JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 4, ISSUE 10
MONTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

ARTIFICIAL INTELLIGENCE AND AUTONOMOUS VEHICLES: RETHINKING LEGAL SUBJECTIVITY IN THE DIGITAL ERA

Nuriddin Khudoyberdiev
LL.M., Penn State Law, The Pennsylvania State University, USA; LL.M. and LL.B., Tashkent State University of Law, Uzbekistan.
n.khudoyberdiev.law@gmail.com

Abstract

This article offers an expanded legal-theoretical and comparative examination of the status of artificial intelligence (AI) systems and autonomous vehicles (AVs) under contemporary law. Building on prior work in cyber law and civil-law theory, it argues that neither full personhood nor the classical object-of-property paradigm is, on its own, adequate to govern the conduct of increasingly autonomous machines. Instead, the article proposes a layered framework in which (i) AVs remain objects of property subject to a special legal regime grounded in product liability, strict liability, and mandatory insurance, and (ii) a narrowly tailored, functional construct of "electronic person" operates exclusively as a liability-channeling device for high-risk autonomous systems, anchored by a compulsory compensation fund. The article surveys the legal responses of the European Union (including the 2024 AI Act and the revised Product Liability Directive), the United States, the United Kingdom, Germany, France, Japan, the Republic of Korea, the People's Republic of China, Singapore and the United Arab Emirates, identifying convergent design principles. It then maps these principles onto the existing legal framework of the Republic of Uzbekistan — in particular the Civil Code, the Laws "On Road Traffic Safety," "On Automobile Transport," "On Personal Data," "On Electronic Document Circulation," and "On Insurance Activities," together with the 2024 Strategy on AI Development — and proposes concrete legislative, regulatory and institutional reforms. Methodologically, the study combines comparative-legal analysis, historical-evolutionary tracing of legal personality, doctrinal analysis of civil liability, and a risk-allocation model drawn from law-and-economics scholarship.

Keywords: artificial intelligence; autonomous vehicles; legal personality; electronic person; civil liability; product liability; strict liability; risk-chain doctrine; insurance; EU AI Act; Uzbekistan; digital era.

1. Introduction

The accelerating deployment of artificial intelligence and increasingly autonomous machines is no longer a futurist projection — it is an ongoing transformation of economic, social, and legal life. Industry forecasts repeatedly cited in policy literature estimate that highly automated and fully autonomous vehicles will, by the mid-2030s, account for a substantial share of the global automotive market, with some scenarios placing that share at around one quarter of new sales [1]. Whatever the precise figures, the direction of travel is clear: a non-trivial fraction of road traffic, freight, urban logistics and last-mile delivery will be operated by systems whose moment-to-moment driving decisions are not made by a human.

That technological shift is, at its heart, a legal problem. Modern private law is built on the assumption that conduct — driving, contracting, harming another person — is the conduct of a human being or of a juridical person staffed by human beings. As Antonios observes, autonomous vehicles are "not only a revolution in transport but a paradigm shift for legal systems themselves" [2]. When a vehicle moves through traffic, decides whether to brake,

swerve, or accelerate, and ultimately collides with another road user, the traditional toolbox of fault, foreseeability and driver duty no longer maps cleanly onto the facts. The most consequential question that this raises is also the simplest to state: who, in law, is responsible?

Although the question is simple to pose, it sits at the intersection of several deep doctrinal debates. The first concerns legal personality itself — whether the category of "person" in law should remain restricted to natural persons and the corporate forms that we have inherited from the nineteenth century, or whether it should expand to encompass artificial agents capable of autonomous action [3]. The second concerns the architecture of civil liability — whether the appropriate regime is tortious fault, strict product liability, no-fault compensation, mandatory insurance, or some combination [4]. The third concerns risk allocation across the value chain — from chip designers and software vendors to vehicle manufacturers, fleet operators and end users [5]. A fourth, less often acknowledged, concerns the moral and political legitimacy of letting algorithms make decisions that have life-or-death consequences for third parties [6].

In most jurisdictions, including the Republic of Uzbekistan, the legal status of AI systems and autonomous vehicles is not yet expressly settled by statute. As Bryson, Diamantis and Grant have argued, the question of legal personality is "one of the most important and difficult legal questions in the field of artificial intelligence" [3]. The uncertainty is particularly acute in the AV context, where serious physical harm to third parties is foreseeable and where the responsibility chain is composed of actors with very different bargaining power and access to information.

