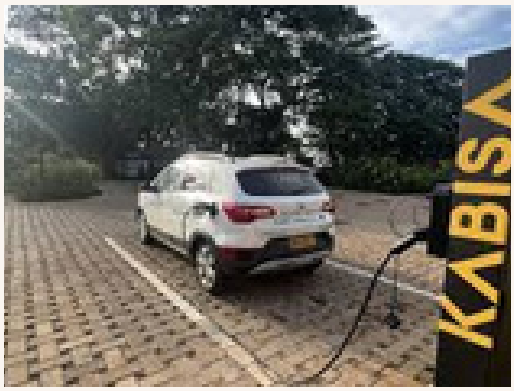
Regulating Autonomous Vehicles and Intelligent Mobility in Rwanda: Legal Foundations, Gaps, and the Path Forward



.Despite the existence of a national data protection framework, several legal uncertainties arise in the context of autonomous vehicle ecosystems. One major issue is identifying the data controller responsible for personal information generated by intelligent transportation systems, particularly where multiple entities, such as vehicle manufacturers, software developers, and cloud service providers, participate in data processing. Another challenge concerns obtaining meaningful consent for continuous geolocation monitoring, since autonomous vehicles often operate through constant data flow rather than discrete data collection events. Additionally, questions remain regarding the permissible duration of trip data storage and the legal treatment of information processed through cross-border cloud computing infrastructures.

To address these emerging challenges, Rwanda may consider developing sector-specific regulatory guidelines governing mobility data governance and artificial intelligence-driven transportation technologies. Such regulations could clarify operational responsibilities, establish retention standards for transportation-related data, and provide safeguards for international data transfers. Developing a specialized legal framework would strengthen privacy protection, promote public confidence in autonomous mobility innovation, and ensure that technological advancement occurs in harmony with fundamental data protection principles.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE RISKS

Autonomous vehicles operate as interconnected digital machines, which makes them particularly vulnerable to cybersecurity threats. Potential risks include remote system hacking, GPS signal spoofing, ransomware attacks targeting vehicle control systems, and sensor interference that may disrupt safe navigation. In Rwanda, cybersecurity protection is partly governed by the Law No. 60/2018 on Prevention and Punishment of Cybercrimes, which criminalizes unauthorized access and interference with computer systems. However, while the law provides general cybercrime protection, it does not yet contain detailed operational standards specifically tailored to autonomous vehicle technology, leaving a regulatory gap in emerging intelligent transportation security management

Given that transportation networks may be considered critical infrastructure; autonomous vehicle systems should ideally be subjected to stronger cybersecurity governance requirements. Regulatory authorities may need to introduce mandatory cybersecurity audits for autonomous mobility operators, enforce real-time incident reporting obligations, establish minimum encryption standards, and require continuous software security updates to counter evolving cyber threats. Without comprehensive cybersecurity regulation, autonomous vehicle ecosystems could expose public transport safety to catastrophic system failures, potentially resulting in large-scale accidents, financial losses, and public security risks. Therefore, proactive legal and technical safeguards are essential to ensure that innovation in autonomous mobility develops alongside robust cyber protection mechanisms.

Autonomous vehicles must be understood legally as a fundamental departure from the traditional assumption that a human being controls a motor vehicle. They are categorized into Levels 0-5 under the framework developed by the Society of Automotive Engineers (SAE). At Levels 0-2, the human driver remains primarily responsible, even where assistance systems exist. However, at Levels 3-5 particularly Levels 4 and 5, the vehicle can operate with little or no human intervention. At the highest level, a vehicle may function entirely without a steering wheel or pedals, meaning the human occupant is no longer "driving" in the conventional legal sense. This technological shift directly challenges long-standing legal definitions built around human agency. Traditional traffic law assumes that a natural person exercises judgment, perception, and control over a vehicle. Traffic offences such as dangerous driving, speeding, or failure to obey signals are framed as human acts. When a fully autonomous vehicle commits a violation, the immediate legal question becomes: who was driving? If the vehicle was operating through software, attributing the offence to a human actor becomes conceptually difficult. The legal system must then decide whether responsibility lies with the owner, the operator, or another party involved in the vehicle's design or deployment.

Finally, insurance law, which traditionally evaluates risk based on driver characteristics such as age and driving history, must also evolve. Autonomous systems transfer risk from human error to technological reliability, cybersecurity strength, and system maintenance. In a fully autonomous context, the "driver" may effectively be replaced by an algorithm that has no legal personality. Consequently, legal responsibility must be re-theorized—shifting from a purely fault-based, human-centered model to one that emphasizes risk allocation, product accountability, and system governance. Autonomous vehicles therefore represent not just a technological innovation, but a doctrinal transformation in the law of responsibility.

