

Dual-Track Synergistic Regulation of Data and Algorithms in Connected and Autonomous Vehicles: A Systematic Literature Review

Jingwen Cai, Yifen Yin, Yuanyuan Yu, Haoqian Hu, Wai In Ho and Chunming Wang *

Faculty of Humanities and Social Sciences, Macao Polytechnic University, Macao 999078, China;
p2412135@mpu.edu.mo (J.C.); yfyin@mpu.edu.mo (Y.Y.); yyyu@mpu.edu.mo (Y.Y.);
p2413560@mpu.edu.mo (H.H.); p2105364@mpu.edu.mo (W.I.H.)

* Correspondence: p2424662@mpu.edu.mo

Abstract

Connected and Automated Electric Vehicles (CAEVs) are rapidly evolving into complex Cyber-Physical-Social Systems (CPSS), generating structural tensions between technological innovation and public safety. Current research in public governance exhibits significant fragmentation. Scholars frequently isolate data privacy compliance from algorithmic safety auditing, treating them as distinct silos. To bridge this gap, this study applies the PRISMA framework to systematically synthesize 135 core peer-reviewed articles, exposing the endogenous limitations of unidimensional regulatory paradigms. Our analysis yields three central insights. First, traditional “notice-and-consent” models fail under the ubiquitous data collection demands of modern V2X environments. Macro-level policies must translate into foundational Privacy-Enhancing Technologies (PETs) through “Law-as-Code” mechanisms. Second, the opacity of end-to-end algorithmic decision-making deconstructs traditional tort liability systems. This necessitates ex-ante quantitative auditing mechanisms—such as Explainable Artificial Intelligence (XAI) and enhanced Threat Analysis and Risk Assessment (TARA 2.0)—to mitigate adversarial attacks and physical-level safety hazards. Third, overcoming cross-national regulatory fragmentation requires constructing a “dual-track synergistic” governance architecture. This framework institutionalizes the coupling of data lifecycle quality workflows with the algorithmic Safety of the Intended Functionality (SOTIF). Ultimately, this review advocates for adaptive regulatory sandboxes and advances the harmonization and mutual recognition of global standards (e.g., ISO/SAE 21434, UN R155/156). Addressing current methodological and empirical data constraints, future academic inquiry must pivot. Researchers should target the value alignment challenges of Large Language Models (LLMs) in autonomous driving and implement multi-stakeholder participatory policy pilots designed to reconcile diverse social values.

Keywords: connected and automated electric vehicles; systematic literature review; dual-track synergistic regulation; data security governance; algorithmic accountability; Law-as-Code; socio-technical systems

Academic Editor: Grzegorz Sierpiński

Received: 29 May 2026

Revised: 11 July 2026

Accepted: 17 July 2026

Published: 18 July 2026

Copyright: © 2026 by the authors. Published by MDPI on behalf of the World Electric Vehicle Association. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction and Problem Statement

Connected and Automated Electric Vehicles (CAEVs) are undergoing a profound evolution from hardware-centric functionalities to software-defined architectures [1]. Operating as highly data-dependent “servgoods,” their core mechanism relies on algorithms to replicate, and progressively supplant, human driving agency [2,3]. Ceding control certainly aligns with the long-term vision of shared mobility in modern smart cities [4,5]. However, it inevitably integrates formerly closed physical vehicles entirely into open digital infrastructures. The deep convergence of underlying communication networks and in-vehicle sensors allows external threats against transportation systems to breach traditional physical boundaries, evolving into interdisciplinary coupled cyber-physical attacks [6,7]. Recent collisions and foundational data contamination incidents have starkly exposed the systemic vulnerabilities of autonomous driving systems to complex weather conditions and malicious hacking [8]. Confronted with escalating systemic intrusion risks, the industry largely views AI-driven cybersecurity defenses as the primary technical pathway to intercept attacks [9]. Yet, this addresses only the technical dimension of risk governance.

When technological evolution creates friction with established institutions, the structural lag of legal norms becomes glaringly apparent. Current road traffic regulations often fall into a regulatory vacuum when confronting highly automated driving systems, primarily due to the absence of directly applicable liability clauses [10]. The core bottleneck lies in the ambiguous legal status and definition of artificial intelligence itself, forming a critical barrier to the commercial deployment of this technology [11]. Faced with the opacity of algorithmic decision-making and potential legal disputes over electronic personhood, traditional actuarial models and the logic of tort attribution are severely challenged. A deep disciplinary chasm separates code design from legal culpability [12]. This fracture extends into post-accident response mechanisms, subjecting traditional vehicle accident investigation organizations to severe institutional dilemmas regarding data retrieval, liability demarcation, and cross-national jurisdiction [13].

The intersection of highly uncertain technological trajectories and complex social ethical demands has transformed CAEV regulation into a highly complex wicked problem [14]. To prevent early regulations from stifling technological innovation, global regulatory bodies generally lean toward non-binding guidelines or the establishment of ad hoc advisory committees. Consequently, the governance landscape exhibits significant fragmentation [15]. Taking early-adopter regions of autonomous driving as an example, the decentralization of licensing authority and testing standards to the local level not only exacerbates institutional inconsistencies but also strands public mobility data in a regulatory blind spot lacking privacy protections [16,17]. This asynchrony between technology and regulation is markedly ubiquitous. The misalignment of global regulatory pacing is evident across various contexts: Europe’s ethical dilemmas and policy barriers surfacing amid multi-stakeholder bargaining [18], the Middle East exposing cybersecurity regulatory gaps while advancing long-term technological visions [19], and China facing transitional pressure to forge a holistic governance system balancing early industry subsidies with prudent market oversight [20]. This siloed state is similarly reflected in the severe divergence of public road-testing guidelines across nations, directly severing the foundation of mutual trust required for the cross-national mutual recognition and sustainable deployment of autonomous technologies [21].

Public reaction to this institutional disconnect is direct and sensitive. Empirical surveys indicate that emerging technology markets actually harbor high social acceptance and expectations for the commercialization of autonomous driving. This bottom-up consumer preference forces governments and automakers to accelerate their strategic deployments [22]. Paradoxically, these high expectations driven by technological convenience

make the current regulatory vacuum all the more conspicuous. Concerns over ambiguous liability demarcations and absent safety mechanisms continue to erode this initially robust foundation of social trust [23]. A joint experiment targeting the United States, Japan, and Germany confirmed that despite divergent political beliefs and cultural backgrounds among respondents, a strong cross-cultural consensus exists in demanding strict legal liability for manufacturers and advocating for stringent product regulation [24]. Prospective scenario analyses issue a clear warning: if the regulatory system maintains its passive stance, the deep-seated contradictions among privacy violations, liability vacuums, and safety risks will rapidly erupt, forming a systemic social risk that impedes deployment [25]. System dynamics models further reveal that fragmented technical fixes divorced from a macro rule-of-law framework are highly prone to deviating from regulatory targets due to time-lag effects between defensive measures and market penetration, potentially triggering a more profound systemic collapse [26]. Bibliometric trends also confirm that foundational attack prevention technologies must achieve institutional coupling with top-level compliance regulatory frameworks [27]. Accordingly, this review strictly confines its research boundaries to the high-risk, complex scenarios of connected and automated vehicles. By stripping away pure engineering discussions of hardware and software, we systematically dissect the evolutionary trajectories of data security and algorithmic auditing to explore a dual-track synergistic regulatory framework capable of resolving the structural fracture between code and law.

2. Literature Screening Process and Descriptive Analysis

The technological characteristics of CAEVs substantively disrupt existing liability allocation and data compliance frameworks. To objectively map the evolutionary trajectory of public governance research in this domain and overcome the subjective sampling bias inherent in traditional narrative reviews, this study established a rigorous literature acquisition and review protocol based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) standard framework [28]. A structured literature screening mechanism effectively strips away non-relevant literature focused purely on underlying mechanical engineering or conventional encryption algorithm optimization. This ensures the final analytical sample aligns precisely with the core concerns of public policy and technology governance.

2.1. PRISMA-Based Literature Retrieval and Double-Blind Screening Procedure

Constructing a robust retrieval strategy is a prerequisite for accurately capturing literature at the intersection of policy and technology. To address the regional and linguistic limitations of single databases—and to comprehensively encompass the academic and policy discourse of China, the world's largest new energy vehicle market—this study integrated three major databases: the Web of Science (WoS) Core Collection, Scopus, and the China National Knowledge Infrastructure (CNKI) (restricted to CSSCI-indexed papers). The research team uniformly anchored the retrieval cutoff date to 24 June 2026, eliminating risks of temporal mismatch across databases. The retrieval strategy constructed a Boolean logic matrix (Table 1) comprising three semantic modules: “Physical Carriers and Connectivity Features,” “Data Security and Algorithmic Risks,” and “Policy Compliance and Governance Dimensions.” This matrix deliberately incorporated the latest technical and legislative terminology, such as OTA, V2X, software-defined vehicles, the AI Act [29], and UN R155 [30]. A logical intersection (AND) operation was implemented across the modules, with no hard cutoff applied to publication years.

Table 1. Core Retrieval Strategy and Boolean Logic Matrix.

Retrieval Module	Core Semantic Category	Boolean Logic and Keyword Strings (TS)
Module 1	Physical Carriers and Connectivity Features	“intelligent connected vehicle *” OR “autonomous vehicle *” OR “connected and automated vehicle *” OR “self-driving car *” OR “software-defined vehicle *” OR “V2X” OR “V2G” OR “OTA”
Module 2	Data Security and Algorithmic Risks	“data security” OR “privacy” OR “algorithm * regulation” OR “cybersecurity” OR “algorithmic accountability”
Module 3	Policy Compliance and Governance Dimensions	govern * OR policy OR policies OR regulat * OR compliance OR law OR “AI Act” OR “UN R155” OR “ISO/SAE 21434 [31]” OR “ISO 21434”

The asterisk represents a wildcard character used for truncation in the database search strategy to capture various word endings.

Confronting the literature redundancy typical of interdisciplinary fields, the research team implemented a cascaded double-blind screening procedure. Two independent reviewers, possessing cross-disciplinary backgrounds in public policy and vehicle engineering, conducted a parallel assessment of the 976 initial records remaining after deduplication. In the first round of preliminary screening, the double-blind observed agreement reached 89.23%, yielding a Cohen’s Kappa coefficient of 0.7687 [32]. This phase intercepted short reports lacking substantive research subjects (Category C3, 387 articles), generalized IoT studies deviating from traffic application scenarios (Category C2, 154 articles), pure engineering simulations (Category C4, 54 articles), and non-target language texts (Category C1, 25 articles).

The retained 356 articles successfully entered the second round of in-depth full-text review. At this stage, the double-blind agreement surged to 91.07% (Cohen’s Kappa = 0.8208). A third senior researcher reviewed and adjudicated the rare classification disputes. To guarantee academic rigor, the screening team initially purged 65 articles identified during the full-text phase as book chapters or non-peer-reviewed conference abstracts (EX-0). Subsequently, the team filtered out 123 psychological questionnaire studies that solely examined public acceptance without supporting compliance frameworks (EX-1). They also excluded energy and civil engineering literature focused on non-governance issues like grid load scheduling (EX-2, 15 articles), and cleared residual mechanical optimization analyses (EX-3, 10 articles) alongside marginal literature deviating from regulatory attributes (EX-4, 8 articles). Following this meticulous cleansing process, the team established a final sample of 135 highly relevant, high-quality articles (Figure 1).

Regarding the exclusion logic for interdisciplinary literature, this study clarifies the following: although pure mechanical control engineering literature (EX-3) was excluded, we deliberately retained computer science literature addressing Privacy-Enhancing Technologies (PETs), edge computing, federated learning, and Explainable Artificial Intelligence (XAI). Within the governance context of modern connected and automated vehicles, “Law-as-Code” has emerged as a critical trend. These underlying architectural designs fundamentally represent the engineering mapping of “Compliance-by-Design,” directly constituting the core empirical foundation for macro-policy implementation.

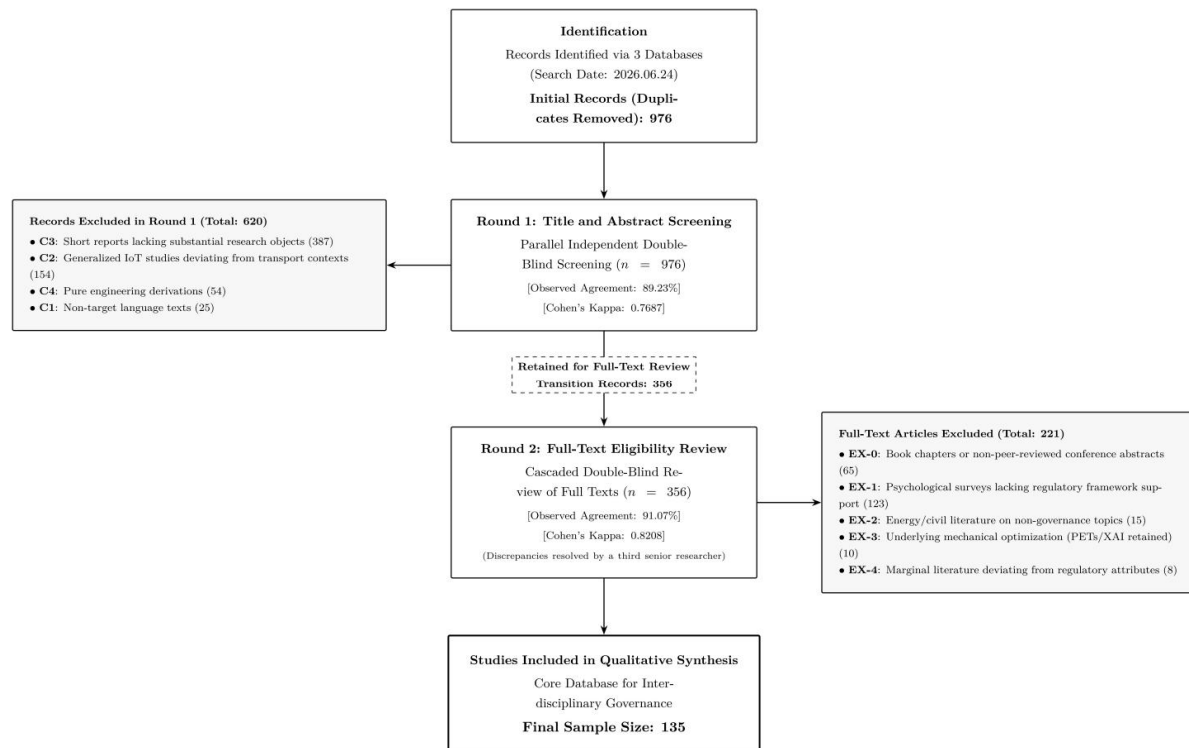


Figure 1. Flowchart of Literature Retrieval and Cascaded Screening Based on PRISMA Standards.