This article therefore pursues three connected aims. First, it reconstructs the conceptual foundations of legal personality in order to ask, with appropriate scepticism, whether "electronic personhood" is a genuine doctrinal innovation or merely a re-labelling of long-standing techniques of legal fiction. Second, it offers a comparative survey of the legislative and case-law responses of jurisdictions that have moved earliest — the European Union, the United States, the United Kingdom, Germany, France, Japan, the Republic of Korea, the People's Republic of China, Singapore and the United Arab Emirates — in order to identify the design principles that are converging across systems. Third, it brings these findings to bear on the law of the Republic of Uzbekistan, identifying gaps in the Civil Code, the Laws on Road Traffic Safety, on Personal Data, and on Insurance Activities, and proposing a set of legislative and institutional reforms calibrated to Uzbekistan's legal tradition and its current digital-development strategy. Pagallo's observation is the point of departure: although jurisdictions disagree on the precise solution, every legal system that takes the technology seriously eventually faces the same need for detailed and deliberate regulatory design [4].

2. Theoretical foundations: legal personality reconsidered

2.1. From natural persons to juridical fictions

The history of legal personality is a history of expansion. Classical Roman law, although it knew the dominant figure of the paterfamilias, also recognised collectivities — municipia, collegia — capable of holding rights distinct from those of their members. Medieval canon law refined the technique through the notion of the persona ficta, by which the Church and ecclesiastical institutions were treated as bearers of rights and duties [11]. Modern corporate law, from the nineteenth century onwards, transformed this artificial-person device into the central engine of capitalist enterprise: limited liability, perpetual succession, and the capacity to sue and be sued were grafted onto entities that had no body, no will, and no soul, but were nonetheless treated by the law as persons.

Solaiman has shown that legal personality is, historically, a malleable category that has been extended in response to social and economic pressure: to corporations, to ships, to temples in some jurisdictions, to rivers and ecosystems in others, and even, in modest experimental forms, to non-human animals such as great apes [11]. The lesson is methodological rather than substantive. Legal personality is not a metaphysical discovery; it is a regulatory technique. The question is therefore never "does this entity really have rights?" but "what consequences follow if we treat it as a bearer of rights and duties for the limited purposes of this body of law?"

2.2. The functional account of legal personality

Building on this insight, scholars in the law-and-technology tradition have developed a functional account of legal personality. On the functional view, an entity is a legal person to the extent that, and only to the extent that, recognising it as such serves identifiable regulatory goals: efficient risk allocation, the protection of victims, the preservation of incentives to develop socially valuable technologies, and the channelling of liability towards the actor best placed to bear it [4][5]. The functional account thereby disconnects legal personality from any underlying claim about consciousness, agency, or moral status.

Applied to AI systems and autonomous vehicles, the functional account suggests two important conclusions. First, granting full legal personality to an AI system — a status comparable to that of a natural or corporate person — is neither necessary nor, in the current state of the technology, desirable. Modern AI systems lack genuine self-awareness, do not have assets of their own from which to satisfy judgments, and cannot meaningfully participate in litigation. Second, however, the functional account does not foreclose narrower, purpose-specific recognitions. A construct of "electronic person" may be defensible if, and only if, it serves a clearly defined regulatory function — most plausibly, the channeling of strict liability and the operation of a mandatory compensation fund.

2.3. The European Parliament's 2017 proposal and its critics

The most prominent doctrinal proposal for electronic personhood emerged from the European Parliament's 2017 Resolution on Civil Law Rules on Robotics, which suggested the creation of "specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause" [10]. The proposal triggered immediate scholarly resistance. In an influential open letter, over 150 European AI and robotics experts argued that electronic personhood would be technically wrong (because it overstates the autonomy of current systems), ethically problematic (because it could be used to dilute the responsibilities of designers and operators), and legally redundant (because existing doctrines of product liability and vicarious liability already provide adequate tools).

