



PART 2

Read the text below and answer questions 14–26.

THE ETHICAL MAZE OF AUTONOMOUS VEHICLES

Autonomous vehicles (AVs) are commonly presented as a technological remedy for an old problem: human error on the road. Fewer collisions, less congestion, and wider access for people who cannot drive are the headline benefits. Yet the ethical landscape does not begin and end with spectacular “trolley problem” thought experiments. Such crash dilemmas are rhetorically powerful but statistically rare, and they can distract from the routine decisions that distribute risk every second an AV operates. Ethical evaluation therefore extends to mundane engineering choices, the evidence required for deployment, and the social and legal arrangements that determine who benefits and who bears harm when systems fail.

At the core of AV ethics lies a safety philosophy built less on utilitarian calculus in emergencies than on preventing emergencies in the first place. Engineers emphasise that most safety is produced by cautious behaviour: maintaining generous following distances, managing speed to preserve stopping margins, and refusing manoeuvres that exceed a vehicle’s confidence in its sensors or control. Even here, however, values are embedded. A system tuned to minimise crashes may tolerate more false positives—braking or yielding unnecessarily—which can frustrate surrounding drivers, degrade traffic flow, or provoke risky human responses. A more assertive system may appear smoother but accept a higher background probability of conflict. The “ethical setting” is therefore not a single switch but a web of thresholds that quietly determine whose time is prioritised, how uncertainty is treated, and how risk is apportioned across passengers, pedestrians, and other road users.

Proving safety becomes hardest at the margins of experience. AVs can be trained and tested extensively in typical environments, yet the most consequential failures often occur in rare, messy situations: an erratic pedestrian stepping off a curb mid-block, a cyclist swerving around debris, a temporary sign placed at an odd angle, or a burst of glare that confuses vision systems. These long-tail events are often called edge cases, and they resist straightforward enumeration. Road testing accumulates real mileage but cannot ethically “hunt” for dangerous scenarios, while simulation can generate vast numbers of events but may miss subtle behaviours that real humans produce. As a result, developers face an ethical question of sufficiency: how much evidence counts as “safe enough,” what uncertainty is acceptable, and how to monitor performance once software updates and new data distributions change what the system encounters.



Data sits at the centre of this debate because AV safety is inseparable from measurement. Vehicles generate and store enormous quantities of sensor logs from cameras, radar, and lidar, capturing not only the vehicle's actions but also fine-grained traces of surrounding people and environments. Companies argue that retaining these logs enables debugging, post-incident analysis, and continuous improvement, especially when rare failures must be reconstructed precisely. Privacy advocates respond that persistent recording can normalise surveillance, particularly if retention periods are long, access rules are unclear, or data is shared with third parties. In practice, policies on retention and access vary widely between firms and jurisdictions, shaping public trust and willingness to accept AVs in everyday life. The ethical challenge is to balance the legitimate need for safety evidence with strict limits on collection, storage, de-identification, and secondary use.

Liability attribution is equally unsettled, especially in partially automated systems that instruct a human to supervise. If the machine performs most steering and braking, the human may become complacent, and their capacity to intervene quickly may be more imagined than real. Critics describe a “moral crumbling” effect: when something goes wrong, responsibility collapses onto the human operator because they are the easiest target, even if meaningful control had already been ceded to automation. Manufacturers, regulators, and insurers must therefore decide whether AV harms resemble product defects, driver negligence, or a hybrid category where responsibility is distributed across designers, operators, and those who authorised deployment. Transparent documentation—training data sources, test coverage, update histories, and incident response procedures—can make liability decisions less arbitrary, but it also raises commercial tensions when firms are reluctant to reveal proprietary details.

Cybersecurity adds another layer of ethical urgency because AVs are connected systems, not isolated machines. Wireless updates, cloud connectivity, and complex sensor interfaces create attack surfaces that traditional vehicles did not have. A successful intrusion could disrupt perception, alter control commands, immobilise fleets, or exfiltrate sensitive information—turning a safety technology into a public hazard. Ethical deployment therefore requires security engineering from the outset: hardened software pipelines, strong authentication, careful key management, and rapid patching when vulnerabilities are discovered. It also requires clear reporting norms so that security flaws are not hidden until they are exploited. In this context, “safety” is not only about preventing crashes but also about preventing malicious manipulation of the system's behaviour.