2.2. Multidimensional Descriptive Statistical Characteristics of Core Literature

The final inclusion of 135 articles provides an objective sample for observing the evolution of global vehicle data governance. External policy agendas frequently drive the trajectory of knowledge production. The temporal distribution of publications (Figure 2) reveals that related research largely stagnated in a slow exploratory phase between 2015 and 2020. A definitive turning point emerged in 2021. Annual publication volume surged into double digits (12 articles) and subsequently maintained a high trajectory, reaching 25 articles in both 2024 and 2025. This surge temporally and spatially aligns with the initiation of specialized vehicle data legislation across major global jurisdictions. More profoundly, it reflects the academic urgency of mandating human oversight, technical robustness, and privacy governance within autonomous driving ethical guidelines [33]. The sudden escalation of industry compliance pressure rapidly translated into academic productivity at the policy research level.

Regarding methodological preferences, knowledge construction exhibits a striking disequilibrium (Figure 3). Fully 84 articles adopted the normative theoretical and policy review paradigm, followed by engineering experiments and architectural design (30 articles). Empirical investigations—represented by qualitative research (10 articles), quantitative analysis (8 articles), and mixed methods (3 articles)—remain relatively scarce. This configuration stems from a chronic misalignment between theoretical focus and industry priorities. Academic discourse languished for years in abstract moral quagmires such as the “trolley problem.” Conversely, automakers operating at the technological frontier focus their actual demands sharply on collision avoidance and liability risk minimization design [34]. Constrained by barriers to acquiring real-world data from underlying vehicular networks, most policy effectiveness evaluations stall at conceptual deduction. This urgently necessitates the introduction of a comparative sociotechnical design perspective to locate empirical anchors for cross-national policy coordination across multiple dimensions, including safety and privacy [35].

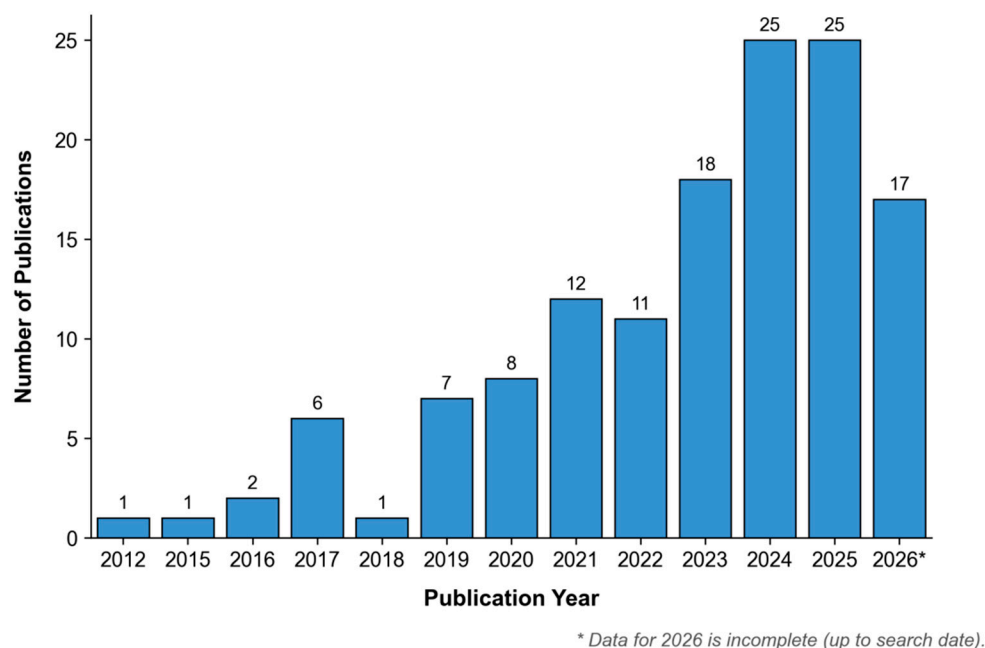


Figure 2. Annual Publication Volume Trend of Core Literature on CAEV Regulation, 2012–2026.

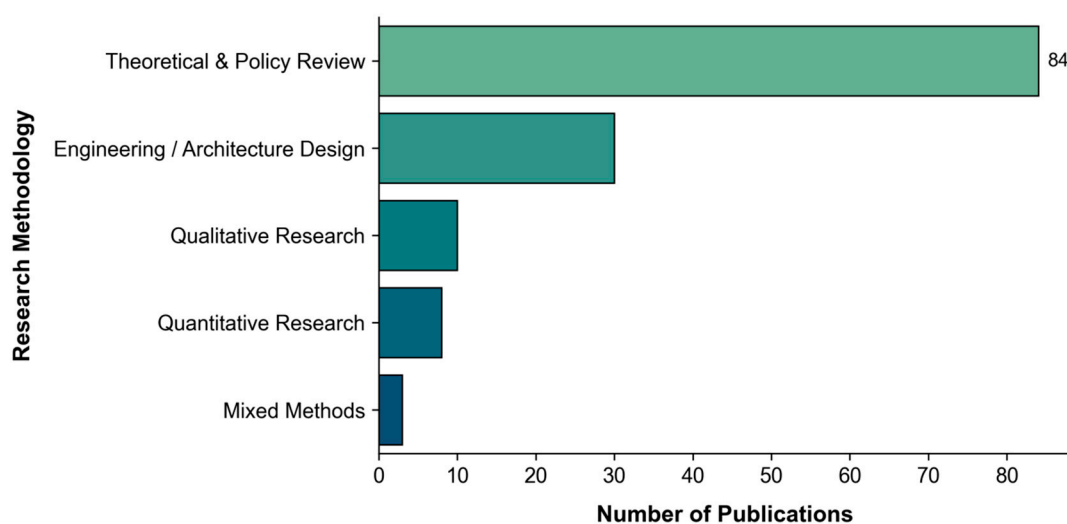


Figure 3. Categories and Distribution Proportions of Research Methods Adopted in The Core Literature.

Projecting the sample across the spatial dimension exposes a phenomenon of geopolitical agglomeration in research (Figure 4). After removing pure theoretical deductions (Theoretical, 46 articles) and global macro-level discourses (Global, 31 articles), the United States (20 articles), China (17 articles), and the European Union (13 articles) constitute the primary sources of academic output. Under the purview of the Holistic Approach to National Security, the operation of connected and automated vehicles generates complex risk spillovers that transcend the cyber-physical-social ternary space [36]. This effect inherently aligns with the distribution of commercial testbeds for high-level autonomous driving worldwide, driving high-frequency academic output from the US, China, and the EU amid their jurisprudential contestation.

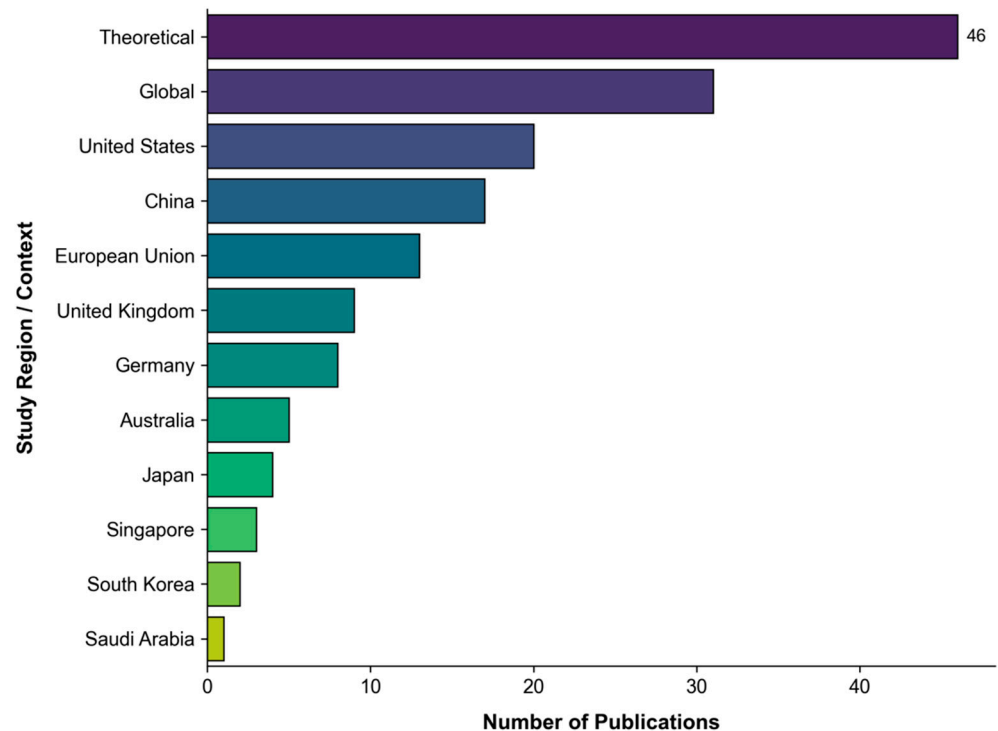


Figure 4. Spatial Distribution Characteristics of Jurisdictions in Empirical Cases Within The Core Literature.

To precisely anchor the governance focus of the core literature and respond to the complexities of policy-making, the review team established four mutually exclusive Thematic Coding Rules during the data extraction phase. Specifically, the “Data Privacy and Security Governance” category exclusively designates literature exploring vehicular data rights allocation, the failure of informed consent, and data leakage prevention mechanisms. The “Macro-Policy and Standard Comparison” category aggregates textual evolution comparisons of top-tier international legislation, such as the AI Act. The “Algorithmic Auditing and Technical Compliance” category is strictly limited to micro-level studies focusing on algorithmic transparency, the Safety of the Intended Functionality (SOTIF), and collision accountability. Meanwhile, the “Dual-Track Synergistic Regulation of Data and Algorithms” category encompasses only those studies that explicitly explore the mutual constraint mechanisms between data workflows and algorithmic decision-making, attempting to construct a lifecycle coordination framework. For cross-disciplinary studies spanning multiple thematic boundaries, the review team adopted a “primary contribution priority” principle during the coding phase. If a study addressed multiple issues, it was uniquely categorized based on its core methodological contribution or the primary regulatory bottleneck it sought to resolve. Notably, if a study substantively proposed and validated a comprehensive framework integrating data lifecycle management with algorithmic security, it was elevated and exclusively assigned to the “dual-track synergistic regulation” category.

Viewed through these coding criteria, the structural blind spots of the current academic knowledge landscape become apparent (Figure 5). Among the 135 samples, a staggering 82 articles fixate their research perspective solely on the “Data Privacy and Security Governance” quadrant. Because vehicle operational logic demands infrastructural surveillance of the environment, this ontological shift overturns traditional privacy boundaries [37]. Consequently, it forces scholars to integrate the contextual integrity framework to reconstruct data flow evaluation systems [38]. However, physical perception is fundamentally a deep coupling of data inputs and algorithmic outputs. Currently, explorations

into “Algorithmic Auditing and Technical Compliance” number a mere 8 articles. Literature attempting to coordinate both dimensions under “Dual-Track Synergistic Regulation” remains in a state of relative scarcity (7 articles).

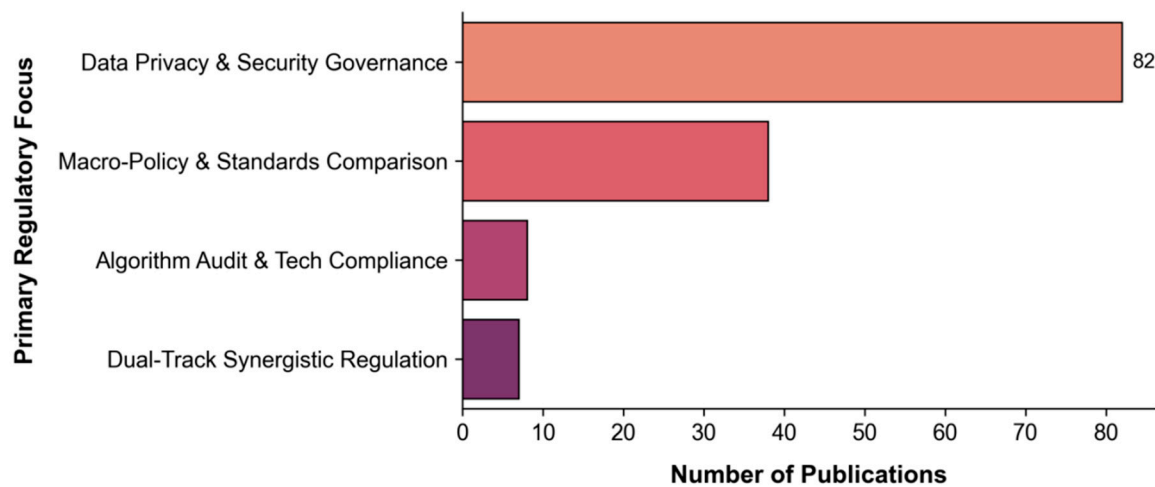


Figure 5. Horizontal Distribution Characteristics of Regulatory Targets in The Core Literature.