These criticisms are largely sound, and the European Union's subsequent regulatory choices reflect them. Neither the 2024 Artificial Intelligence Act nor the 2024 revision of the Product Liability Directive adopt electronic personhood. Instead, both instruments operate within the inherited categories of obligations on "providers," "deployers" and "importers," and tighten the rules of product liability so that the burden of opaque algorithmic decision-making does not fall on victims. Nevertheless, the European Parliament's proposal performed a useful diagnostic function: it forced the question of where, in the value chain of an autonomous system, the locus of legal responsibility ought to lie. That question remains the core of this article.

3. Concepts and terminology

Terminological precision is a precondition for sound legal design. Three distinctions matter for what follows.

3.1. Artificial intelligence as a regulatory concept

The international standard ISO/IEC 22989:2022 defines an AI system as an engineered system that generates outputs such as predictions, content, recommendations or decisions for a given set of human-defined objectives. The European Union's AI Act largely tracks this definition while emphasising the system's ability to infer, from the input it receives, how to generate outputs that can influence physical or virtual environments. For legal purposes the key features are three: (i) the system is engineered (not a natural process); (ii) it produces outputs that affect the world; and (iii) it does so with at least some degree of autonomy from real-time human input.

3.2. Levels of vehicle automation

The SAE J3016 taxonomy distinguishes six levels of driving automation, from Level 0 (no automation) to Level 5 (full automation under all conditions). Levels 0–2 retain the human driver as the legally responsible operator. At Level 3 (conditional automation), the system performs the dynamic driving task under defined conditions but expects the human to resume control on request. At Levels 4 and 5, no human intervention is required within the operational design domain. Most current regulatory debate concerns Levels 3 and 4, because those are the regimes in which a vehicle is genuinely driving itself, and yet the legal infrastructure (driver's licences, traffic offences, motor-insurance third-party regimes) has been built around a human driver.

3.3. "Electronic person" as a functional construct

In what follows, "electronic person" denotes a narrowly defined and purpose-limited legal construct attached to a registered high-risk autonomous system. It is not a claim that the system is conscious, sentient, or deserving of moral standing. The construct serves three discrete functions: (i) to identify, in the public registry, the autonomous system whose operation gives rise to harm; (ii) to channel strict liability to a compulsory compensation fund associated with that system; and (iii) to support the operation of mandatory insurance and the recovery actions that follow indemnification. On this view, electronic personality is closer in nature to the registration of a ship or aircraft than to the legal personality of a human or a corporation.

4. Comparative analysis of international approaches

Across the major jurisdictions that have legislated in this area, four design principles recur with notable regularity: (i) regulation by risk tier, rather than by technology type; (ii) clear allocation of responsibility to identifiable actors in the value chain; (iii) mandatory insurance and victim-protection mechanisms; and (iv) transparency, traceability and post-market monitoring. The following subsections briefly survey the most influential national and supranational responses.

4.1. European Union

The European Union has assembled, over the past five years, the most comprehensive regulatory architecture for AI in any jurisdiction. The cornerstone is Regulation (EU) 2024/1689 — the Artificial Intelligence Act — which classifies AI systems by risk (prohibited, high-risk, limited-risk and minimal-risk) and imposes graduated obligations on providers and deployers. AI systems used as safety components of road vehicles fall within the high-risk category, triggering obligations on data governance, risk management, technical documentation, human oversight, accuracy, robustness and cybersecurity.

On the civil-liability side, the 2024 revision of the Product Liability Directive (Directive (EU) 2024/2853) extends strict producer liability to software (including AI), introduces a rebuttable presumption of defectiveness where the claimant faces evidential difficulties because of technical complexity, and adopts disclosure obligations designed to reduce the informational asymmetry between victims and producers. The European Parliament's earlier flirtation with electronic personhood has been quietly abandoned in favour of a thoroughgoing strengthening of the existing product-liability regime.

4.2. United States

The United States has, characteristically, pursued a layered regulatory approach. At the federal level, the National Highway Traffic Safety Administration regulates automated driving systems through the Federal Motor Vehicle Safety Standards and an evolving series of policy documents (Automated Vehicles Comprehensive Plan and successor instruments). States vary considerably: California, Arizona, Nevada and Florida have enacted permissive frameworks that authorise driverless testing and deployment, while other states retain more restrictive rules.

