and computers are co-pilots, determining "cause" will become increasingly complex. Even in these early days, we see human-machine finger pointing playing out. In January 2018, a driver arrested for drunk driving apparently explained that his "Tesla had been set on autopilot." Tesla responded that its autopilot function should be used "only with a fully attentive driver."104 These claims will continue. During this time of transitional human-machine cooperation, insurance and litigation will likely develop criteria for determining a crash's cause(s). Did the human override the computer? Was the human paying attention—and to a sufficient degree? Did the computer properly alert the human? Did the computer notify the human early enough? Did the computer misinterpret data? The fact-specific queries and aggregate test cases to determine liability will likely be crafted by insurers, litigators, and regulators

Literature review

The issue of liability in autonomous vehicles (AVs) has attracted significant scholarly attention across legal, technological, and policy-oriented disciplines. Existing literature reflects a broad consensus that the emergence of artificial intelligence (AI)-driven transportation systems fundamentally challenges traditional liability frameworks, particularly those grounded in human agency and negligence.

1. Evolution of Liability Frameworks: From Negligence to Product Liability

A central theme in the literature is the transition from driver-centric negligence models toward product liability regimes. Traditional tort law assigns responsibility based on a driver's failure to exercise reasonable care. However, as automation increases, the human driver's role diminishes, necessitating a reallocation of liability.

Scholars emphasize that at lower levels of automation (SAE Levels 0–2), liability remains primarily with the human driver. In contrast, at higher levels (Levels 3–5), responsibility increasingly shifts toward manufacturers and software developers . This shift is reinforced by systematic reviews indicating that AV adoption leads to a structural migration of liability from individuals to technological systems and their producers .

Legal scholars such as Kingston (2018) further debate whether AI systems should be treated as products or services, noting that this classification significantly influences applicable liability doctrines. While product liability allows strict liability claims for defective systems, negligence frameworks require proof of fault, which becomes increasingly complex in AI-driven environments .

2. Complexity of Causation and Multi-Actor Responsibility

Another major strand of literature addresses the problem of causation in AV-related accidents. Unlike traditional collisions, AV incidents involve multiple actors, including manufacturers, programmers, vehicle owners, and even data providers.

Comparative legal studies highlight that liability attribution remains fragmented across jurisdictions. For example, some countries adopt strict safety-based liability systems, while others rely on hybrid approaches combining negligence and product liability . This fragmentation creates uncertainty, particularly in cross-border contexts and global markets.

Game-theoretic and policy-oriented research further demonstrates that improper liability allocation may create moral hazard, where human drivers behave less cautiously in the presence of automated systems. Therefore, optimal liability design is crucial not only for justice but also for maintaining road safety and public trust .

3. Regulatory Gaps and Global Policy Responses

The literature consistently identifies a regulatory lag behind technological innovation. Governments worldwide have adopted cautious and often non-binding approaches to AV regulation, prioritizing innovation over strict legal enforcement.

Studies show that most jurisdictions rely on soft law instruments, such as guidelines and pilot programs, rather than comprehensive statutory frameworks . While countries like Germany and the United Kingdom have introduced more structured legal regimes, many others continue to operate within fragmented or experimental regulatory environments.

Additionally, scholars argue that the coexistence of autonomous and human-driven vehicles during the transition period introduces further legal ambiguity, particularly in determining shared liability and operational responsibility .

4. Ethical and Algorithmic Liability

A growing body of research explores the ethical dimensions of AV decision-making, particularly in unavoidable accident scenarios. These discussions often center on algorithmic responsibility and the so-called “moral machine” problem.

Autonomous systems rely on complex algorithms to process environmental data and make real-time decisions, often more efficiently than human drivers. However, this capability introduces new forms of risk, including biased decision-making and lack of transparency .

Scholars argue that embedding ethical decision-making into algorithms may expose developers to pre-programmed liability, as decisions are no longer spontaneous but intentionally designed. This raises fundamental questions about accountability, foreseeability, and legal responsibility.

5. Emerging Role of Insurance and Economic Implications

The literature also highlights significant transformations in the insurance sector. As liability shifts toward manufacturers, traditional motor insurance models based on driver risk are expected to decline.

Research suggests that product liability insurance and corporate risk models will replace individual coverage, fundamentally reshaping the economics of transportation systems . This transition may also influence consumer adoption rates, as clearer liability rules tend to increase public trust in AV technologies.