This unidimensional research trajectory, which artificially severs data from algorithms, severely undermines the regulatory system’s efficacy in addressing systemic risks. Evolutionary game analysis confirms that stakeholders’ micro-decisions in privacy and security governance are deeply constrained by the perceived value of compliance costs [39]. Facing continuously evolving cyberattacks, the automotive industry’s defense lines can no longer rely on single-point defenses divorced from the algorithmic context. Constructing bundled risk management frameworks and embracing cross-boundary threat intelligence sharing has become an inevitable choice [40]. Deeply integrating data regulation with algorithmic auditing and establishing an iterative evaluation system of “anticipate, include, reflect, and respond” from the perspective of Responsible Research and Innovation (RRI) [41] is not merely an objective necessity to shatter current theoretical bottlenecks. It constitutes the core logical departure point for this paper’s subsequent substantive construction of the dual-track synergistic mechanism.

3. Dimensions of Data Security and Privacy Governance in Connected and Automated Vehicles

3.1. Infrastructural Surveillance and the Deconstruction of Privacy Protection Paradigms

The global automotive market’s structural transition toward Battery Electric Vehicles (BEV) and Plug-in Hybrid Electric Vehicles (PHEV) does more than fundamentally reshape energy propulsion. It substantively propels the escalation of vehicular Level of Autonomy [42]. This deep intertwining of electrification and intelligence dictates that high-level autonomous vehicles must rely on widely distributed charging infrastructure [43]. Physical energy replenishment triggers high-frequency data interactions within the Vehicle-to-Grid (V2G) environment. The vehicle’s formerly closed physical shell dissolves. It evolves into a mobile sensing node that continuously streams trajectories, preferences, and identity characteristics to the smart grid and cloud, thereby subjecting vehicle location privacy within traditional grid architectures to structural exposure risks [44].

Throughout this process, the routine activation of in-vehicle biometric devices (such as facial recognition and eye tracking) [45] compounds with the mandatory, continuous state exchanges exacted by emergency systems like eCall [46]. Together, they cause the

protective boundaries of personal data to dissolve [47]. Modern V2X perception of occupants and the environment transcends the logic of traditional data “capture.” It sweeps indiscriminate external pedestrians—not just drivers—into a round-the-clock surveillance network. This state, defined by academia as “panoptic data surveillance,” substantively deprives individuals of their relative anonymity within mobile spaces [48]. Highly sensitive information, such as movement trajectories, morphs into commercially lucrative operational assets for platform enterprises. This commodification breeds the risk of unfair standard form data contracts that exploit the behavioral vulnerabilities of occupants [49].

Confronting continuous and imperceptible data flows, the long-established “notice-and-consent” principles across major global jurisdictions fall into a structural dilemma [50]. Risks of excessive automotive data collection, leakage, and the outflow of critical data continue to escalate, forming a pronounced “three-level, three-category” risk posture [51]. Empirical evaluations confirm a troubling reality. The static compliance standards of the EU’s GDPR [52], the existing notice-and-consent mechanisms in Germany and the wider EU [53], and Australia’s evolving privacy frameworks [54] all exhibit glaring regulatory blind spots when managing high-frequency interactive vehicular data streams.

Conceptual lag surrounding state intervention deepens this crisis. In the United States, for instance, the traditional Fourth Amendment “automobile exception”—which permits warrantless searches based on a vehicle’s physical mobility—becomes untenable in a data-driven context [55]. Urban administrators implement real-time location monitoring through the Mobility Data Specification (MDS). This practice breaches highly sensitive privacy thresholds, constituting de facto administrative searches [56]. The enactment of the UK’s Investigatory Powers Act [57] issues a similar warning. Its mandatory data retention mechanisms objectively force Original Equipment Manufacturers (OEMs) to act as covert extension nodes for state mass surveillance [58].

3.2. Cross-National Regulatory Fragmentation and the Contestation over Public-Private Data Ownership

The multidimensional threats of data abuse compel nations to tighten regulations on cross-border data flows. Consequently, global data governance exhibits profound fragmentation. Text clustering analysis based on BERTopic reveals that the GDPR, CCPA [59], and South Korea’s PIPA [60] harbor significant structural fissures regarding mobility data jurisdiction and liability exemption clauses [61]. In China, the world’s largest market for connected and automated vehicles, regulatory logic attempts to strike a dynamic balance between the baseline of national security and the interconnected development of the industry [62–64]. However, an empirical examination of privacy policies from the top ten domestic connected vehicle manufacturers reveals a stark reality. Enterprises hold a distinct advantage in the contestation over data ownership, frequently subjecting consumers’ statutory data rights to covert curtailment [65]. This confirms that the data security of autonomous driving confronts compounding challenges from technical vulnerabilities, legal lag, and social ethics [66].

The rapid emergence of novel business models continuously strains the carrying capacity of existing rules. Usage-Based Insurance (UBI) reshapes the traditional dual relationship between policyholders and insurers. The actuarial thirst for granular driving data fundamentally conflicts with current high privacy standards [67]. Resolving this requires the urgent introduction of a tiered regulatory framework of “standardization-validation-remedy” to reconstruct the boundaries of the obligation to inform [68]. In ride-hailing and Robotaxi services, the public’s deep-seated concerns regarding data abuse have become a critical social barrier hindering large-scale deployment [69]. Surveys targeting emerging markets like Serbia confirm that a privacy trust deficit is the primary negative factor delaying the popularization of high-level autonomous driving [70].

Dismantling this trust crisis urgently requires reconstructing the governance paradigm. Regulators must abandon isolated rights protection centered on “absolute personal control” and pivot toward “altruism” and synergistic control by multiple stakeholders [71]. Effective arrangements to resolve ownership disputes are emerging. These include establishing a two-tier public-private cooperative protection architecture where “administrative agencies regulate automakers, and automakers protect user privacy” [72], or building a government-led Open Data Platform (CAV-ODP) to integrate public and private interests [73]. Furthermore, introducing a regulatory sandbox mechanism from a Legal Design perspective provides a crucial institutional buffer to conduct policy pilots in a controlled environment and achieve classified and graded data regulation [74,75].

3.3. Law-as-Code: The Underlying Technical Mapping of Data Compliance

Abstract policy reviews divorced from underlying code architectures fundamentally fail to address the systemic risks confronting connected and automated vehicles. Data governance within the automotive industry is undergoing a paradigm shift from ex-post legal accountability toward Privacy-by-Design [76]. This “Law-as-Code” trend dictates that macro-compliance frameworks must map precisely onto both vehicular hardware nodes and cloud computing infrastructure.

The technical prerequisite for implementing classified and graded regulation lies in precisely quantifying data misuse risks. The Misuse Risk scoring model (MR-score), constructed via metrics of sensitivity, scale, and identifiability, provides regulatory agencies with a quantitative analytical fulcrum to intercept high-risk datasets [77]. Regarding cybersecurity risk assessment, traditional Threat Analysis and Risk Assessment (TARA) methods are undergoing readaptation. Their coverage radius extends beyond merely preventing hacker attacks to encompassing full-lifecycle compliance reviews of data [78]. Synergizing Privacy Impact Assessments (PIA) with misuse case modeling enables manufacturers to substantively block unauthorized user profiling pathways early in the product design phase [79].

Confronting the high mobility and short-duration connectivity of vehicles, relying solely on centralized cloud encryption proves increasingly inadequate. Edge computing architectures permit instantaneous data desensitization at the on-board terminal near the perception source. This generates “non-personal data” devoid of specific identity pointers, technically circumventing stringent privacy reviews at the source [80]. The synergistic deployment of Federated Learning (FL) and Differential Privacy (DP) mandates that vehicles exchange only model parameters rather than raw driving data. This fundamentally eliminates the leakage risk associated with Single Point of Failure (SPOF) attacks on central servers [81]. Within dynamic V2X environments, fusing federated learning with permissioned blockchains further resolves the chronic scalability deficits of traditional privacy protection mechanisms [82].

To establish the immutability and credibility of data workflows, permissioned blockchains and Zero-Knowledge Proofs (ZKP) are widely embedded within V2X architectures [83]. Although decentralized cryptographic mechanisms substantially enhance data audit transparency, their indelible nature objectively generates inherent tension with the “right to be forgotten” codified in data protection regulations [84]. To bridge this techno-policy fracture, constructing Trusted Data Spaces (TDS) that integrate edge-cloud federated architectures emerges as the technical foundation for the full-lifecycle governance of multi-source heterogeneous data [85]. As system dynamics modeling reveals, an effective cybersecurity regulatory framework must strike a rational dynamic balance among data accessibility, control thresholds, commercial investment, and privacy redlines [86]. To visually demonstrate how compliance mandates materialize into concrete technical practices, Table 2 systematically maps the pathways of key data policies into underlying architectures.

Table 2. Data Security Compliance Demands and Underlying Technical Mapping Mechanisms in CAEVs.

Core Regulatory/Policy Demand Dimensions	Mapped Underlying Privacy-Enhancing Technologies (PETs) & Security Architectures	Engineering Implementation Mechanisms & Compliance Verification Logic	Core Supporting Literature
Classified and Graded Data Regulation & Minimization of Collection	Edge Computing & Misuse Risk scoring (MR-score)	Instantaneously desensitizes data at the source to generate non-personal data; utilizes MR-score to quantify dataset sensitivity and match access privileges.	[77,80]
Prevention of Raw Data Leakage & Blockage of Cross-Border Workflows	Federated Learning (FL) & Differential Privacy (DP)	Local on-board trained models exchange only gradient parameters; injects differential noise to prevent reverse engineering by attackers, breaking down data silos.	[81,82]
Source Blockage of Full-Lifecycle Privacy Threats	Joint Modeling of TARA & Privacy Impact Assessment (PIA)	Translates excessive collection risks into quantified threat nodes, operationalizing Privacy-by-Design to achieve early vulnerability interception.	[76,78,79]
Data Immutability & Audit Transparency Enhancement	Permissioned Blockchains & Zero-Knowledge Proofs (ZKP)	Distributed ledgers record data invocation hash values to ensure traceability; ZKP verifies identity validity without disclosing data content.	[83,84]
Data Sandbox Testing for High-Risk Cross-Domain Scenarios	Trusted Data Spaces (TDS) & Regulatory Sandboxes	Constructs a controlled testing environment integrating edge-cloud federated architectures, providing a technical prototype for legitimate data workflows between governments and automakers.	[74,75,85]

4. Restructuring Liability and Quantitative Auditing in Algorithmic Regulation

4.1. The Fracture of Attribution Logic Triggered by Algorithmic Decision-Making

The substantive transfer of control in connected and automated vehicles triggers a systemic restructuring of the traffic accident liability allocation framework. The technological replication of human driving behavior by autonomous systems decouples the core regulatory arena from physical operations into deep code spaces, exposing the dilemma of inconsistent liability attribution standards globally [87]. This displacement triggers an applicability crisis for negligence tort law. AI decision-support tools interpose complex code driven by statistical probabilities between human operators and harmful outcomes. This configuration subjects traditional attribution pathways grounded in the duty of reasonable care to severe applicability constraints [88]. The realm of criminal liability confronts parallel challenges. Traditional criminal law's identification of mens rea and actus reus struggles to untangle algorithmic decision logic, while the evidentiary cost of tracing whether manufacturers or users breached their duty of care remains prohibitively high [89]. Bridging this chasm urgently requires introducing a hybrid attribution framework at the legislative level that balances strict liability and vicarious liability [90].

Confronting the latent moral dilemmas of algorithmic decision-making, scholars previously attempted to construct circular ethical frameworks for anticipatory regulation [91]. However, pure ethical speculation divorced from engineering practice fails to address the real-world product liability and systemic risks induced by autonomous driving [92]. The lag in judicial practice forces private voluntary standards to substantively fill the

vacuum of safety governance. In tort litigation, whether manufacturers comply with these private standards has become the core benchmark for evaluating their duty of care [93].

Establishing mandatory mechanisms for risk interception and transfer is a critical countermeasure. Vehicular big data provides a real-time basis for granular Usage-Based Insurance (UBI) pricing [94]. Yet, when responding to collective systemic failures triggered by large-scale cyberattacks, traditional commercial insurance models expose shortfalls in carrying capacity. This demands that regulators explore establishing national compensation agencies or reinsurance pools to safeguard victim rights [95]. A more operable institutional vision advocates constructing mandatory liability insurance centered dually on product liability and cybersecurity, concurrently mandating vehicles to equip event data recorders (EDRs) or “black box” technologies. Solidifying the temporal states of algorithmic decisions effectively enhances the traceability of the accident process, thereby resolving the evidentiary deadlock for victims [96].