On civil liability, the U.S. position is shaped by the law of products liability under the Restatement (Third) of Torts: Products Liability, supplemented by state tort law on negligence and strict liability. A 2023 federal compilation cited by Litman recorded more than 310 reported incidents involving automated driving systems, an increase of approximately 13.5% over the preceding year [12]. As Abbott has argued, the persistence of a fault-based regime, designed for human drivers, generates systematic mismatches when applied to machines that may, in absolute terms, be safer than human drivers, but whose errors are different in kind [13].

4.3. United Kingdom

The United Kingdom has gone further than most jurisdictions in adapting motor-insurance law to autonomous driving. The Automated and Electric Vehicles Act 2018 creates a single insurer-pays model: where an accident is caused by an automated vehicle driving itself, the insurer of the vehicle is directly liable to the victim, who is thereby spared the need to identify a particular negligent actor. The insurer is then subrogated to any claims against manufacturers or software providers. The Automated Vehicles Act 2024 builds on this foundation, creating an authorisation regime for AV deployment, statutory safety standards and a regulator with significant investigatory powers. The British model is widely regarded as the most coherent integration of motor insurance and product liability yet attempted.

4.4. Germany

Germany was, in 2017, the first major jurisdiction to legislate specifically on conditionally automated driving, through amendments to the Road Traffic Act (Straßenverkehrsgesetz). In 2021, a further amendment authorised Level 4 driverless operation within defined operational design domains and introduced the role of the "technical supervisor." Liability remains anchored in the long-standing rule of strict keeper's liability under § 7 StVG, complemented by product-liability claims against manufacturers. Mandatory event-data recording is a centrepiece of the regime, enabling ex post reconstruction of the vehicle's decisions.

4.5. France

France has chosen a path closer to the German model, with successive amendments to the Code de la route authorising automated driving and a 2021 ordinance integrating Level 3 and Level 4 vehicles into the road-traffic and insurance regime. Victim-protection rules under the Loi Badinter (1985), which already establish a near-absolute right to compensation for victims of road traffic accidents involving motor vehicles, dovetail well with autonomous driving and have not required structural revision.

4.6. Japan

Japan amended its Road Traffic Act and Road Transport Vehicle Act in 2019 and again in 2022 to permit Level 3 and, within carefully delimited zones, Level 4 driverless operation. Civil liability for traffic accidents continues to follow the Automobile Liability Security Act, which imposes a strict liability rule on the keeper of the vehicle and compels third-party insurance. Product liability operates as a second layer through the Product Liability Act of 1994. Japanese policy explicitly favours a "keeper-pays-first, recover-later" structure that is functionally similar to the British single-insurer model.

4.7. Republic of Korea

The Republic of Korea has been a pioneer in dedicated AI and robotics legislation, beginning with the Intelligent Robots Development and Distribution Promotion Act of 2008. The Act on the Promotion of the AI Industry and Framework for Establishing Trustworthy AI, debated and progressively adopted from 2023 onwards, supplies a framework for risk-based regulation. For autonomous vehicles, the Act on the Promotion of and Support for Commercialization of Autonomous Vehicles establishes test districts and authorisation procedures.

4.8. People's Republic of China

China combines local experimentation with central guidance. Major cities — Beijing, Shanghai, Shenzhen, Guangzhou — have adopted local regulations authorising the testing and, increasingly, commercial deployment of automated driving services within defined zones. At the national level, the Interim Measures for the Management of Generative AI Services (2023) and earlier algorithmic-recommendation rules establish ex ante registration and transparency obligations. The Civil Code (2020) provides the underlying liability framework, supplemented by the Road Traffic Safety Law.

4.9. Singapore

Singapore's Road Traffic (Autonomous Motor Vehicles) Rules and the broader sandbox regime administered by the Land Transport Authority have made the city-state a leading site for AV testing. The 2020 Model AI Governance Framework, although non-binding, has been highly influential as a template for risk-based AI governance in Southeast Asia.

4.10. United Arab Emirates and other jurisdictions

The United Arab Emirates has pursued an aggressive policy of attracting AV deployment, with dedicated regulations in Dubai and Abu Dhabi. According to several recent surveys, more than forty-five jurisdictions worldwide had, by 2023, adopted specific legal instruments addressing AI or autonomous vehicles [13]. The pace of legislative activity is itself a relevant fact: between 2015 and 2022, the global stock of AI-related legal instruments grew several-fold.