LIABILITY AND CIVIL RESPONSIBILITY

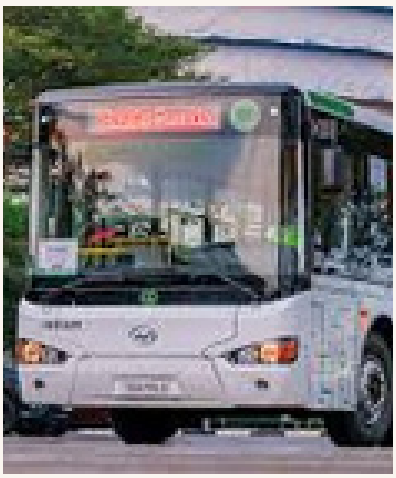
Under the general principles of civil liability applicable in Rwanda, a claimant must ordinarily establish four essential elements: the existence of a duty of care, breach of that duty, causation, and resulting damage. In traditional traffic accident cases, liability is usually attributed to the driver based on negligence. However, the introduction of autonomous vehicles challenges this framework because harm may occur without direct human misconduct. Instead, accidents involving autonomous systems may stem from technical or systemic failures such as defective software design, sensor malfunction, algorithmic errors, insufficient system maintenance, or inadequately trained data models. This development suggests that courts may gradually move from a driver-centered negligence approach toward a product-oriented liability analysis.

In situations where harm results from system defects rather than user behavior, manufacturers and developers may be held responsible under product liability principles. Comparative legal experience, particularly within the European Union, demonstrates that strict product liability can be imposed on producers regardless of fault when defective design or manufacturing causes injury. Adopting a similar approach in Rwanda could support legal certainty by establishing that entities involved in creating autonomous mobility technologies bear responsibility when system flaws directly cause harm. Such a framework could also encourage higher safety standards in the development and deployment of artificial intelligence-driven transportation systems.

To address emerging legal uncertainties, Rwanda may consider enacting comprehensive legislation establishing clear rules on joint and several liabilities for autonomous vehicle-related harm. Such reform would enhance consumer protection, support technological innovation, and provide predictability for investors and industry participants. By defining responsibility across the autonomous mobility value chain, the law would ensure that victims receive adequate compensation while maintaining balanced risk allocation among technology developers, service providers, and users.

DATA PROTECTION AND PRIVACY IMPLICATIONS

Autonomous vehicles rely heavily on continuous data collection and processing to function effectively. These systems gather various forms of information, including geolocation signals, traffic movement patterns, environmental readings, and in some cases biometric or facial recognition inputs. In Rwanda, data protection is governed by Law No. 58/2021 Relating to the Protection of Personal Data and Privacy, which requires that personal data be processed lawfully, collected for clearly defined purposes, limited to what is necessary, and protected through appropriate security measures. These general protections provide an important foundation for regulating emerging technologies such as autonomous mobility systems.



Despite the existence of a national data protection framework, several legal uncertainties arise in the context of autonomous vehicle ecosystems. One major issue is identifying the data controller responsible for personal information generated by intelligent transportation systems, particularly where multiple entities, such as vehicle manufacturers, software developers, and cloud service providers, participate in data processing. Another challenge concerns obtaining meaningful consent for continuous geolocation monitoring, since autonomous vehicles often operate through constant data flow rather than discrete data collection events. Additionally, questions remain regarding the permissible duration of trip data storage and the legal treatment of information processed through cross-border cloud computing infrastructures.

To address these emerging challenges, Rwanda may consider developing sector-specific regulatory guidelines governing mobility data governance and artificial intelligence-driven transportation technologies. Such regulations could clarify operational responsibilities, establish retention standards for transportation-related data, and provide safeguards for international data transfers. Developing a specialized legal framework would strengthen privacy protection, promote public confidence in autonomous mobility innovation, and ensure that technological advancement occurs in harmony with fundamental data protection principles.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE RISKS

Autonomous vehicles operate as interconnected digital machines, which makes them particularly vulnerable to cybersecurity threats. Potential risks include remote system hacking, GPS signal spoofing, ransomware attacks targeting vehicle control systems, and sensor interference that may disrupt safe navigation. In Rwanda, cybersecurity protection is partly governed by the Law No. 60/2018 on Prevention and Punishment of Cybercrimes, which criminalizes unauthorized access and interference with computer systems. However, while the law provides general cybercrime protection, it does not yet contain detailed operational standards specifically tailored to autonomous vehicle technology, leaving a regulatory gap in emerging intelligent transportation security management.