4.2. Explainable AI and the Engineering Implementation of Ex-Ante Auditing

Overcoming the technical opacity of algorithms cannot rely solely on ex-post liability retrospection. The deep penetration of AI components in vehicles disrupts traditional physical testing protocols. Consequently, establishing an ex-ante auditing methodology encompassing transparency, robustness, and fairness has become a consensus [97]. As end-to-end autonomous driving architectures highly couple perception with control, decision-making opacity intensifies significantly. Mandating the embedding of Explainable Artificial Intelligence (XAI) mechanisms is a prerequisite for demarcating the liability boundaries between manufacturers and users, constituting the technical support for achieving multi-level regulatory alignment [98].

Constructing trustworthy decision models requires XAI to provide ex-post explanations that transcend mere code presentation. This enables regulators without technical backgrounds to accurately evaluate the causal weights of behaviors such as lane changing and braking [99]. Nevertheless, software-dimensional explainability remains at risk of malicious tampering without constraints from the underlying hardware architecture. The EGIS dual-brain controller architecture provides a definitive engineering reference. By establishing an independent, hardware-isolated safety monitoring layer outside the main system, and by implementing human override control and file state rollbacks, this architecture satisfies the mandatory compliance standards of the EU AI Act regarding human oversight and recoverability for high-risk systems [100].

In-depth algorithmic auditing demands a systemic upgrade of existing Threat Analysis and Risk Assessment (TARA) processes. Analytical methods oriented toward traditional vehicles struggle to adapt to high-level autonomous driving scenarios devoid of human driver intervention. By integrating Privacy Impact Assessments with expert subjectivity calibration, the TARA 2.0 framework provides an enhanced risk management pathway for operationalizing the ISO/SAE 21434 standard [101]. Bridging the isolated functional-oriented and component-oriented threat analysis pathways within automotive systems directly translates cybersecurity requirements into specific use-case defense designs. This effectively eliminates latent vulnerabilities and redundancies within the system-level architecture of software-defined vehicles [102].

4.3. Quantifying Algorithmic Bias and Standardizing Safety Risk Management

Algorithmic compliance auditing must ultimately transition from qualitative descriptions to quantitative evaluations based on traffic safety impacts. Statistical biases and distorted safety incentive mechanisms latent within algorithmic decision-making imperceptibly breed road-level inequities and physical collision hazards [103]. Quantifying and

rectifying such biases presupposes dismantling the blurred boundaries between algorithmic inputs and outputs. Based on top-tier legal sources such as the Data Security Law [104], structurally categorizing the data sustaining algorithmic operations into training data, operational data, and derived data—while implementing principles of recording and transparency across the entire algorithmic pipeline—constitutes the core prerequisite for severing bias contagion and quantifying evaluation deviations [105]. The deep convergence of technical safety, cybersecurity, and ethical risks breaks the singular perspective of traditional functional safety, establishing a three-dimensional constraint space for unified algorithmic safety standards [106].

The core challenge confronting current algorithmic auditing has evolved from internal logical deviations to external Adversarial Machine Learning (AML) attacks. Attack vectors such as evasion and data poisoning directly disrupt traffic perception networks, inducing catastrophic consequences. Traditional safety evaluations lack fine-grained control over covert threats. Introducing a tailored extension profile to the NIST Cybersecurity Framework (NIST CSF)—thereby directly anchoring core functions like Identify, Protect, and Respond to the mitigation of adversarial threats—fills the evaluation void at the operational level of transportation network systems [107]. Deeply synergizing adversarial attack defenses with emerging standards like the NIST AI Risk Management Framework and MITRE ATLAS signifies that algorithmic safety has transitioned from a pure laboratory robustness proposition into a standardized governance engineering effort spanning the full lifecycle [108]. Table 3 delineates the primary current demands for algorithmic safety compliance and their corresponding engineering quantification and auditing mechanisms.

Table 3. Mapping of Algorithmic Regulatory Demands to Ex-Ante Auditing and Quantitative Mechanisms.

Core Regulatory and Compliance Demand Dimensions	Corresponding Algorithmic Auditing and Quantitative Technical Tools	Audit Execution Mechanisms and Regulatory Verification Logic	Core Supporting Literature
Deciphering Algorithmic Black Boxes and Retroactive Liability Tracing	Explainable AI (XAI) and “Black Box” Technologies (EDRs)	Mandates the output of causal weights for decision features; solidifies and retains operational and derived data in real-time for forensic identification.	[96,98,99,105]
Human Oversight and System Recoverability	Physically Isolated Dual-Brain Controller Architectures (e.g., EGIS)	An independent monitoring layer continuously verifies primary algorithmic behavior, mandating human override control and state rollbacks upon deviation from safety thresholds.	[100]
Full-Lifecycle Vulnerability and Robustness Auditing	TARA 2.0 and Functional-Component Integration Models	Strips the human driver assumption, integrates use-case and component boundaries, and mandates adversarial vulnerability enumeration during early design phases.	[97,101,102]
Adversarial Attack Defense and Bias Quantification	Tailored NIST CSF Profiles Aligned with AML Standards	Indexes data poisoning and evasion attacks; implements quantitative bias isolation on training data to align with standards such as MITRE ATLAS.	[103,106–108]

5. Dual-Track Synergistic Governance Mechanism for Data and Algorithms in CAEVs

5.1. From Isolated Functional Safety to Dual-Track Synergistic Design

The exponential leap in the systemic complexity of connected and automated vehicles precipitates an applicability crisis for traditional static-rule-based certification methods [109]. This compels regulatory paradigms to undergo a systemic evolution toward

goal-oriented and risk-defense-based assurance case frameworks. Historically, automotive safety engineering relied heavily on the ISO 26262 [110] standard, its purview firmly confined to physical hazards induced by the inherent faults of electrical and electronic (E/E) systems. Confronting highly open vehicular communication environments, this singular “functional safety” perspective struggles to counter complex cyberattacks triggered by malicious data injection. This necessitates the comprehensive introduction of cybersecurity engineering lifecycle methods, epitomized by ISO/SAE 21434 [111]. The industry has initiated attempts to shatter the segregation of these two standards. By constructing a unified Cybersecurity and Safety Management System (CSSMS) that integrates functional safety with cybersecurity, stakeholders simultaneously reduce redundant compliance costs and dissolve latent redundancies within development workflows [112].

The core essence of dual-track synergistic governance lies in establishing a unidirectional veto relationship of “data quality” over “algorithmic physical safety.” Divorced from real-world physical scenarios, “data contamination” is by no means confined to static privacy breaches. Its more fatal threat lies in directly triggering the catastrophic failure of the algorithm’s Safety of the Intended Functionality (SOTIF). Threat modeling targeting autonomous driving cyber-physical systems (CPS) confirms that minuscule adversarial perturbations at the environmental data layer can breach the robustness boundaries of machine learning algorithms, compelling controllers to output lethal steering or braking commands [113]. However, a mature synergistic framework transcends this unidirectional constraint by establishing a bidirectional feedback loop. When ex-ante or run-time algorithmic safety risks are detected—such as a sudden drop in adversarial robustness or anomalous decision weights exposed by Explainable AI (XAI)—these algorithmic anomalies must serve as active triggers to initiate renewed data validation and governance protocols. For instance, if an autonomous controller’s inference output deviates from the established safety baseline, the system should automatically retroactively audit the source data, purging potential poisoning nodes or recalibrating the dataset’s sampling distribution. This reverse-trigger mechanism ensures dynamic error-correction and the mutual evolution of both data and algorithms.

Taking systemic cascading impacts within Vehicle-to-Everything (V2X) ecosystems as an example, quantitative simulation evaluations expose pronounced systemic vulnerabilities. In a typical cyber-physical attack scenario, compromised Roadside Units (RSUs) continuously broadcast fabricated Variable Speed Limits (VSL) or phantom lane closures into the road network. Once decision-making algorithms in connected vehicles unconditionally adopt these contaminated command data, they directly trigger large-scale chain-reaction rear-end collisions and systemic traffic paralysis across the highway network [114]. The feasibility of attacks in such dynamic scenarios depends heavily on the real-time state of external data sources. Traditional static qualitative assessments fail to capture the full spectrum of these threats. Therefore, data-driven quantitative simulation models must be introduced to precisely measure the attacker’s “Window of Opportunity” [115]. Constructing a trustworthy AI ecosystem requires uniformly embedding data protection, explainability, and adversarial robustness into full-lifecycle Trust, Risk and Security Management (TRiSM) workflows. This ultimately completes a holistic governance chain at the foundational level, seamlessly linking data input sanitization with algorithmic output accountability [116].

5.2. Engineering Mapping of Law-as-Code and Standard Validation

Before implementing “Law-as-Code,” it is imperative to clearly delineate the legal efficacy and implementation hierarchy of the various regulatory instruments discussed, as this constitutes the jurisprudential foundation for compliance mapping. The current governance ecosystem for connected and automated vehicles is primarily structured

across three hierarchical levels. First, macro-level statutory laws (such as the EU GDPR and the AI Act) possess the highest legal binding force, establishing inviolable baseline principles and severe punitive measures for non-compliance. Second, type-approval regulations (such as UNECE R155/R156) function as mandatory prerequisites for market access; they wield transnational administrative enforcement power, directly determining whether a vehicle is legally permitted on public roads. Third, voluntary technical standards (such as ISO/SAE 21434) serve as operational engineering guidelines. While lacking direct statutory mandate, these standards are frequently weaponized in judicial tort litigation as a critical compliance shield to assess whether a manufacturer has fulfilled its “duty of reasonable care.”

Bridging the implementation gap between macro-regulatory intentions and micro-code execution relies heavily on the systematic anchoring of full-ecosystem certification routes by the Standards Coverage Map (SCM) [117]. Within this mapping process, Over-the-Air (OTA) technology acts as the core pipeline connecting external data clouds with in-vehicle execution algorithms, constituting a critical node in the offensive-defensive contest. Constructing a secure OTA update ecosystem requires manufacturers globally to translate mandatory UN R155 and UN R156 [118] regulations into operational paradigms spanning the entire vehicle lifecycle [119]. Industry practice has begun systematically embedding open security frameworks like Uptane into OTA update cycles. This approach adopts a “Security-by-Design” philosophy to defend against downgrade and malicious firmware flashing attacks [120]. Taking the OTA upgrade of the Lane Keeping Assist (LKA) function as an example, rigorous Threat Analysis and Risk Assessment (TARA) enables engineering teams to precisely identify dozens of attack vectors and deploy targeted cryptographic defenses. This execution provides a highly valuable empirical sample for the compliant implementation of advanced driver assistance systems [121]. The Chinese market has similarly established a data encryption and Root of Trust (RoT) protection technology system covering the “cloud-pipe-device” end-to-end architecture by deeply integrating UNECE protocols with mandatory national standards [122].

Achieving cross-dimensional dual-track synergy requires shattering the long-standing organizational silos separating privacy protection from security analysis. By integrating the LINDDUN privacy model with traditional security attributes, the Privacy-enhanced Threat Analysis and Risk Assessment (PeTARA) method synchronously intercepts privacy leakage and system hijacking risks during the initial design phases of vehicular electrical and electronic architectures [123]. Addressing the operational vacuum in the implementation process of ISO/SAE 21434, academia is accelerating the engineering transformation of methodologies. The HEAVENS 2.0 model compensates for the flaws of preceding architectures, achieving precise responsiveness to United Nations vehicle cybersecurity regulations [124]. Concurrently, the MARISMA-CAR model creatively incorporates the threat tiering mechanism of the European Union Agency for Cybersecurity (ENISA), providing actionable operational guidelines that extend directly into the component design phase [125]. Furthermore, the Model-based Overall Defense Assurance framework (ODFa2) optimizes the tradeoff algorithms for defense strategies, substantially enhancing the timeliness of engineering validation [126].

The diversity of engineering implementations dictates that compliance auditing must possess robust cross-tier evaluation capabilities. Standardized analytical models demonstrate formidable universality. They effectively compare the security protection levels of centralized High-Performance Computing (HPC) against distributed node architectures [127], assess OSI model-layer threats and regulatory mapping for in-vehicle Ethernet [128], and systematically define attack surfaces for emerging Remote Monitoring and Telemetry (RMTO) scenarios [129]. To dissolve the semantic barriers between abstract regulatory provisions and concrete development tasks, mapping regulatory requirements

directly onto mature software weakness enumeration dictionaries—such as STRIDE and CAPEC—provides upstream and downstream supply chains with unambiguous vulnerability defense checklists [130,131]. Simultaneously, integrating toolchains based on the Business Process Model and Notation (BPMN) and the EAST-ADL language drastically lowers the cognitive threshold for non-technical managers attempting to comprehend complex attack trees [132,133]. During the mass-production validation phase, coupling the prioritization review system of the Analytic Hierarchy Process (AHP) with in-depth penetration testing furnishes regulatory agencies with quantitative bases and practical empirical tools to rapidly assess the compliance maturity of massive automaker supply chains [134–137]. Table 4 visually encapsulates this complex transmission mechanism.

Table 4. Engineering Mapping Mechanisms of Dual-Track Synergistic Governance for CAEVs.