The social consequences of automation broaden the ethical lens beyond engineering and law. Large-scale AV deployment may disrupt employment in trucking, delivery, taxis, and logistics support, even if new roles emerge in fleet operations and maintenance. The



transition costs are likely to be unevenly distributed across regions and worker groups, raising questions about who should fund retraining, wage support, or phased adoption. At the same time, AVs can reproduce or amplify inequality through algorithmic bias. If training data under-represents certain neighbourhoods, lighting conditions, body types, or mobility aids, detection and prediction may degrade precisely where vulnerability is higher. Fairness thus involves more than one demographic metric; it includes which areas are prioritised for service, who is excluded by design choices, and whether safety improvements are shared broadly rather than concentrated in affluent districts.

Regulation increasingly responds by defining operational limits rather than accepting blanket claims of autonomy. Many systems are certified only within an operational design domain—a set of road types, speeds, weather conditions, and mapping quality where performance is validated. One common tool is geofencing, which restricts vehicles to mapped zones or conditions where risks are better understood. When the system detects it is leaving that domain—due to heavy rain, sensor obstruction, unfamiliar road layouts, or ambiguous markings—it should not improvise beyond evidence. Instead, it is expected to execute a minimum-risk manoeuvre, such as slowing down, signalling, and pulling over to a safe stop. This regulatory stance embodies a practical ethic: reducing service is preferable to operating beyond proven capability, even if it occasionally disappoints users or limits commercial scale.

Questions 14–17

Complete the table below. Choose **NO MORE THAN TWO WORDS** from the text for each answer.

Autonomous vehicle safety and governance

Area	Risk / Context	Control, evidence or concern
Safety and validation	Everyday driving hazards	Cautious 14 maintains following distances and stopping margins
	Rare situations known as 15	Cannot be represented fully through either road testing or simulation
Data and accountability	Need to reconstruct failures	Detailed sensor 16 retained for debugging; may also enable surveillance



Area	Risk / Context	Control, evidence or concern
	Unclear division of human and machine control	Transparent documentation can support less arbitrary liability decisions
System controls	Malicious interference with connected vehicles	Secure software, authentication and rapid patching protect safety and data
	Operation outside a validated design domain	17 restricts vehicles to approved mapped areas; minimum-risk manoeuvres provide a fallback

Questions 18–22

Choose **TRUE** if the statement agrees with the information given in the text, choose **FALSE** if the statement contradicts the information, or choose **NOT GIVEN** if there is no information on this.

18 The passage suggests that trolley-style crash dilemmas are the most important ethical issue for autonomous vehicles.

19 The passage indicates that neither simulation nor road testing can represent the full range of real-world driving conditions.

20 The passage states that all AV companies must delete sensor logs after a fixed number of days.

21 The passage suggests that responsibility is difficult to assign when humans supervise systems that control most driving.

22 The passage states that transparent documentation could make liability decisions less arbitrary.

Questions 23–26

Select the correct answer.

23 Why does the passage raise privacy concerns about AV data?

A Developers are prohibited from retaining data after completing a safety investigation.

B Sensor logs may capture detailed information about surrounding people and environments.



- C** De-identification removes every risk associated with the secondary use of data.
- D** Rules governing data retention and access are identical across firms and jurisdictions.

24 Why is cybersecurity essential for autonomous vehicles?

- A** Attacks could manipulate vehicle behaviour, immobilise fleets, or expose sensitive information.
- B** Wireless updates and cloud connectivity reduce the number of possible attack routes.
- C** Security measures can be added after deployment without affecting vehicle safety.
- D** Reporting vulnerabilities is unnecessary if a vehicle continues operating normally.

25 What concern does the passage raise about employment?

- A** New maintenance roles will prevent any workers from being displaced.
- B** Employment effects will be limited to taxi drivers in affluent cities.
- C** Transition costs will be distributed evenly across regions and worker groups.
- D** Automation may disrupt driving and logistics work, creating a need for retraining and other support.

26 What does the passage suggest about minimum-risk manoeuvres?

- A** They allow vehicles to continue normally outside their validated operating conditions.
- B** They automatically expand the mapped area in which a vehicle is authorised to operate.
- C** They provide a fallback when a vehicle detects that it is moving beyond proven capability.
- D** They guarantee that an autonomous vehicle will never be involved in a collision.

Answer Key

- 14. behaviour
- 15. edge cases
- 16. logs
- 17. geofencing
- 18. FALSE
- 19. TRUE
- 20. NOT GIVEN
- 21. TRUE
- 22. TRUE



23. B

24. A

25. D

26. C