4.11. Convergent design principles

Despite differences of doctrine, the major jurisdictions are converging on a recognisable pattern. The first convergent principle is risk-based regulation: obligations scale with the seriousness of potential harm and the autonomy of the system. The second is value-chain responsibility: the law identifies multiple actors — provider, deployer, importer, keeper, user — and assigns them differentiated duties. The third is victim primacy: the victim should not bear the burden of identifying the technically responsible actor. The fourth is traceability: event-data recording, audit logs and post-market monitoring are mandatory. The fifth is the integration of insurance: mandatory third-party motor insurance remains the front line of victim protection, with product-liability and recovery actions operating in the background.

5. Civil liability for autonomous vehicles: a structured framework

The legal architecture for harm caused by an AV can usefully be analysed in three layers: the front layer of victim compensation, the middle layer of inter-defendant allocation, and the back layer of preventive incentives. This section examines each, before turning to the role that a properly constrained "electronic person" construct can play.

5.1. The victim-compensation layer

The function of the front layer is to ensure that a victim of an AV-related accident is compensated promptly, fully and without having to litigate the internal workings of the vehicle. Three regulatory techniques dominate. The first is strict keeper's liability, in the German tradition, under which the registered keeper of the vehicle answers for harm caused by it regardless of fault, backed by compulsory third-party insurance. The second is the British single-insurer model under the Automated and Electric Vehicles Act 2018, in which the motor insurer pays the victim directly and then exercises rights of recovery. The third is no-fault compensation, exemplified by New Zealand's Accident Compensation Corporation and certain Canadian provinces, in which a public or quasi-public fund compensates victims regardless of cause and without tort litigation.

Each of these techniques shares the same victim-protective logic: it severs, at the front of the system, the question of who pays from the question of who, ultimately, ought to pay. From the victim's perspective, the inscrutability of the AV's decision-making is rendered legally irrelevant.

5.2. The inter-defendant allocation layer

Once the victim has been compensated, the law must determine how the loss is allocated among the actors in the value chain: the vehicle manufacturer, the supplier of the automated driving system, the supplier of components and sensors, the operator of any back-office or cloud infrastructure, the registered keeper, and — where applicable — the user. The dominant doctrinal tool here is product liability, supplemented by negligence claims, contractual indemnities and recourse against component suppliers.

The most useful conceptual device for analysing this allocation is what may be called the "risk-chain" doctrine. The risk chain identifies, for each foreseeable category of harm, the actor best placed (i) to detect the risk, (ii) to prevent or mitigate it at lowest cost, and (iii) to bear residual losses through insurance or self-insurance. The doctrine does not displace product liability or negligence; rather, it provides an analytical scaffold for applying them coherently across a complex value chain. In the AV context, the risk chain typically locates primary responsibility on the manufacturer of the integrated automated driving system, with secondary responsibility on component suppliers and the operator of any cloud-side infrastructure that participates in the driving task.

5.3. The preventive-incentive layer

The third layer ensures that the cost of harm is, over time, internalised by the actors whose design choices produced it, thereby creating incentives for safer engineering. Mandatory event-data recording, post-market surveillance, transparency obligations and regulator-administered penalties are the key instruments. The EU AI Act, the UK Automated Vehicles Act 2024 and the German StVG amendments converge in requiring data recording sufficient to permit ex post reconstruction of the AV's behaviour.

5.4. The role of "electronic person" as a liability-channeling device

Against this background, the contribution of an "electronic person" construct should be modest and functional. It should not be a vehicle for relieving manufacturers and operators of

their substantive obligations. It should rather operate as a registry-anchored identifier of a high-risk autonomous system, to which a compulsory compensation fund is attached. The fund is financed by the value-chain actors in proportion to their risk-creating share. Victims may proceed against the fund without litigating the internal allocation; the fund then exercises rights of recovery against the actors in accordance with the inter-defendant allocation layer.

This construct — which may be called an "electronic person fund", following Abbott's suggestion [13] — has three advantages. It preserves the victim-protective virtues of strict liability without overburdening any single actor. It creates a clear focal point for insurance, regulatory supervision and recovery. And it does not require any premature recognition of moral or constitutional status for AI systems.

6. Insurance models for autonomous vehicles

Insurance is not merely an adjunct to AV liability law; it is its operational backbone. The three principal models in use are the traditional motor-insurance model, the integrated single-insurer model, and the compensation-fund model.