Regulatory Demands and Legal Source Domains	Accommodating Engineering Standards and Evaluation Frameworks	Technical Mapping Mechanisms and Implementation Efficacy	Core Supporting Literature
Overall Ecological Security Certification Coordination	Standards Coverage Map (SCM)	Categorizes heterogeneous network and data privacy standards to construct an integrated compliance pathway.	[117]
Software Update Lifecycle Management (e.g., UN R156, GB standards [138])	OTA Security Architecture Design and Uptane Framework	Establishes end-to-end “cloud-pipe-device” encryption to defend against downgrade attacks and malicious firmware flashing.	[119–122]
Intended Functionality and Data Contamination Interception (Addressing SOTIF risks)	Simulation-level TARA and WOLVES Framework	Quantifies the systemic cascading physical impacts of externally contaminated data (e.g., RSU spoofing) on decision-making algorithms.	[114,115,139]
Synergistic Privacy and Security Development	PeTARA and HEAVENS 2.0 Integration Methods	Synchronously introduces the LINDDUN model during the initial architecture design phase to eliminate compliance review blind spots.	[123,124]
Supply Chain Compliance Context Alignment (Implementing UN R155)	STRIDE/CAPEC Threat Dictionary Mapping and BPMN Visualization	Translates abstract regulations into specific software weakness codes, lowering the review cognitive threshold for non-technical managers.	[130–132]

5.3. Cross-National Policy Coordination and Adaptive Regulatory Pathways

The high homogeneity of underlying engineering languages cannot mask the profound divergence of macro-regulatory systems. Constrained by indigenous legal traditions and industrial interests, nations exhibit starkly different institutional resilience and evolutionary trajectories when advancing dual-track synergistic mechanisms. The early federal policy framework of the United States appeared particularly dispersed when addressing autonomous driving. Authority over privacy, cybersecurity, and driving regulation was severed and dispersed across distinct functional departments. This jurisdictional fragmentation severely restricted the systemic efficacy of the U.S. in coordinating responses to compound risks [140]. Even within the framework of the UN 158 Agreement [141], which attempts to establish unified global standards, member states retained substantial disparities regarding the stringency and execution details of verification testing procedures during the operational translation of UN R155 into domestic legislation. These variances are driven largely by territorial administrative conventions [142].

Confronting the ethical dilemmas and governance disconnections brought by disruptive technologies, select jurisdictions have pioneered highly forward-looking adaptive regulatory pathways. Singapore’s governance logic intertwines the “prescriptive” and the

“experimental.” By establishing highly controlled regulatory sandboxes, the city-state not only accomplished closed-loop testing of data collection and algorithmic decision-making within physically isolated environments. More importantly, it effectively absorbed public-level ethical concerns into ad hoc regulatory frameworks through broad multi-stakeholder participation [143,144]. Conversely, China demonstrates pronounced characteristics of incremental evolution. While comprehensive national-level legislation ferments, China leverages high-density policy pilot zones, such as Beijing, to conduct cross-regional synergistic legislative pilots, thereby accumulating institutional reserves through local regulatory competition [139,145]. Concurrently, it positions ex-ante mandatory cybersecurity technical standards as core safeguards. This rigid baseline effectively reconciles the structural tension between rapid technological evolution and legal stability [146]. The European Union, relying on its massive regional synergistic advantage, funds 5G Cooperative, Connected and Automated Mobility (CCAM) pilot projects. This bottoms-up approach drives the standardization process for complex scenarios, such as backward-facing perception safety [147].

Ultimately, bridging global regulatory fissures relies on constructing a highly inclusive Comprehensive Cybersecurity Regulatory Framework (CRF). This framework necessitates breaking through traditional unilateral administrative directives. Instead, it must integrate four major policy tools: “regulation,” “supply,” “economic incentives,” and “moral suasion.” Such integration systemically diffuses technological reliability defects, privacy-ceding anxieties, and the latent inequities that algorithmic decision-making might inflict upon Vulnerable Road Users (VRUs) [148]. Dynamic modeling analysis issues a further warning: a future CRF must achieve a dynamic equilibrium across four dimensions—data accessibility constraints, regulatory control thresholds, the protection of automakers’ commercial investments, and the boundaries of public data privacy [149]. Only upon the bedrock of mutual recognition of technical standards and cross-border trust in data can the globalized deployment of connected and automated vehicles truly fulfill its social promise to enhance the overall resilience and efficiency of transportation systems.

6. Discussion and Conclusions

6.1. Paradigm Evolution of Dual-Track Synergistic Regulation and Cross-Disciplinary Literature Dialogue

As quintessential Cyber-Physical-Social Systems (CPSS), CAEVs undergo a regulatory architectural evolution that fundamentally epitomizes the continuous contestation between technological advancement and institutional resilience. The “dual-track synergistic regulation of data and algorithms” governance mechanism proposed in this review aims to systemically overcome the theoretical limitations of “unidimensional governance” that have long plagued both academia and industry. Engaging in a deep horizontal and vertical dialogue between our theoretical deductions and existing mainstream research clearly delineates the incremental theoretical contribution of this synergistic mechanism.

A substantial body of existing academic literature tends to treat cybersecurity and data privacy as mutually parallel compliance tracks. This artificial academic compartmentalization breeds structural vulnerabilities within the defense architecture. For instance, within the engineering-oriented research camp, scholars strive to deeply integrate ISO/SAE 21434 with Threat Analysis and Risk Assessment (TARA) models, emphasizing the interception of external hackers’ physical intrusions directly from the component design phase [101]. Conversely, within the purview of law and public policy, mainstream discourse frequently confines itself to analyzing the applicability crisis of the EU’s GDPR or the *Data Security Law* when confronting “panoptic data surveillance.” These studies attempt to patch privacy loopholes by refining “notice-and-consent” rules [37]. This paradigm of parallel academic evolution entirely neglects the strong coupling relationship

between “data flows” and “decision-making logic” interior to modern software-defined vehicles. Distinct from studies that in isolation explore Explainable Artificial Intelligence (XAI) or the robustness of adversarial machine learning [97,108], our synthesis corroborates that “data quality” holds a unidirectional veto over the algorithmic “Safety of the Intended Functionality (SOTIF).” Divorced from instantaneous sanitization and cryptographic authentication at the underlying environmental data source, any upper-layer advanced algorithmic defense lines will forfeit their defensive efficacy against adversarial attacks such as data poisoning.

Scholars introducing a comparative sociotechnical design perspective have acutely observed that governance challenges within complex technological systems possess a mutually constitutive mechanism [35]. The dual-track synergistic framework constructed in this paper acts as a profound response to this theoretical frontier. It dictates transcending singular privacy protection compliance or isolated functional safety certification, mandating the compulsory binding of the secure, full-lifecycle flow of data with the causal weight output of algorithmic decision-making. Macroscopically, this mechanism resonates with evolutionary game theory’s demands regarding multi-stakeholder perceived value and synergistic control [39]. Microscopically, at the engineering level, it furnishes the “Law-as-Code” support mechanism requisite for implementing emerging top-tier regulations like the EU AI Act.

6.2. Research Limitations and Future Prospects

The knowledge graph of any systematic literature review remains constrained by its methodological boundaries. Relying upon the PRISMA standard framework, this study strictly confined its sample pool to peer-reviewed English and Chinese top-tier academic databases. While safeguarding academic rigor and theoretical policy depth, this retrieval strategy objectively excluded a vast array of industry white papers yet to be translated into academic articles, internal security architecture specifications from Original Equipment Manufacturers (OEMs), and grey literature. Crucially, constrained by the automotive industry’s formidable walls of commercial secrecy protection and strict barriers to data sharing, real-world attack samples and internal defensive negative data from underlying Vehicular Ad-hoc Networks (VANETs) remain exceedingly difficult to procure. Consequently, the assessment of the dual-track synergistic mechanism’s actual efficacy—in this study and the vast majority of current academic discourse—remains partially anchored in normative deduction and simulation modeling phases. It lacks the empirical data support derived from mass-produced vehicle models confronting Advanced Persistent Threats (APT) on real-world open roads. Furthermore, the high concentration of empirical cases within the three major jurisdictions of China, the United States, and the European Union potentially obscures the unique geopolitical regulatory frictions and technical standard barriers confronting the Global South as it integrates into the intelligent transportation ecosystem.

Addressing current methodological and empirical data constraints, future academic inquiry into the public governance of connected vehicles must breach traditional policy text analysis. It necessitates a strategic pivot toward the following two uncharted evolutionary frontiers.

First, the “value alignment” challenges provoked by the integration of Large Language Models (LLMs) into vehicles. As multimodal large models rapidly penetrate end-to-end autonomous driving architectures, vehicles transcend being mere terminals executing mechanical commands; they evolve into intelligent agents possessing complex common-sense reasoning capabilities. Recent cutting-edge explorations issue a stark warning: when processing sensitive vehicular data encompassing precise locations and real-time traffic conditions, the built-in safety guardrails of LLMs are highly susceptible

to circumvention via complex prompt injection, triggering profound, large-scale data leaks [150]. More intractably, traditional functional safety standards remain entirely incapable of constraining the “hallucinations” of LLMs. A systemic quantitative evaluation mechanism is still lacking to ascertain whether the inferential outputs of these large models strictly adhere to territorial traffic regulations and human moral values. Constructing a high-level safety alignment framework exclusive to autonomous driving multi-agent systems—ensuring that model outputs yield absolute obedience to physical safety baselines and ethical norms—will constitute the next uncharted technological frontier in algorithmic auditing.

Second, participatory governance and regulatory pilot research aimed at reconciling diverse values. The deployment of disruptive transportation technologies is never merely about pure code verification; it represents the reallocation of urban spaces, public resources, and social trust. Cross-national empirical surveys profoundly reveal that in constructing the vision of autonomous mobility, the relationship among the public, regulators, and automakers defies a simplistic binary of “support” or “opposition.” Instead, it is interwoven with optimism, ambivalence, and deep-seated mistrust [151]. Stakeholder interests clash in pronounced structural conflicts, particularly regarding data management privileges, accident liability apportionment, and the delineation of cybersecurity boundaries. To defuse this tension, traditional top-down bureaucratic regulation has proven rigid. Future research must dedicate itself to substantively embedding public-level ethical concerns into the policy-making workflow. Relying upon government-led cross-domain Trusted Data Spaces [75] and regulatory sandbox mechanisms, researchers should launch large-scale policy pilots. Furthermore, within the iterative framework of Responsible Research and Innovation (RRI) [41], system dynamics models should be leveraged to continuously simulate the long-term cascading impacts of regulatory policies on industrial investment and public privacy [149]. Only by establishing such a highly inclusive participatory governance ecosystem can we substantively heal the profound fractures among stakeholders regarding data rights allocation and algorithmic accountability.

6.3. Conclusions

Amid the wave of software-defined vehicles reshaping the modern transportation landscape, CAEVs transmit the virtual risks of cyberspace into the critical infrastructure systems of the physical society with unprecedented depth. Through the systematic synthesis and multidimensional deconstruction of global core literature, this study reveals that attempting to repel systemic threats by relying on isolated data privacy compliance or singular algorithmic robustness enhancement is fundamentally flawed. Shattering the black-box deadlock of liability attribution and the fragmented dilemma of cross-national regulation fundamentally requires establishing the holistic governance architecture of “dual-track synergistic regulation of data and algorithms.” This architecture necessitates not only reconstructing a composite attribution system at the macro-legal level that balances strict liability with mandatory insurance [96]. It also demands the deep convergence of Privacy-Enhancing Technologies, Threat Analysis models, and Explainable AI at the micro-engineering level, actualizing the mandatory code mapping of abstract compliance requirements. Confronting the rapidly approaching critical threshold of technological leaps, only by organically integrating technological innovation, regulatory evolution, and societal public value under an open and mutually trusted international standard system can the large-scale deployment of connected and automated vehicles truly fulfill its social promise to elevate human mobility and welfare.