6**. Uzbek Perspective: AI Regulation and Legal Development**

Recent Uzbek legal scholarship increasingly recognizes artificial intelligence (AI) as a new object of legal regulation, particularly in relation to liability and risk governance. Early doctrinal work by Uzbek researchers emphasizes that AI should be treated not as a legal subject, but as a technological instrument requiring human accountability. For example, S. Tuhtamirzaev (2025) argues that AI introduces “new legal risks affecting individuals, society, and state institutions,” and therefore requires the adoption of a specialized Law on Artificial Intelligence in Uzbekistan His work highlights: the absence of clear liability allocation mechanisms, the growing societal risks of AI misuse,and the urgency of legislative reform.

Similarly, research emerging from the Cyber Law scientific school at Tashkent State University of Law emphasizes that AI regulation must be grounded in national legal traditions while incorporating global standards These scholars advocate a doctrinal (normative) approach, focusing on adapting civil and administrative liability principles.

While the majority of AV liability literature focuses on developed jurisdictions, emerging economies such as Uzbekistan are increasingly engaging with AI-related legal challenges.

Recent legislative developments in Uzbekistan demonstrate a proactive approach to regulating artificial intelligence, particularly in relation to data protection and accountability. In 2025, Uzbekistan introduced draft legislation aimed at defining AI in legal terms, establishing liability for misuse, and protecting personal data .

Although specific regulations on autonomous vehicles remain underdeveloped, Uzbek scholars and policymakers emphasize:

the need for clear accountability mechanisms in AI systems

the importance of data governance and privacy protection

and the adoption of international best practices in liability frameworks

Methodology

Research Design and Qualitative FrameworkThis study adopts a qualitative research design to explore the evolving legal infrastructure surrounding autonomous vehicles (AVs). The central focus is the "Liability Rubicon" crossed at SAE Level 4 and Level 5, where the human driver is no longer the primary legal actor [1, 2]. Through qualitative synthesis, the research evaluates the theoretical shift from human-centric negligence to a "computer driver" legal construct, interpreting how algorithmic performance replaces personal conduct as the core of legal inquiry [2, 3]

Doctrinal Legal ResearchThe doctrinal component involves a systematic analysis of established tort principles, including negligence, strict product liability, and vicarious liability 4-6. The study examines how traditional "duty of care" standards are being adapted for systems that lacks human "intent" [7, 8]. A significant portion of this research analyzes the transition of fault from the actions of an operator to the design and functionality of the system [2, 9]. This includes assessing the "Reasonable Human Driver" standard versus the "Reasonable Computer Driver" standard to determine which benchmarks effectively promote public safety [3, 10, 11]. Comparative Legal AnalysisA comparative framework is utilized to contrast decentralized regulatory models, such as the United States' "patchwork" of state laws, with more unified statutory approaches in Europe and Asia [12-14]. Key legislative instruments analyzed include the United Kingdom's Automated and Electric Vehicles Act (AEVA) 2018, Germany's Remote Control Act (StVFernLV), and the European Union's new Product Liability Directive (PLD) [13, 15, 16]. This comparison highlights how different jurisdictions manage the shift toward manufacturer liability and the role of "authorized self-driving entities" [13, 17].

Case Study Methodology to test theoretical frameworks against real-world failures, the research employs a case study approach focused on notable incidents. This includes the 2018 Uber Tempe crash, which serves as the seminal example of the "responsibility gap" in semi-autonomous modes . Additionally, the 2018 Tesla crash involving Walter Huang and the landmark Benavides v. Tesla (2025) verdict are analyzed to understand how courts handle design-defect theories and foreseeable misuse .

Data Collection: Forensic Telemetry and Secondary SourcesData collection relies on two primary pillars:

Forensic Data Analysis: The study evaluates the role of Event Data Recorders (EDRs) as the vital "black box" solution for crash reconstruction. This includes analyzing telemetry from LIDAR, radar, and sensor fusion to establish causation between human error and system malfunction.

Discussion

The Evolution of Fault: From Negligence to Strict LiabilityThe transition to higher levels of autonomy necessitates a seismic shift in the legal paradigm. For Level 1 through Level 3 systems, the human operator remains part of the safety-critical loop, and negligence remains the relevant framework. However, as vehicles reach Level 4 and Level 5, the "operator" is no longer a human in the driver's seat but an algorithm [1, 3]. Proving negligence in complex, proprietary AI code presents an "uphill battle" for plaintiffs [9, 39]. Consequently, strict product liability is widely considered the most appropriate framework for full autonomy, as it focuses on whether the product was defective rather than whether the manufacturer exercised "all possible care" [9, 40, 41].