Given that transportation networks may be considered critical infrastructure; autonomous vehicle systems should ideally be subjected to stronger cybersecurity governance requirements. Regulatory authorities may need to introduce mandatory cybersecurity audits for autonomous mobility operators, enforce real-time incident reporting obligations, establish minimum encryption standards, and require continuous software security updates to counter evolving cyber threats. Without comprehensive cybersecurity regulation, autonomous vehicle ecosystems could expose public transport safety to catastrophic system failures, potentially resulting in large-scale accidents, financial losses, and public security risks. Therefore, proactive legal and technical safeguards are essential to ensure that innovation in autonomous mobility develops alongside robust cyber protection mechanisms.

Given that transportation networks may be considered critical infrastructure; autonomous vehicle systems should ideally be subjected to stronger cybersecurity governance requirements. Regulatory authorities may need to introduce mandatory cybersecurity audits for autonomous mobility operators, enforce real-time incident reporting obligations, establish minimum encryption standards, and require continuous software security updates to counter evolving cyber threats. Without comprehensive cybersecurity regulation, autonomous vehicle ecosystems could expose public transport safety to catastrophic system failures, potentially resulting in large-scale accidents, financial losses, and public security risks. Therefore, proactive legal and technical safeguards are essential to ensure that innovation in autonomous mobility develops alongside robust cyber protection mechanisms.

INSURANCE AND RISK ALLOCATION

Traditional motor insurance systems are primarily designed around human driving behavior, where risk assessment depends on factors such as driver experience, road conduct, and accident history. However, autonomous vehicles significantly alter this risk structure because a large proportion of traffic accidents globally are associated with human error, while autonomous mobility systems shift potential liability toward software reliability, sensor performance, and system architecture. In Rwanda, the insurance regulatory framework may need modernization to determine whether insurance coverage should attach to the vehicle itself, the technology manufacturer, or a combination of ecosystem participants. Key policy questions include whether liability insurance should follow the autonomous vehicle regardless of ownership and whether minimum mandatory insurance thresholds should be revised to reflect technological risks associated with intelligent transportation.

Policy reform may also consider the introduction of a structured compensation mechanism for autonomous vehicle-related accidents. Rwanda could evaluate the possibility of establishing a no-fault compensation model to ensure that victims receive prompt financial recovery without requiring complex proof of negligence in technologically induced accidents. Such a framework would reduce litigation complexity and improve public confidence in autonomous mobility adoption. At the same time, insurance regulators and private insurers would benefit from clear statutory guidance on risk allocation, premium calculation models, and underwriting standards for autonomous systems, thereby reducing uncertainty and supporting sustainable development of advanced transportation technologies.

CRIMINAL LAW CONSIDERATIONS

Autonomous vehicles introduce complex challenges to traditional criminal law because liability in criminal justice systems is generally based on human intent, known as mens rea. In Rwanda, the criminal justice framework under the Rwanda Penal Code primarily assumes that unlawful conduct is committed through human action accompanied by intention, recklessness, or negligence. However, autonomous vehicles operate through algorithmic decision-making processes, which raises important legal questions when traffic violations or accidents occur. For example, it remains unclear whether criminal responsibility should be imposed on vehicle owners, software developers, or corporate entities when harm results from system operation rather than human control.

The emergence of algorithm-induced harm may require legislative reform to address accountability in intelligent transportation systems. Situations involving software defects, machine-learning errors, or cybersecurity manipulation could produce outcomes that resemble criminal negligence without satisfying traditional intent requirements.

Therefore, policymakers may need to consider introducing legal provisions that clarify corporate criminal liability, establish standards for technological due diligence, and define responsibility across the autonomous mobility supply chain. Such reforms would ensure that the criminal justice system remains effective in addressing harm while accommodating technological innovation in transportation.

ETHICAL AND HUMAN RIGHTS DIMENSIONS

Autonomous vehicles raise important ethical and human rights considerations because these systems may be required to make real-time decisions that directly affect human life and safety. Critical moral questions arise regarding how an autonomous vehicle should respond in unavoidable collision scenarios, often referred to as the "trolley problem" in ethical theory, where the system may have to choose between different harmful outcomes. There is also concern that machine-learning algorithms could unintentionally produce biased outcomes if training data reflects social or demographic inequalities. In Rwanda, any regulatory framework governing autonomous mobility must align with the constitutional guarantees of human dignity, equality, and privacy established under the national constitutional order.