Author Contributions: Conceptualization, Y.Y. (Yifen Yin) and Y.Y. (Yuanyuan Yu); methodology, C.W.; software, C.W. and J.C.; validation, J.C.; formal analysis, H.H. and W.I.H.; data curation, H.H.; writing—original draft preparation, C.W., J.C. and H.H.; writing—review and editing, Y.Y. (Yifen Yin) and Y.Y. (Yuanyuan Yu) and C.W.; visualization, J.C.; supervision, Y.Y. (Yifen Yin); project administration, W.I.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original data presented in the study are openly available in FigShare at <http://doi.org/10.6084/m9.figshare.32494149>.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Bodei, C.; Vincenzi, M.D.; Matteucci, I. From hardware-functional to software-defined vehicles and their security issues. In *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*; IEEE: New York, NY, USA, 2023; pp. 1–10. <https://doi.org/10.1109/INDIN51400.2023.10217971>.
2. Tien, J.M. The Sputnik of servgoods: Autonomous vehicles. *J. Syst. Sci. Syst. Eng.* **2017**, *26*, 133–162. <https://doi.org/10.1007/s11518-016-5325-1>.
3. Wan, F. Regulatory challenges and legal responses to autonomous driving in the era of artificial intelligence. *J. Beijing Norm. Univ.* **2025**, *03*, 150–160. (In Chinese)
4. Greifenstein, M.; La Delfa, A.; Han, Z. A framework for preparing cities for the successful implementation of shared autonomous vehicles: An integrative literature review. *Sustain. Cities Soc.* **2025**, *130*, 106515. <https://doi.org/10.1016/j.scs.2025.106515>.
5. Lim, H.S.M.; Taeihagh, A. Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies* **2018**, *11*, 1062. <https://doi.org/10.3390/en11051062>.
6. Elongha, G.; Almuthaybiri, M.; Mgembe, I. Cross-disciplinary threats mitigation framework for AI autonomous vehicles. *Issues Inf. Syst.* **2024**, *25*, 483–495. https://doi.org/10.48009/3_iis_2024_136.
7. Bridgelall, R. Perspectives on Securing the Transportation System. *Vehicles* **2022**, *4*, 1332–1343. <https://doi.org/10.3390/vehicles4040070>.
8. Chougule, A.; Chamola, V.; Sam, A.; Yu, F.R.; Sikdar, B. A comprehensive review on limitations of autonomous driving and its impact on accidents and collisions. *IEEE Open J. Veh. Technol.* **2024**, *5*, 142–161. <https://doi.org/10.1109/OJVT.2023.3335180>.
9. Hamza, G.; Taher, Y.; Es-sadek, M.Z.; Tmiri, A. Cybersecurity in autonomous vehicles: A comprehensive review study of cyber-attacks and AI-based solutions. *Int. J. Eng. Trends Technol.* **2024**, *72*, 101–116. <https://doi.org/10.14445/22315381/IJETT-V72I1P111>.
10. Gaeta, M.C. The regulation of certain aspects of autonomous driving in the Italian legal system. *Eur. J. Priv. Law Technol.* **2022**, *1*, 263–288. <https://doi.org/10.57230/ejplt221MCG>.
11. Czech, P. Artificial intelligence as a basic problem when implementing autonomous vehicle technology in everyday life. *Sci. J. Silesian Univ. Technol. Ser. Transp.* **2024**, *122*, 49–60. <https://doi.org/10.20858/sjsutst.2024.122.3>.
12. Tarr, J.-A.; Wilkinson, D.; Tarr, A. Insurance in the Digital Age: Legal and Regulatory Challenges. *J. Bus. Law* **2024**, *2024*, 205–236. Available online: <https://eprints.qut.edu.au/246209/> (accessed on 25 June 2026).
13. Ito, H.; Kester, J. Governing beyond innovation: Exploring the impact of connected and automated vehicles on the organization of vehicle accident investigations. *Int. J. Sustain. Transp.* **2023**, *17*, 1171–1182. <https://doi.org/10.1080/15568318.2022.2160283>.
14. Dunphy, A. Is the regulation of connected and automated vehicles (CAVs) a wicked problem and why does it matter? *Comput. Law Secur. Rev.* **2024**, *52*, 105944. <https://doi.org/10.1016/j.clsr.2024.105944>.
15. Taeihagh, A.; Lim, H.S.M. Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transp. Rev.* **2019**, *39*, 103–128. <https://doi.org/10.1080/01441647.2018.1494640>.
16. Fagnant, D.J.; Kockelman, K. Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transp. Res. Part A Policy Pract.* **2015**, *77*, 167–181. <https://doi.org/10.1016/j.tra.2015.04.003>.
17. Mallinson, D.J.; Azevedo, L.; Best, E.; Robles, P.; Wang, J. The Future of AI Is in the States: The Case of Autonomous Vehicle Policies. *Bus. Politics* **2024**, *26*, 180–199. <https://doi.org/10.1017/bap.2023.19>.
18. de Leo, G.; Miragliotta, G. Barriers to autonomous vehicles adoption in Europe: Insights from literature and interviews. *J. Urban Mobil.* **2026**, *9*, 100194. <https://doi.org/10.1016/j.urbmob.2026.100194>.

19. Shatnawi, I.; Gonzalez, J.N.; Masoud, N. Toward AV-CAV deployment in the Kingdom of Saudi Arabia: A readiness assessment based on expert feedback. *Res. Transp. Bus. Manag.* **2025**, *60*, 101378. <https://doi.org/10.1016/j.rtbm.2025.101378>.
20. Yu, J. The framework and key points of autonomous vehicle industry governance. *Adm. Law. Rev.* **2019**, *02*, 114–125. (In Chinese)
21. Abu Bakar, A.I.; Abas, M.A.; Muhamad Said, M.F.; Tengku Azhar, T.A. Synthesis of Autonomous Vehicle Guideline for Public Road-Testing Sustainability. *Sustainability* **2022**, *14*, 1456. <https://doi.org/10.3390/su14031456>.
22. Dudziak, A.; Stoma, M.; Kuranc, A.; Caban, J. Assessment of Social Acceptance for Autonomous Vehicles in Southeastern Poland. *Energies* **2021**, *14*, 5778. <https://doi.org/10.3390/en14185778>.
23. Yang, Y.; Song, Z. The public perception and adaptability of laws and regulations of autonomous driving vehicles. *Humanit. Soc. Sci. Commun.* **2025**, *12*, 1224. <https://doi.org/10.1057/s41599-025-05600-6>.
24. Hemesath, S.; Tepe, M. Multidimensional preference for technology risk regulation: The role of political beliefs, technology attitudes, and national innovation cultures. *Regul. Gov.* **2024**, *18*, 1264–1283. <https://doi.org/10.1111/rego.12578>.
25. Ryan, M. The future of transportation: Ethical, legal, social and economic impacts of self-driving vehicles in the year 2025. *Sci. Eng. Ethics* **2020**, *26*, 1185–1208. <https://doi.org/10.1007/s11948-019-00130-2>.
26. Khan, S.K.; Shiwakoti, N.; Stasinopoulos, P. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Accid. Anal. Prev.* **2022**, *165*, 106515. <https://doi.org/10.1016/j.aap.2021.106515>.
27. Dias Lousã, M.; Teixeira, H.; Pereira de Moraes, J.C. The evolution of cybersecurity in self-driving cars: Insights from bibliometric research. *Int. J. Innov. Sci.* **2025**, *17*, 880–900. <https://doi.org/10.1108/IJIS-06-2024-0158>.
28. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. <https://doi.org/10.1136/bmj.n71>.
29. EU AI Act; EU artificial intelligence act: Up-to-date developments and analyses of the EU AI Act. Future of Life Institute: Cambridge, USA, 2026. Available online: <https://artificialintelligenceact.eu/> (accessed on 9 July 2026).
30. UN Regulation No. 155; Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. United Nations Economic Commission for Europe: Geneva, Switzerland, 2021. Available online: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security> (accessed on 9 July 2026).
31. ISO/SAE 21434; Road Vehicles—Cybersecurity Engineering. International Organization for Standardization & SAE International: Geneva, Switzerland, 2021. Available online: <https://www.iso.org/standard/70918.html> (accessed on 9 July 2026).
32. Landis, J.R.; Koch, G.G. The Measurement of Observer Agreement for Categorical Data. *Biometrics* **1977**, *33*, 159–174. <https://doi.org/10.2307/2529310>.
33. Lütge, C.; Poszler, F.; Acosta, A.J.; Danks, D.; Gottehrer, G.; Mihet-Popa, L.; Naseer, A. AI4People: Ethical Guidelines for the Automotive Sector—Fundamental Requirements and Practical Recommendations. *Int. J. Technoethics* **2021**, *12*, 101–125. <https://doi.org/10.4018/IJT.20210101.oa2>.
34. Martinho, A.; Herber, N.; Kroesen, M.; Chorus, C. Ethical issues in focus by the autonomous vehicles industry. *Transp. Rev.* **2021**, *41*, 556–577. <https://doi.org/10.1080/01441647.2020.1862355>.
35. Hess, D.J.; Lee, D.; Biebl, B.; Fränze, M.; Lehnhoff, S.; Neema, H.; Niehaus, J.; Pretschner, A.; Sztipanovits, J. A comparative, sociotechnical design perspective on Responsible Innovation: Multidisciplinary research and education on digitized energy and Automated Vehicles. *J. Responsible Innov.* **2021**, *8*, 421–444. <https://doi.org/10.1080/23299460.2021.1975377>.
36. Zhao, T.; Wang, Y. Derived risks of urban autonomous vehicles from the perspective of macro-security: Spatiotemporal patterns and prevention mechanisms. *Urban Dev. Stud.* **2025**, *32*, 57–66. (In Chinese)
37. Gekker, A.; Hind, S. Infrastructural surveillance. *New Media Soc.* **2020**, *22*, 1414–1436. <https://doi.org/10.1177/1461444819879426>.
38. Jannusch, T.; David-Spickermann, F.; Shannon, D.; Ressel, J.; Völler, M.; Murphy, F.; Furxhi, I.; Cunneen, M.; Mullins, M. Surveillance and privacy—Beyond the panopticon. An exploration of 720-degree observation in level 3 and 4 vehicle automation. *Technol. Soc.* **2021**, *66*, 101667. <https://doi.org/10.1016/j.techsoc.2021.101667>.
39. Lu, C.; Xin, X. Key stakeholder perceived value influence on autonomous vehicles privacy and security governance—An evolutionary analysis based on the prospect theory. *Asia Pac. J. Innov. Entrep.* **2024**, *18*, 131–155. <https://doi.org/10.1108/APJIE-12-2023-0242>.
40. Okomanyi, A.O.; Sherwood, A.R.; Shittu, E. Exploring effective strategies against cyberattacks: The case of the automotive industry. *Environ. Syst. Decis.* **2024**, *44*, 779–809. <https://doi.org/10.1007/s10669-024-09971-0>.
41. Chen, T.; Liu, Y. How to govern autonomous driving?—Function realization, ethical challenges, and governance system of autonomous driving. *Zhejiang Acad. J.* **2025**, *4*, 37–48. (In Chinese) <https://doi.org/10.16235/j.cnki.33-1005/c.2025.04.005>

42. Dudziak, A.; Drożdziel, P.; Stoma, M.; Caban, J. Market Electrification for BEV and PHEV in Relation to the Level of Vehicle Autonomy. *Energies* **2022**, *15*, 3120. <https://doi.org/10.3390/en15093120>.
43. Dižo, J.; Blatnický, M.; Semenov, S.; Mikhailov, E.; Kostrzewski, M.; Drożdziel, P.; Šťastniak, P. Electric and plug-in hybrid vehicles and their infrastructure in a particular European region. *Transp. Res. Procedia* **2021**, *55*, 629–636. <https://doi.org/10.1016/j.trpro.2021.07.029>.
44. Stegelmann, M.; Kesdogan, D. V2GPriv: Vehicle-to-grid privacy in the smart grid. In *Cyberspace Safety and Security*; Xiang, Y., Lopez, J., Kuo, C.C.J., Zhou, W., Eds.; Springer: Cham, Switzerland, 2012; Volume 7672. https://doi.org/10.1007/978-3-642-35362-8_9.
45. Zheng, G. Data rule of law and future transportation: A modest proposal on data governance for autonomous vehicles. *China Law Rev.* **2022**, *01*, 202–214. (In Chinese)
46. Funta, R. Automated driving and data protection: Some remarks on fundamental rights and privacy. *Kryt. Prawa* **2021**, *13*, 106–118. <https://doi.org/10.7206/kp.2080-1084.495>.
47. Xu, Z. Legal regulation of data processing for intelligent and connected vehicles: Realities, challenges, and approaches. *J. Lanzhou Univ.* **2022**, *50*, 100–111. (In Chinese) <https://doi.org/10.13885/j.issn.1000-2804.2022.02.009>
48. Collingwood, L. Privacy implications and liability issues of autonomous vehicles. *Inf. Commun. Technol. Law* **2017**, *26*, 32–45. <https://doi.org/10.1080/13600834.2017.1269871>.
49. Hacker, P. Personal data, exploitative contracts, and algorithmic fairness: Autonomous vehicles meet the internet of things. *Int. Data Priv. Law* **2017**, *7*, 266–286. <https://doi.org/10.1093/idpl/ixp014>.
50. Du, M. Dilemmas and approaches of privacy protection in the operation of autonomous vehicles. *J. Henan Univ. Econ. Law* **2021**, *36*, 28–40. (In Chinese)
51. Zhang, X.; Qiu, B. Data security risks of autonomous vehicles and their governance. *J. Anhui Norm. Univ.* **2025**, *53*, 125–135. (In Chinese) <https://doi.org/10.14182/j.cnki.j.anu.2025.05.013>
52. Regulation (EU) 2016/679; General Data Protection Regulation. Publisher: Official Journal of the European Union: Brussels, Belgium, 2016. Available online: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed on 9 July 2026).
53. Zhang, T.; Jiang, Y. Personal data protection for intelligent vehicles: Explorations and enlightenment from the European Union and Germany. *Ger. Stud.* **2019**, *34*, 92–113, 151. (In Chinese)
54. Daly, A. Privacy in automation: An appraisal of the emerging Australian approach. *Comput. Law Secur. Rev.* **2017**, *33*, 836–846. <https://doi.org/10.1016/j.clsr.2017.05.009>.
55. Barrett, L. Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception. *Georget. Law. J.* **2017**, *106*, 181–208. Available online: https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/note-Herbie-Fully-Downloaded-Data-Driven-Vehicles-and-the-Automobile-Exception_Barrett.pdf (accessed on 25 June 2026).
56. Pearson, A. Putting the Blindfolds on Driverless Panopticons. *Columbia J. Law Soc. Probl.* **2023**, *56*, 245–293. Available online: <https://jlsplaw.columbia.edu/files/2023/02/Vol56-2-Pearson.pdf> (accessed on 25 June 2026).
57. Chapter 25; Investigatory Powers Act 2016. Publisher: UK Parliament: London, UK, 2016. <https://www.legislation.gov.uk/ukpga/2016/25/contents> (accessed on 9 July 2026).
58. Marson, J.; White, M.; Ferris, K. The Investigatory Powers Act 2016 and connected vehicles: A new form of panspectric veillance looming? *Statut. Law Rev.* **2023**, *44*, hmac004. <https://doi.org/10.1093/slr/hmac004>.
59. AB-375; California Consumer Privacy Act of 2018. Publisher: California State Legislature: Sacramento, USA, 2018. https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (accessed on 9 July 2026).
60. Act No. 10465; Personal Information Protection Act. Publisher: National Assembly of South Korea: Seoul, Republic of Korea, 2011. Available online: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG (accessed on 9 July 2026).
61. Kim, K.; Han, H.; Yoo, S. BERTopic Modeling Analysis of Privacy Protection Trends in New Trade Rules for the Mobility Industry. *Teh. Vjesn. Tech. Gaz.* **2026**, *33*, 1047–1055. <https://doi.org/10.17559/TV-20250901002936>.
62. Li, R. Autonomous driving data regulation from the dual perspectives of data security and industrial development. *Adm. Reform* **2021**, *08*, 79–85. (In Chinese) <https://doi.org/10.14150/j.cnki.1674-7453.2021.08.008>
63. Zhao, H. The path selection of “Internet of Vehicles” data governance in China from the perspective of comparative law. *J. Shanghai Univ. Financ. Econ.* **2021**, *23*, 139–152. (In Chinese) <https://doi.org/10.16538/j.cnki.jsufe.2021.05.010>
64. Chen, B. Coordinating security and connectivity to promote data governance for autonomous driving. *People's Trib.* **2023**, *18*, 73–77. (In Chinese)
65. Sun, T.; Xu, Y.; Wang, H.; Chen, Z. A Legal Study: How Do China's Top 10 Intelligent Connected Vehicle Companies Protect Consumer Rights? *World Electr. Veh. J.* **2025**, *16*, 140. <https://doi.org/10.3390/wevj16030140>.