Forensic Clarity and the "Black Box" ArbiterThe implementation of mandatory Event Data Recorders (EDRs) is the primary solution to "human-machine finger-pointing" [25, 26]. At a nominal cost of $20 per vehicle, advanced EDRs record high-resolution telemetry that reveals the vehicle's perception path and algorithmic intent [25, 42, 43]. This forensic data allows investigators to distinguish between software bugs, hardware failures, and improper human intervention [25, 44, 45]. Without such transparency, the informational asymmetry between manufacturers and victims would stifle consumer trust and legal recourse . central point of contention is whether an AI system should be judged against a "reasonable human driver" or a "reasonable computer driver" standard [3, 10]. The human standard provides a familiar baseline for juries but may be too lenient for technology marketed as "super-human" [48, 49]. Conversely, a "reasonable computer driver" standard benchmarks performance against industry "state-of-the-art" technical feasibility [3, 10]. To bridge this gap, the "AI-Chaperone Liability" model assigns responsibility to the entity with supervisory authority over the AI—ensuring that victims are compensated even if a specific "bug" cannot be isolated in code [5, 50]. Economic and Insurance Marketplace DisruptionThe insurance industry faces inevitable disruption as the "responsibility of driving" shifts from humans to machines . Personal auto insurance, which historically dominated the market, is projected to shrink significantly, while commercial and product liability lines will grow [38]. Underwriting will pivot from assessing human risk factors, such as age and history, to evaluating the reliability of specific hardware and software versions . However, insurance severity may rise, as minor collisions now involve expensive exterior sensor suites that require complex recalibration

Ethical Programming and Algorithmic Bias AVs introduce "ghoulish" ethical dilemmas, specifically the "trolley problem," where algorithms must be programmed to prioritize certain lives in unavoidable collisions . Furthermore, evidence of algorithmic bias—where systems are less effective at detecting pedestrians with darker skin—exposes manufacturers to both tort and civil rights litigation. Mandatory audits of machine-learning datasets are essential to identify and mitigate these discriminatory outcomes before they result in tragedy . Integrating Autonomy into the Uzbekistan Legal SystemWhile international models like the UK AV Act provide advanced frameworks, a localized gap remains in Uzbekistan [34, 35]. Local scholarship has focused on general AI ethics, but the Uzbekistan Civil Code (e.g., Article 1017) must be updated to specifically address AV liability and forensic data protocols [34, 35]. Transitioning to a model of strict liability for "AI-Chaperones" in the domestic context would provide the legal clarity necessary for manufacturers to invest in the region while ensuring public safety.

Conclusion and Recommendations

Closing the Responsibility Gap: A Summary of Findings The transition toward fully autonomous vehicles (AVs) represents a "seismic shift" in transportation that current legal frameworks are largely unprepared to navigate 1, 2. This study has demonstrated that as human control is phased out in SAE Level 4 and 5 systems,

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-4| Issue-7| 2026 Published: |30-07-2026|

the traditional "negligence" model—which relies on a human driver's duty of care—becomes an "uphill battle" for victims seeking redress 3-5. Proponents emphasize that this transition could save up to lives annually by mitigating the human errors responsible for 94% of crashes [6, 7]. However, the absence of a "human in the loop" necessitates a move toward strict product liability, where manufacturers and developers are held responsible for algorithmic failures regardless of intent [4, 8, 9]. The research further identifies the critical role of forensic telemetry. Investigations into real-world accidents, such as the 2018 Uber Tempe crash, prove that without data from Event Data Recorders (EDRs), it is nearly impossible to distinguish between a software bug and improper human backup intervention 10, 11. Economically, the insurance market is poised for a massive pivot; as personal auto policies shrink, commercial product liability will expand to cover automated fleets [12, 13]. Finally, the study highlights a "responsibility gap" where traditional vicarious liability fails to address the unique human-machine relationship, leading to the proposal of the AI-Chaperone Liability model [14, 15].