Autonomous vehicles rely heavily on continuous data collection and processing to function effectively. These systems gather various forms of information, including geolocation signals, traffic movement patterns, environmental readings, and in some cases biometric or facial recognition inputs. In Rwanda, data protection is governed by Law No. 58/2021 Relating to the Protection of Personal Data and Privacy, which requires that personal data be processed lawfully, collected for clearly defined purposes, limited to what is necessary, and protected through appropriate security measures. These general protections provide an important foundation for regulating emerging technologies such as autonomous mobility systems.

REGULATORY GAPS AND INSTITUTIONAL READINESS

The development of autonomous mobility regulation should also be consistent with Rwanda's broader technological governance strategy, including the principles outlined in the national artificial intelligence policy. The Constitution of Rwanda provides fundamental protection of individual rights, while the Rwanda Information Society Authority promotes ethical digital transformation. Rwanda's national AI policy emphasizes transparency, fairness, and accountability in algorithmic decision-making, and these values should be operationalized within transport regulation to ensure that autonomous vehicle deployment does not compromise privacy rights, social justice, or public trust in emerging intelligent transportation systems.

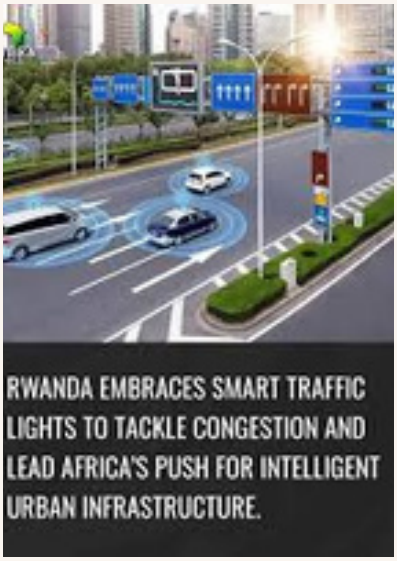
To maintain its position as a regional innovation leader, Rwanda may need to adopt a proactive regulatory strategy that balances technological advancement with public safety and legal certainty. Developing a dedicated autonomous vehicle legal framework would help establish testing protocols, safety certification requirements, operational standards, and institutional oversight mechanisms. Such reforms would strengthen consumer protection, promote responsible technological innovation, and ensure that the country's transport modernization agenda progresses in harmony with economic competitiveness, cybersecurity protection, and long-term sustainable development objectives.

RECOMMENDATIONS FOR REFORM

To ensure safe and sustainable deployment of autonomous mobility technologies in Rwanda, comprehensive legal reform is necessary. The first priority should be the enactment of a dedicated Autonomous Mobility Act that clearly defines autonomous systems, establishes vehicle testing and certification standards, and allocates liability among technology developers, manufacturers, and operators. Such legislation would provide legal certainty for industry participants while protecting public safety. The law should also outline compliance obligations for autonomous system deployment and create enforceable operational safety benchmarks for intelligent transportation technologies.

Regulatory innovation can be further supported through the establishment of supervised regulatory sandboxes that allow controlled pilot testing of autonomous vehicles before full market deployment. Rwanda should also develop sector-specific data governance guidelines to ensure that mobility-related data processing is consistent with existing privacy protection standards. In addition, introducing strict product liability provisions for high-risk artificial intelligence systems would help clarify responsibility when algorithmic design or system malfunction causes harm. Strengthening cybersecurity certification requirements in line with international automotive security standards would also reduce digital vulnerability in connected transportation systems.

Finally, ethical governance should be integrated into the regulatory architecture through the creation of specialized artificial intelligence mobility oversight mechanisms. Establishing review boards or monitoring institutions dedicated to autonomous transportation would help evaluate safety performance, algorithmic fairness, and long-term societal impact. These reforms would position Rwanda as a forward-looking technology jurisdiction that promotes innovation while maintaining strong legal, ethical, and security protections in the emerging field of autonomous mobility.



CONCLUSION

The emergence of autonomous vehicles and intelligent mobility systems represents a fundamental transformation in modern transportation. In Rwanda, these technologies are moving from theoretical innovation toward practical regulatory reality. While the country has already established a strong foundation in digital governance, cybersecurity protection, and personal data regulation, the introduction of algorithm-driven transportation requires further legal and institutional adaptation. Traditional legal doctrines were developed primarily for human-operated systems, and the transition toward intelligent mobility will demand modernization of liability principles, safety governance, and technological oversight mechanisms.