66. Xu, Y.; Wei, J.; Mi, T.; Chen, Z. Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics. *World Electr. Veh. J.* **2025**, *16*, 6. <https://doi.org/10.3390/wevj16010006>.
67. Krausová, A.; Matejka, J. Autonomous vehicles and in-vehicle data in the context of motor insurance. *Lawyer Q.* **2020**, *10*, 153–169. Available online: <https://old.tlq.ilaw.cas.cz/index.php/tlq/article/view/403/408#> (accessed on 25 June 2026).
68. Zhu, J. Research on data notification and protection mechanisms of UBI auto insurance under the Internet of Vehicles. *Financ. Regul. Res.* **2020**, *08*, 102–114. (In Chinese) <https://doi.org/10.13490/j.cnki.frr.2020.08.006>
69. Beguni, C.; Căilean, A.-M.; Zadobrischi, E.; Avătămăniței, S.-A.; Lavric, A.; Stoian, F.-M. The Convergence of Artificial Intelligence and Public Policy in Shaping the Future of Ride-Hailing: A Review. *Smart Cities* **2026**, *9*, 40. <https://doi.org/10.3390/smartcities9020040>.
70. Cveticanin, L.; Luzanin, O.; Ninkov, I. Privacy and personal data protection in self-driving car: Suggestion for legal regulation in Serbia. *Balk. Soc. Sci. Rev.* **2023**, *22*, 171–189. <https://doi.org/10.46763/BSSR232222171c>.
71. Song, Z.; Xu, Y. Logical basis and path optimization of legal governance for autonomous driving data. *J. Chongqing Univ.* **2026**, 1–17. <https://link.cnki.net/urlid/50.1023.c.20260204.1332.002>. (In Chinese)
72. Yu, J. Public-private partnership protection of user privacy for autonomous vehicles. *Adm. Law Rev.* **2026**, *03*, 169–181. (In Chinese)
73. Deng, H.; Hu, Q.; Guan, C.; Chen, Y.S.; Menendez, M. Building a government-owned open data platform for connected and autonomous vehicles. *Cities* **2024**, *149*, 104918. <https://doi.org/10.1016/j.cities.2024.104918>.
74. Zheng, L. Sandbox regulatory construction for autonomous driving data security. *Forum Sci. Technol. China* **2023**, 154–162. (In Chinese) <https://doi.org/10.13580/j.cnki.fstc.2023.05.008>
75. Hews, R.; Dunphy, A. Vehicle generated data regulatory sandbox: A legal design approach to policy prototyping for connected and automated vehicles. *Law Innov. Technol.* **2026**, *18*, 107–140. <https://doi.org/10.1080/17579961.2026.2633683>.
76. Schoonmaker, J. Proactive privacy for a driverless age. *Inf. Commun. Technol. Law* **2016**, *25*, 96–128. <https://doi.org/10.1080/13600834.2016.1184456>.
77. Lu, Y.; Li, H.; Tu, H.; Liu, J.; Yuan, Y.; van Lint, H. Quantitative assessment on the misuse risk of intelligent connected vehicle data. *J. Transp. Eng. Part A Syst.* **2026**, *152*, 04025133. <https://doi.org/10.1061/JTEPBS.TEENG-9361>.
78. Liu, D.; Liu, Z.; Liu, Y.; Qiu, B.; Wang, S. Research on automobile data security risk analysis based on TARA method. In Proceedings of the 2024 IEEE 9th International Conference on Data Science in Cyberspace (DSC), Jinan, China, 23–26 August 2024; pp. 162–170. <https://doi.org/10.1109/DSC63484.2024.00029>.
79. De Santis, M.; Esposito, C.; Mastroianni, M. Privacy risks in connected vehicles: Profiling threats and mitigation strategies. In *Computational Science and Its Applications—ICCSA 2025 Workshops*; Gervasi, O.; et al., Eds.; Springer: Cham, Switzerland, 2026; Volume 15893. https://doi.org/10.1007/978-3-031-97645-2_19.
80. Munn, L. Staying at the Edge of Privacy: Edge Computing and Impersonal Extraction. *Media Commun.* **2020**, *8*, 270–279. <https://doi.org/10.17645/mac.v8i2.2761>.
81. Znidi, F.; Morsy, M.; Rathore, H. Future on wheels: Safeguarding privacy in tomorrow's connected vehicles-FUTURE-SP. *IEEE Access* **2024**, *12*, 179857–179878. <https://doi.org/10.1109/ACCESS.2024.3505158>.
82. Hammedi, R.; Brown, D.J.; Kaiwartya, O.; Gaur, P. Securing Data in Vehicles: Privacy-Preserving Frameworks for Dynamic CAV Environments. *Sensors* **2026**, *26*, 1326. <https://doi.org/10.3390/s26041326>.
83. Baayeh, K.; Beleya, P.; Akhtar, S.; Airawaty, D. Blockchain-based data integrity and privacy in vehicle-to-everything (V2X) communication networks: A systematic literature review. *Multidiscip. Rev.* **2026**, *9*, 2026350. <https://doi.org/10.31893/multi-rev.2026350>.
84. Dargahi, T.; Ahmadvand, H.; Alraja, M.N.; Yu, C.-M. Integration of blockchain with connected and autonomous vehicles: Vision and challenge. *J. Data Inf. Qual.* **2021**, *14*, 5. <https://doi.org/10.1145/3460003>.
85. Hu, J.; Zhang, J.; Wu, J.; Yang, Y.; Long, C.; Li, B. Trusted data spaces for vehicle-road-cloud collaboration: Architecture, challenges, and future directions. *IEEE Netw.* **2026**, *ahead of prints*. <https://doi.org/10.1109/MNET.2026.3669250>.
86. Khan, S.K.; Shiwakoti, N.; Stasinopoulos, P.; Warren, M. Modelling cybersecurity regulations for automated vehicles. *Accid. Anal. Prev.* **2023**, *186*, 107054. <https://doi.org/10.1016/j.aap.2023.107054>.
87. Alawadhi, M.; Almazrouie, J.; Kamil, M.; Khalil, K.A. Review and analysis of the importance of autonomous vehicles liability: A systematic literature review. *Int. J. Syst. Assur. Eng. Manag.* **2020**, *11*, 1227–1249. <https://doi.org/10.1007/s13198-020-00978-9>.
88. Selbst, A.D. Negligence and AI's Human Users. *Boston Univ. Law. Rev.* **2020**, *100*, 1315–1376. Available online: <https://www.bu.edu/bulawreview/files/2020/09/SELBST.pdf> (accessed on 25 June 2026).

89. Li, M. Security risks and criminal governance in the application of artificial intelligence. *J. East China Univ. Sci. Technol.* **2025**, *40*, 129–145. (In Chinese)
90. Maskur, M.A.; Masyhar, A.; Damayanti, R.; Ramada, D.P.; Sanyal, S. Reimagining Criminal Liability in the Age of Artificial Intelligence: Toward a Comparative and Reform-Oriented Legal Framework. *J. Law Leg. Reform* **2025**, *6*, 1805–1838. <https://doi.org/10.15294/jllr.v6i4.35540>.
91. Saleh, A.M.S. A Cyclic Framework for Ethical Implications of Artificial Intelligence in Autonomous Vehicles. *Int. J. Adv. Comput. Sci. Appl.* **2024**, *15*, 340–355. Available online: https://thesai.org/Downloads/Volume15No3/Paper_35-A_Cyclic_Framework_for_Ethical_Implications.pdf (accessed on 25 June 2026).
92. Popescu Ljungholm, D. Autonomous car regulation in the smart transportation infrastructure: Ethical issues, legal liabilities, and privacy concerns. *Geopolit. Hist. Int. Relat.* **2019**, *11*, 7–12. <https://doi.org/10.22381/GHIR11220191>.
93. Marchant, G. Swords and Shields: Impact of Private Standards for Liability Determinations of Autonomous Vehicles. *J. Tort Law* **2025**, *18*, 311–332. <https://doi.org/10.1515/jtl-2025-0016>.
94. Dhar, V. Equity, safety, and privacy in the autonomous vehicle era. *Computer* **2016**, *49*, 80–83. <https://doi.org/10.1109/MC.2016.326>.
95. Abuelenin, A.H.M. Cybersecurity breaches in connected and autonomous vehicles: Rethinking liability and insurance frameworks. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2025**, *19*, 1211–1219. <https://doi.org/10.12716/1001.19.04.19>.
96. Qi, M. Legal construction of compulsory liability insurance for artificial intelligence: A case study of intelligent driving. *Orient. Law* **2025**, *06*, 17–32. (In Chinese) <https://doi.org/10.19404/j.cnki.dffx.2025.06.004>
97. Llorca, D.F.; Hamon, R.; Junklewitz, H.; Grosse, K.; Kunze, L.; Seiniger, P.; Swaim, R.; Reed, N.; Alahi, A.; Gómez, E.; et al. Testing autonomous vehicles and AI: Perspectives and challenges from cybersecurity, transparency, robustness and fairness. *Eur. Transp. Res. Rev.* **2025**, *17*, 38. <https://doi.org/10.1186/s12544-025-00732-x>.
98. Wei, C.; Zhao, J.; Sun, L. Achieving regulatory alignment for E2E autonomous driving in China: A framework for tort liability and data governance. *Comput. Law Secur. Rev.* **2025**, *59*, 106192. <https://doi.org/10.1016/j.clsr.2025.106192>.
99. Chamola, V.; Hassija, V.; Sulthana, A.R.; Ghosh, D.; Dhingra, D.; Sikdar, B. A review of trustworthy and explainable artificial intelligence (XAI). *IEEE Access* **2023**, *11*, 78994–79015. <https://doi.org/10.1109/ACCESS.2023.3294569>.
100. Kim, D.; Park, S.W.; Park, J.W. EGIS: A resilient and recoverable dual-brain controller architecture for physical AI systems under the EU AI Act. In Proceedings of the 2025 25th International Conference on Control, Automation and Systems (ICCAS), Incheon, Republic of Korea, 4–7 November 2025; pp. 2212–2217. <https://doi.org/10.23919/ICCAS66577.2025.11301361>.
101. Benyahya, M.; Collen, A.; Lenard, T.; Nijdam, N.A. TARA 2.0 for connected and automated vehicles. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 11864–11878. <https://doi.org/10.1109/TITS.2025.3574638>.
102. Mazzara, B.; Davidovich, I. Integrating functional and component-level threat analyses in automotive systems: A holistic approach to risk assessment. In Proceedings of the WCX SAE World Congress Experience, Detroit, MI, USA, 16 April 2024. <https://doi.org/10.4271/2024-01-2797>.
103. Lim, H.S.M.; Taeihagh, A. Algorithmic Decision-Making in AVs: Understanding Ethical and Technical Concerns for Smart Cities. *Sustainability* **2019**, *11*, 5791. <https://doi.org/10.3390/su11205791>.
104. Order No. 84; Data Security Law of the Peoples Republic of China. Publisher: National Peoples Congress: Beijing, China, 2021. Available online: <https://database.cyberpolicyportal.org/api/files/1664278723048r9y58968qht.pdf> (accessed on 9 July 2026).
105. Chen, Y. Classification, preservation, and compliance of autonomous driving algorithm data under the Data Security Law. *Sci. Technol. Law* **2022**, *03*, 85–92. (In Chinese) <https://doi.org/10.19685/j.cnki.cn11-2922/n.2022.03.010>
106. Cao, J. On the algorithm safety regulation of autonomous vehicles. *J. East China Univ. Political Sci. Law.* **2023**, *26*, 22–33. (In Chinese)
107. Almuhammadi, S.; AlBaluchi, H.; Alawida, M. A NIST CSF-based cybersecurity profile for AI and machine learning systems in transportation networks. *J. Transp. Secur.* **2026**, *19*, 34. <https://doi.org/10.1007/s12198-026-00355-w>.
108. Tekeste, B.; Al-Hussaini, K.; Fung, B.C.M.; Alawadhi, I.; Fachkha, C. Adversarial machine learning: A 20-year survey of attacks, defenses, and standards. *IEEE Access* **2026**, *14*, 69778–69812. <https://doi.org/10.1109/ACCESS.2026.3690620>.
109. Cobos, L.-P.; Ruddle, A.R.; Sabaliauskaite, G. Cybersecurity Assurance Challenges for Future Connected and Automated Vehicles. In Proceedings of the 31st European Safety and Reliability Conference, Angers, France, 19–23 September 2021; pp. 2038–2045. https://doi.org/10.3850/978-981-18-2016-8_412-cd.
110. ISO 26262:2018; Road Vehicles—Functional Safety. Publisher: ISO: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/standard/68383.html> (accessed on 9 July 2026).