Under the traditional model, applicable in most jurisdictions today, the registered keeper insures against third-party liability for losses caused by the vehicle. The model performs well when a human driver is unambiguously the cause of harm, but it strains when responsibility lies with the manufacturer's software.

Under the integrated single-insurer model, championed by the United Kingdom, the same insurer covers both human-driver fault and harm caused by the vehicle driving itself. Subrogation against manufacturers and software providers operates in the background. The model is widely regarded as the most efficient and victim-friendly of the three, though it depends on a mature, well-capitalised insurance market.

Under the compensation-fund model, harm is paid out of a dedicated fund financed by mandatory contributions from value-chain actors. Variants of this model have been proposed in academic literature [13] and are increasingly attractive in jurisdictions where the insurance market is still developing. The model dovetails naturally with the "electronic person fund" construct described above.

7. Data protection and privacy in the operation of autonomous vehicles

Modern AVs are also data-processing machines on a remarkable scale. A single mid-range autonomous test vehicle generates hundreds of gigabytes of sensor and telemetry data per hour. Some of this data is necessary for the dynamic driving task; some supports product improvement; some has substantial commercial value beyond the driving function itself. Several legal regimes apply concurrently: general data-protection law (the GDPR in the EU, the Law of the Republic of Uzbekistan on Personal Data, similar instruments elsewhere), sector-specific road-safety and event-data rules, and intellectual-property and trade-secret rules over the algorithms themselves.

Three issues are especially pressing. The first is the legal basis for processing data about persons other than the vehicle's occupants — pedestrians, drivers of other vehicles, bystanders — whose images and behaviours are continuously captured by AV sensors. The second is the relationship between data-protection rules and accident-investigation rules: in particular, the conditions under which event-data may be disclosed to regulators, insurers, courts and victims. The third is cross-border data flows: AV fleets typically transmit data to manufacturer cloud

infrastructure located outside the country of operation, raising classical issues of jurisdiction and adequacy.

8. Algorithmic decision-making and ethical pre-commitments

The image of an AV being forced to "choose" between two harmful outcomes — the so-called trolley-problem scenario — is regularly used to dramatise the moral complexity of automated driving. As a description of how AVs actually operate, it is misleading: AVs are generally programmed to maximise predictable safety margins, not to optimise over discrete moral dilemmas at the moment of collision. But the underlying point survives the simplification. AV designers must, ex ante, make choices about how the vehicle will behave in foreseeable conflicts between different categories of harm; those choices have moral content; and they cannot be left entirely to the engineering judgment of private firms.

The German Ethics Commission on Automated and Connected Driving (2017) articulated a set of principles — the primacy of human life over property, the impermissibility of discriminating among potential victims on grounds such as age, sex, or physical characteristics, and the priority of avoiding harm to uninvolved third parties — that have since become an international reference point. The EU AI Act and various national frameworks broadly converge on similar substantive constraints. The legal question, in domestic terms, is how to translate these principles into binding norms: through statutory enactment, through regulator-issued technical standards, or through judicial review of manufacturers' design choices in the context of liability proceedings.

9. The legal framework of the Republic of Uzbekistan

9.1. The current state of regulation

Uzbek law does not yet contain a dedicated statute on artificial intelligence or on autonomous vehicles. The relevant legal infrastructure must therefore be assembled from a number of general instruments. The Civil Code of the Republic of Uzbekistan supplies the general law of obligations, including the rules on tortious liability and on liability for harm caused by sources of heightened danger (Articles 985 et seq.), under which a motor vehicle qualifies as such a source. The Law "On Road Traffic Safety" and the Law "On Automobile Transport" establish the regulatory framework for vehicles and their use. The Law "On Personal Data" (2019, as amended) governs the processing of personal data, including data generated by sensors. The Law "On Electronic Document Circulation" supplies a partial basis for the recognition of electronic acts. The Law "On Insurance Activities" and the Law "On Compulsory Insurance of Civil Liability of Vehicle Owners" organise the motor-insurance market.

At the policy level, the Republic of Uzbekistan has, in recent years, taken substantial steps to articulate its digital strategy. The Decree of the President of the Republic of Uzbekistan on the further development of artificial intelligence (2024) sets the strategic direction for AI development through 2030, including the goals of building a national AI research and development infrastructure, training qualified specialists, and adopting modern regulatory standards. The "Digital Uzbekistan 2030" strategy provides the wider context.