Strategic Policy Recommendations

To successfully integrate autonomous systems into the social fabric, the following data-driven and legally grounded recommendations are proposed:

1. Codify AI-Chaperone Liability as a New Strict Liability TortLegislators should establish a specific legal construct for entities—individuals or corporations—that have supervisory authority or the power to override an AI system [14, 16]. This "AI-Chaperone" model ensures that victims are compensated by the party that engages the technology for a "traditionally human task," such as driving, even if a specific coding defect cannot be pinpointed [17, 18]. This prevents manufacturers from using "technical complexity" as a shield against liability [19].

2. Standardize "Minimal Risk Maneuver" and Handover ProtocolsFor Level 3 systems, regulatory bodies must mandate a minimum 10-second handover window 3, 20. If the driver fails to respond within this period, the vehicle must be programmed to execute a "minimal risk maneuver"—independently bringing the car to a controlled stop, ideally outside active traffic lanes

. Clear indicators (visual, auditory, and haptic) must alert occupants of the system's status and any request for control transition.

3. Mandate Advanced Event Data Recorders (EDRs)Governments must require all Level 3–5 vehicles to carry EDRs that record at least 30 seconds of high-resolution sensor data (LIDAR, radar) and "algorithmic intent" prior to impact . To protect consumer trust, the law should establish that this data belongs to the

vehicle owner and prohibit commercial data mining without explicit, informed consent [28, 29].

4. Establish National Reinsurance Pools for Mass-Hacking EventsTo address the systemic risk of cybersecurity breaches—where an entire fleet could be compromised simultaneously—nations should create state-backed reinsurance pools similar to the UK's "Pool Re" or "Flood Re" models . This would provide a guarantee fund for victims of cyber-terror or mass-malfunction where the financial burden would be too great for a single insurer or manufacturer [33, 34].

5. Mandatory Ethical Audits for Algorithmic BiasManufacturers must be required to perform routine audits on their machine-learning training sets [35, 36]. Studies indicating that some object-detection models are 5% less effective at identifying pedestrians with darker skin must be addressed through mandatory diverse dataset requirements to prevent discriminatory safety outcomes [37, 38].

Integration into the Uzbekistan Legal System

Uzbekistan is in a unique position to adopt "forward-looking" legislation that avoids the regulatory "patchwork" seen in the United States. To modernize the Uzbek Civil Code, the following domestic reforms are recommended:

Amend Article 1017 of the Civil Code: Explicitly categorize high-level autonomous driving software as a "source of increased danger" subject to strict liability, ensuring that manufacturers bear the burden of proof in the event of an accident [41, 42].

Update the Criminal Code (Chapter XXI): Introduce new categories for "Information Technology Crimes" that specifically address the unlawful modification of autonomous transport software or the failure of a manufacturer to provide "safety-critical" updates [43, 44].

Reform the Administrative Code (Chapter XI): Add administrative penalties for "AI-Chaperones" (fleet operators) who fail to monitor system engagement or disable factory safety features, such as emergency braking, as seen in the Uber case [11, 43].Local courts should move away from human-centric benchmarks and judge AV performance against the "state-of-the-art" technical feasibility available in the global industry [45, 46].

By embracing these forensic and algorithmic liability standards, Uzbekistan can create a stable, predictable legal environment that attracts investment while ensuring the highest level of protection for its citizens.

REFERENCES:

1. Anderson, J. M., Kalra, N., Stanley, K. D., Sorensen, P., Samaras, C., & Oluwatola, O. A. (2016). Autonomous vehicle technology: A guide for policymakers. RAND Corporation.

2. Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., & Rahwan, I. (2018). The moral machine experiment. Nature, 563(7729), 59–64. https://doi.org/10.1038/s41586-018-0637-

3. Bagloee, S. A., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous vehicles: Challenges, opportunities, and future implications. Transportation Research Part C, 69, 299–308.

4. Bonnefon, J. F., Shariff, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. Science, 352(6293), 1573–1576.

5. Bose, U. (2015). Liability issues in autonomous vehicle technology. Santa Clara Law Review, 56(2), 215–245.

6. Brookings Institution. (2025). Autonomous vehicles and transportation safety.

7. Calo, R. (2015). Robotics and the lessons of cyberlaw. California Law Review, 103(3), 513–563.

8. Casey, B. W., & Niblett, A. (2016). Self-driving laws. University of Toronto Law Journal, 66(4), 429–442.

9. Chagal-Feferkorn, K. (2015). Am I an algorithm or a product? Santa Clara High Technology Law Journal, 31, 99–140.

10. Clarke, R. (2019). Regulatory challenges of autonomous vehicles. Computer Law & Security Review, 35(2), 105–112.

11. European Commission. (2022). Proposal for a directive on AI liability.

12. European Parliament. (2020). Civil liability regime for artificial intelligence.

13. Gurney, J. K. (2013). Sue my car not me. University of Illinois Journal of Law, Technology & Policy, 247–277.

14. Hevelke, A., & Nida-Rümelin, J. (2015). Responsibility for accidents. Science and Engineering Ethics, 21(3), 619–630.