111. Siddiqui, F.; Khan, R.; Tasdemir, S.Y.; Hui, H.; Sonigara, B.; Sezer, S.; McLaughlin, K. Cybersecurity engineering: Bridging the security gaps in advanced automotive systems and ISO/SAE 21434. In *Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, Florence, Italy, 20–23 June 2023; pp. 1–6. <https://doi.org/10.1109/VTC2023-Spring57618.2023.10200490>.
112. Cas, S.G.; Salceanu, A. Autonomous and electrical vehicles development using optimized processes defined by cyber security and safety management system. In *Proceedings of the 2021 International Conference on Electromechanical and Energy Systems (SIELMEN)*; IEEE: New York, NY, USA, 2021; pp. 257–261. <https://doi.org/10.1109/SIELMEN53755.2021.9600343>.
113. Ghosh, S.; Zaboli, A.; Hong, J.; Kwon, J. An integrated approach of threat analysis for autonomous vehicles perception system. *IEEE Access* **2023**, *11*, 14752–14777. <https://doi.org/10.1109/ACCESS.2023.3243906>.
114. Jayaratne, D.N.D.; Lu, Q.; Rakib, A.; Ramli, M.A.; Mepparambath, R.M.; Shaikh, S.A.; Nguyen, H.N. A quantitative methodology for systemic impact assessment of cyber threats in connected vehicles. *Comput. Secur.* **2026**, *160*, 104729. <https://doi.org/10.1016/j.cose.2025.104729>.
115. Kamtam, S.H.; Lu, Q.; Rakib, A.; Ramli, M.A.; Mepparambath, R.M.; Shaikh, S.A.; Nguyen, H.N. WOLVES: Window of opportunity attack feasibility likelihood value estimation through a simulation-based approach. *Comput. Secur.* **2025**, *157*, 104549. <https://doi.org/10.1016/j.cose.2025.104549>.
116. Ray, P.P. A review of TRiSM frameworks in artificial intelligence systems: Fundamentals, taxonomy, use cases, key challenges and future directions. *Expert Syst.* **2026**, *43*, e70213. <https://doi.org/10.1111/exsy.70213>.
117. Benyahya, M.; Collen, A.; Nijdam, N.A. Analyses on standards and regulations for connected and automated vehicles: Identifying the certifications roadmap. *Transp. Eng.* **2023**, *14*, 100205. <https://doi.org/10.1016/j.treng.2023.100205>.
118. *UN Regulation No. 156; Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Update Management System*. Publisher: UNECE: Geneva, Switzerland, 2021. Available online: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update> (accessed on 9 July 2026).
119. Kurumbudel, P. Cybersecurity in automotive OTA update systems and automotive software stores [Paper presentation]. In *Proceedings of the Symposium on International Automotive Technology*, Pune, India, 28 January 2026. <https://doi.org/10.4271/2026-26-0621>.
120. Iyieke, V.; Jadidbonab, H.; Rakib, A.; Bryans, J.; Dhaliwal, D.; Kosmas, O. An adaptable security-by-design approach for ensuring a secure over the air (OTA) update in modern vehicles. *Comput. Secur.* **2025**, *150*, 104268. <https://doi.org/10.1016/j.cose.2024.104268>.
121. Menekşe, M.D.; Özçetin, O.; Doğan, K.F.; Sevim, T.; Mersin, G.; Çekerek, M.N. Threat analysis and risk assessment with cybersecurity countermeasures for over-the-air enabled lane keeping assist. In *2024 Innovations in Intelligent Systems and Applications Conference (ASYU)*; IEEE: New York, NY, USA, 2024; pp. 1–6. <https://doi.org/10.1109/ASYU62119.2024.10756971>.
122. Wen, H.; Chen, R.; Wang, J.; Wu, H. Research on the regulatory framework and full-chain security protection scheme for OTA updates of intelligent connected vehicles. In *Proceedings of the 2025 4th International Conference on Cyber Security, Artificial Intelligence and the Digital Economy*; ACM: New York, NY, USA, 2025; pp. 1–8. <https://doi.org/10.1145/3729706.3729707>.
123. Luo, F.; Li, Z.; Tong, Y.; Liao, Z.; Zhang, Z.; Liu, Q. PeTARA: A privacy-enhanced threat analysis and risk assessment method for intelligent connected vehicles. *J. Inf. Secur. Appl.* **2026**, *98*, 104408. <https://doi.org/10.1016/j.jisa.2026.104408>.
124. Lautenbach, A.; Almgren, M.; Olovsson, T. Proposing HEAVENS 2.0—An automotive risk assessment model. In *Proceedings of the 5th ACM Computer Science in Cars Symposium*; ACM: New York, NY, USA, 2021. <https://doi.org/10.1145/3488904.3493378>.
125. Barletta, V.S.; Caivano, D.; De Vincentiis, M.; Sánchez, L.E.; Santos-Olmo, A.; Serrano, M.A. MARISMA-CAR: A preliminary approach to risk assessment in automotive security. In *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)*; IEEE: New York, NY, USA, 2024; pp. 574–579. <https://doi.org/10.1109/MASS62177.2024.00091>.
126. Zhou, Z.; Zhi, Q.; Tao, L.; Ping, P.; Long, Q. ODFa²: Overall defense framework against cyber-attacks on intelligent connected vehicles. *IEEE Trans. Veh. Technol.* **2024**, *73*, 6318–6331. <https://doi.org/10.1109/TVT.2023.3345156>.
127. Tany, N.S.; Suresh, S.; Sinha, D.N.; Shinde, C.; Stolojesu-Crisan, C.; Khondoker, R. Cybersecurity Comparison of Brain-Based Automotive Electrical and Electronic Architectures. *Information* **2022**, *13*, 518. <https://doi.org/10.3390/info13110518>.
128. De Vincenzi, M.; Costantino, G.; Matteucci, I.; Fenzl, F.; Plappert, C.; Rieke, R.; Zelle, D. A systematic review on security attacks and countermeasures in automotive Ethernet. *ACM Comput. Surv.* **2024**, *56*, 135. <https://doi.org/10.1145/3637059>.
129. Iyieke, V.; Bryans, J.; Robinson, T.; Kosmas, O.; Shipman, A.; Jadidbonab, H. An adaptable security by design approach for ensuring a secured remote monitoring teleoperation (RMTO) of an autonomous vehicle. In *WCS SAE World Congress Experience, Detroit, MI, USA, 18 April 2023*; SAE Technical Papers; SAE International: Warrendale, PA, USA, 2023.

130. Sommer, F.; Gierl, M.; Kriesten, R.; Kargl, F.; Sax, E. Combining cyber security intelligence to refine automotive cyber threats. *ACM Trans. Priv. Secur.* **2024**, *27*, 16. <https://doi.org/10.1145/3644075>.
131. Ilg, M.; Rieger, V.; Angermeier, D. A systematic approach to modeling software-defined vehicles and their security needs. In *Proceedings of the AmE 2023—Automotive meets Electronics; 14. GMM Symposium*; IEEE: New York, NY, USA, 2023; pp. 68–72. Available online: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10227707> (accessed on 25 June 2026).
132. Fischer, A.; Tolvanen, J.P.; Kolagari, R.T. Automotive Cybersecurity Engineering with Modeling Support. In *Proceedings of the 2024 19th Conference on Computer Science and Intelligence Systems (FedCSIS)*; IEEE: New York, NY, USA, 2024; pp. 319–329. <https://doi.org/10.15439/2024F5017>.
133. Fischer, A.; Tolvanen, J.P.; Kolagari, R.T. Embedded systems security co-design: Modeling support for managers and developers. In *Software, System, and Service Engineering*; Kardas, G., Geylani, K., Ivan, L., Boris, M., Aleksandar, P., Łukasz, R., Mirosław, S., Jakub, S., Adam, P., Eds.; Springer: Cham, Switzerland, 2025; Volume 542. https://doi.org/10.1007/978-3-031-84913-8_8.
134. Xie, H.; Wang, L. Cybersecurity Threat Analysis and Risk Assessment for Intelligent Connected Vehicles. *Promet—Traffic Transp.* **2026**, *38*, 412–423. <https://doi.org/10.7307/ptt.v38i2.1067>.
135. Zhu, K.; Tian, D.; Zou, B.; Cai, P.; Li, Y. Testing practice of cybersecurity validation of intelligent connected vehicles. In *Advances and Applications in SmartRail, Traffic, and Transportation Engineering*; Jia, L., Wang, Y., Easa, S., Eds.; Springer: Singapore, 2025; Volume 1432. https://doi.org/10.1007/978-981-96-7441-1_12.
136. Liu, Y.; Yang, X.; Li, M.; Zhou, S. Threat Analysis and Risk Assessment for Applying Cybersecurity Engineering. *Proc. SPIE-Int. Soc. Opt. Eng.* **2023**, 12602, 1260218. <https://doi.org/10.1117/12.2668050>.
137. Lim, D.-S.; Lee, S.-J. Autonomous Vehicle Ecosystem Security: Utilizing Autonomous Vehicle Security-Level Checks through Analytic Hierarchy Process. *Appl. Sci.* **2024**, *14*, 8247. <https://doi.org/10.3390/app14188247>.
138. GB/T 40861-2021; General Requirements for Cybersecurity Of Vehicle. Publisher: State Administration for Market Regulation: Beijing, China, 2021. Available online: <https://openstd.samr.gov.cn/bzgk/std/> (accessed on 9 July 2026).
139. Yu, L.Y.; Zhu, Q.; Zheng, L. Autonomous Vehicles Regulation in Beijing. *Tsinghua China Law Rev.* **2024**, *17*, 132–165. Available online: <https://www.tsinghuachinalawreview.law.tsinghua.edu.cn/UploadFiles/2025-01-31/ibauyyl7yc2zt3nm.pdf?W3ZvbC4xNy5uby4xXzVdQXV0b25vbW91cyBWZWWhpY2xlcYBSZWd1bGF0aW9uIGluI-EJlaWppbmcucGRm> (accessed on 25 June 2026).
140. Hanna, M.J.; Kimmel, S.C. Current US federal policy framework for self-driving vehicles: Opportunities and challenges. *Computer* **2017**, *50*, 32–40. <https://doi.org/10.1109/MC.2017.4451211>.
141. Revision 3; Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles. Publisher: UNECE: Geneva, Switzerland, 2017. Available online: <https://unece.org/trans/main/wp29/wp29regs> (accessed on 9 July 2026).
142. Roberts, A.; Marksteiner, S.; Soyuturk, M.; Yaman, B.; Yang, Y. A global survey of standardization and industry practices of automotive cybersecurity validation and verification testing processes and tools. *SAE Int. J. Connect. Autom. Veh.* **2024**, *7*, 199–213. <https://doi.org/10.4271/12-07-02-0013>.
143. Pande, D.; Taihagh, A. Navigating the governance challenges of disruptive technologies: Insights from regulation of autonomous systems in Singapore. *J. Econ. Policy Reform* **2023**, *26*, 298–319. <https://doi.org/10.1080/17487870.2023.2197599>.
144. Tan, S.Y.; Taihagh, A. Adaptive governance of autonomous vehicles: Accelerating the adoption of disruptive technologies in Singapore. *Gov. Inf. Q.* **2021**, *38*, 101546. <https://doi.org/10.1016/j.giq.2020.101546>.
145. Li, S. Research on legislation issues of autonomous vehicles. *Adm. Law. Rev.* **2019**, *2*, 104–113. (In Chinese)
146. Li, R. Legal regulation of cybersecurity for autonomous vehicles. *Adm. Reform* **2019**, *10*, 43–49. (In Chinese) <https://doi.org/10.14150/j.cnki.1674-7453.2019.10.002>
147. Centenaro, M.; Berlato, S.; Carbone, R.; Burzio, G.; Cordella, G.F.; Ranise, S.; Riggio, R. Security considerations on 5G-enabled back-situation awareness for CCAM. In *Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF)*; IEEE: New York, NY, USA, 2020; pp. 245–250. <https://doi.org/10.1109/5GWF49715.2020.9221064>.
148. Martínez-Buelvas, L.; Rakotonirainy, A.; Grant-Smith, D.; Oviedo-Trespalcacios, O. Policy considerations for the safe and equitable integration of connected and automated vehicles. *Case Stud. Transp. Policy* **2025**, *22*, 101631. <https://doi.org/10.1016/j.cstp.2025.101631>.
149. Khan, S.K.; Shiwakoti, N.; Stasinopoulos, P.; Warren, M. Cybersecurity regulatory challenges for connected and automated vehicles—State-of-the-art and future directions. *Transp. Policy* **2023**, *143*, 58–71. <https://doi.org/10.1016/j.tranpol.2023.09.001>.

150. Kong, X.; Braunl, T.; Fahmi, M.; Wang, Y. A superalignment framework in autonomous driving with large language models. In Proceedings of the 2024 IEEE Intelligent Vehicles Symposium (IV), Jeju Island, Republic of Korea, 2–5 June 2024; pp. 1715–1720. <https://doi.org/10.1109/IV55156.2024.10588403>.
151. Acheampong, R.A.; Legacy, C.; Kingston, R.; Stone, J. Imagining urban mobility futures in the era of autonomous vehicles—Insights from participatory visioning and multi-criteria appraisal in the UK and Australia. *Transp. Policy* **2023**, *136*, 193–208. <https://doi.org/10.1016/j.tranpol.2023.03.020>.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.