9.2. Gaps and uncertainties

Despite these foundations, four significant gaps remain. First, the existing rules on "sources of heightened danger" in the Civil Code, although extending naturally to autonomous vehicles, do not distinguish among levels of automation, do not address the role of software providers, and

do not provide for compulsory event-data recording. Second, the Law on Compulsory Insurance of Civil Liability of Vehicle Owners is structured around the figure of the human driver and does not accommodate the case in which the vehicle is itself driving. Third, the Law on Personal Data does not yet provide tailored rules for the high-volume, high-resolution data flows generated by AV sensors, including the rights of bystanders. Fourth, no national authority is currently designated as the regulator with primary responsibility for AV authorisation, post-market surveillance and accident investigation.

10. Proposals for legislative and institutional reform in Uzbekistan

Drawing on the comparative analysis and on the theoretical framework developed above, the article proposes the following package of reforms, calibrated to the institutional capacities of the Republic of Uzbekistan and respectful of its legal tradition.

1. Adopt a framework Law on Artificial Intelligence Systems modelled on the risk-based architecture of the EU AI Act, but adjusted to local conditions. The Law should define AI systems, classify them by risk, set obligations for providers and deployers, and designate a competent regulator. The principles of technological neutrality, safety primacy and clarity of liability should be expressly stated.

2. Amend the Civil Code to introduce a narrowly defined construct of "electronic person" operating as a liability-channeling device for registered high-risk autonomous systems. The amendment should expressly state that the construct does not confer constitutional or fundamental rights and is functional in nature.

3. Establish, by statute, an Electronic Person Compensation Fund financed by mandatory contributions from manufacturers, software providers and operators of high-risk autonomous systems, with a public scheme of contribution rates calibrated to risk-creating share. Victims should have a direct right of action against the fund; the fund should have subrogated rights of recovery against the value-chain actors.

4. Amend the Law on Road Traffic Safety to authorise, within defined operational design domains and under regulatory authorisation, the operation of Level 3 and Level 4 autonomous vehicles, and to integrate event-data recording obligations.

5. Amend the Law on Compulsory Insurance of Civil Liability of Vehicle Owners to introduce a single-insurer model on the British template: the insurer of the vehicle is directly liable to the victim where the vehicle is driving itself, with rights of subrogation against manufacturers and software providers.

6. Amend the Law on Personal Data to introduce specific rules for the processing of data generated by autonomous vehicles, including rights of pedestrians and other non-occupants, transparency obligations, and the conditions for cross-border transfer of telemetry data.

7. Designate a competent regulatory authority — either an existing body with expanded powers or a new agency under the Cabinet of Ministers — with responsibility for authorising AV deployment, monitoring post-market performance, and investigating accidents. The authority should be empowered to require disclosure of relevant algorithmic and event-data information.

8. Implement, by reference, the principal international standards in the area: ISO/IEC 22989 (AI concepts and terminology), ISO/IEC 23894 (AI risk management), ISO/PAS 21448 (Safety of the Intended Functionality for road vehicles), and ISO 26262 (Functional safety). National adoption of these standards aligns Uzbek practice with international best practice and reduces the compliance burden on cross-border operators.

9. Invest in legal-technical capacity: judicial training programmes, prosecutorial guidance, and the establishment within the Tashkent State University of Law and other institutions of dedicated research centres on AI and law, drawing on existing experience in cyber law.

11. Conclusion

This article has argued for an approach to the legal status of artificial intelligence systems, and of autonomous vehicles in particular, that resists both the temptation of full electronic personhood and the inertia of treating AVs as ordinary objects of property. AI systems and AVs occupy a distinctive position in modern law: they are not persons, but they are not, either, the inert mechanical instruments around which classical motor-vehicle law was built. The legal response should be correspondingly tailored. A special legal regime for AVs — grounded in product liability, strict keeper's liability, mandatory insurance, and a registered compensation fund associated with each high-risk autonomous system — captures the regulatory benefits of personhood-like constructs without their conceptual costs.