15. HLEG AI. (2019). Ethics guidelines for trustworthy AI. European Commission.

16. Kalra, N., & Paddock, S. (2016). Driving to safety. Transportation Research Record, 2673, 1–9.

17. Kim, T. (2020). Liability frameworks for AVs. Journal of Law & Technology, 35(2), 112–130.

18. Kingston, J. (2018). Artificial intelligence and legal liability. In Research handbook on AI law.

19. Kroll, J. A., Huey, J., Barocas, S., Felten, E., Reidenberg, J., Robinson, D., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165, 633–705.

20. Lin, P. (2016). Why ethics matters. In Autonomous driving. Springer.

21. Marchant, G. E., & Lindor, R. A. (2012). Autonomous vehicles and liability. Santa Clara Law Review, 52, 1321–1340.

22. McCarthy, J. (2007). What is artificial intelligence? Stanford University.

23. National Highway Traffic Safety Administration. (2020). Automated vehicles for safety.

24. OECD. (2021). Artificial intelligence in society. OECD Publishing.

25. Parschau, T., & Hitchens, M. (2019). AV legal frameworks. Computer Law & Security Review, 35(2), 225–233.

26. Petit, N. (2017). Law and regulation of AI. European Journal of Risk Regulation, 8(3), 1–15. 27. Riehl, B. (2018). Legal implications of AVs. Harvard Journal of Law & Technology, 31, 567–590.

28. SAE International. (2018). J3016 automation levels.

29. Shavell, S. (2007). Economic analysis of accident law. Harvard University Press.

30. Smith, B. W. (2017). Automated driving and liability. Michigan State Law Review, 1–74.

31. Solum, L. B. (1992). Legal personhood for AI. North Carolina Law Review, 70, 1231–1287.

32. Stilgoe, J. (2018). Governance of self-driving cars. Social Studies of Science, 48(1), 25–56.

33. Tuhtamirzaev, S. (2025). AI legal risks in Uzbekistan. Uzbek Legal Journal, 12(1), 45–60.

34. UK Parliament. (2018). Automated and Electric Vehicles Act.

35. UNECE. (2021). Automated lane keeping systems regulation.

36. Vellinga, N. E. (2017). Self-driving deployment. Computer Law & Security Review, 33(6), 847–863.

37. Vladeck, D. C. (2014). Machines without principals. Washington Law Review, 89, 117–150. 38. Wagner, G. (2018). Liability rules. European Review of Private Law, 26(5), 687–704.

39. Walker Smith, B. (2014). Automated vehicles legality. Texas A&M Law Review, 1, 411–521.

40. Yeung, K. (2018). Algorithmic regulation. Regulation & Governance, 12(4), 505–523.

41. Zhao, J., & Zhang, Y. (2020). AI liability challenges. AI & Society, 35, 1–10.

42. Evas, T. (2020). EU AI liability framework. European Parliamentary Research Service.

43. Floridi, L., et al. (2018). AI ethics principles. Minds and Machines, 28, 689–707.

44. Goodall, N. J. (2014). Ethical decision-making in AVs. Transportation Research Record, 2424, 58–65.

45. Koopman, P., & Wagner, M. (2017). Autonomous vehicle safety. SAE International Journal. 46. Nyholm, S., & Smids, J. (2016). Ethics of accidents. Ethical Theory and Moral Practice, 19, 1275–1289.

47. Pagallo, U. (2013). The laws of robots. Springer.

48. Scherer, M. U. (2016). Regulating AI systems. Harvard Journal of Law & Technology, 29, 353–400.

49. Selbst, A. D. (2017). Disparate impact in AI. Georgia Law Review, 52, 1–52.

50. Wischmeyer, T. (2020). AI and transparency. German Law Journal, 21, 223–245.