Three propositions support the framework. First, the legal nature of AI and AVs is dual: they remain objects of property subject to a special legal regime, while at the same time being eligible for a narrow, functional "electronic person" construct used solely to channel liability. Second, the legal problems they generate — allocation of liability, insurance, data protection, ethical decision-making — form a coherent regulatory cluster that calls for an integrated legislative response, not a series of ad hoc fixes. Third, in the legal framework of the Republic of Uzbekistan, this response should be built incrementally, guided by the principles of technological neutrality, safety primacy, clarity of liability, and faithful integration of international standards into domestic law.

Beyond Uzbekistan, the article's analytical framework — victim layer, allocation layer, prevention layer, and a functional electronic-person construct anchored in a compensation fund — may be useful for any legal system grappling with the same questions. The deeper claim is methodological. Legal personality has always been a regulatory technique rather than a metaphysical category; the appropriate test for any candidate extension is not whether the entity in question is "really" a person, but whether recognising it as one for specific, bounded purposes advances identifiable regulatory goals. Measured against that test, the cautious electronic-person framework defended here is justified; broader claims to AI personhood are, for the time being, not.

References

1. Mosquet X., Andersen M., Arora A. Revolution in the Driver's Seat: The Road to Autonomous Vehicles. Boston, Boston Consulting Group, 2020, p. 45.

2. Antonios E. Autonomous Vehicles: Regulatory Challenges and the Response from Germany and UK. Mitchell Hamline Law Review, 2020, vol. 46, no. 5, pp. 1105–1121.

3. Bryson J.J., Diamantis M.E., Grant T.D. Of, for, and by the people: the legal lacuna of synthetic persons. Artificial Intelligence and Law, 2017, vol. 25, no. 3, pp. 273–291.

4. Pagallo U. The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht, Springer Netherlands, 2013.

5. Calo R. Robotics and the Lessons of Cyberlaw. California Law Review, 2015, vol. 103, no. 3, pp. 513–563.

6. Teubner G. Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law. Journal of Law and Society, 2006, vol. 33, no. 4, pp. 497–521.

7. Turner J. Robot Rules: Regulating Artificial Intelligence. London, Palgrave Macmillan, 2019.

8. Scherer M.U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. Harvard Journal of Law and Technology, 2016, vol. 29, no. 2, pp. 353–400.

9. Lemley M.A., Casey B. Remedies for Robots. University of Chicago Law Review, 2019, vol. 86, no. 5, pp. 1311–1396.

10. European Parliament. Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Brussels, 2017.

11. Solaiman S.M. Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy. Artificial Intelligence and Law, 2017, vol. 25, no. 2, pp. 155–179.

12. Litman T. Autonomous Vehicle Implementation Predictions: Implications for Transport Planning. Victoria, Victoria Transport Policy Institute, 2023.

13. Abbott R. The Reasonable Computer: Disrupting the Paradigm of Tort Liability. George Washington Law Review, 2018, vol. 86, no. 1, pp. 1–45.

14. Hallevy G. The Criminal Liability of Artificial Intelligence Entities — from Science Fiction to Legal Social Control. Akron Intellectual Property Journal, 2010, vol. 4, no. 2, pp. 171–201.

15. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series, 12 July 2024.

16. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. Official Journal of the European Union, L series, 18 November 2024.

17. Automated and Electric Vehicles Act 2018 (UK), c. 18.

18. Automated Vehicles Act 2024 (UK), c. 10.

19. Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes — Gesetz zum autonomen Fahren (Germany), Bundesgesetzblatt I, 12 July 2021.

20. Inoyatov N.Kh. Artificial Intelligence and Autonomous Vehicles: Issues of Legal Subjectivity in the Digital Era. Yurisprudensiya, 2025, vol. 5, no. 2, pp. 38–46. DOI: 10.51788/tsul.jurisprudence.5.2./ECZK6798.

21. Civil Code of the Republic of Uzbekistan. Tashkent, Adolat publ., consolidated edition.

22. Law of the Republic of Uzbekistan No. ZRU-547 of 2 July 2019 on Personal Data (as amended).

23. Law of the Republic of Uzbekistan No. ZRU-741 of 23 February 2022 on Road Traffic Safety.

24. Decree of the President of the Republic of Uzbekistan on measures for the further development of artificial intelligence (2024).

25. ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology. International Organization for Standardization, Geneva, 2022.

26. ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management. International Organization for Standardization, Geneva, 2023.