SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 1.1, (2026), pp. 5317-5328
Open Access. Online & Print

DOI: 10.5281/zenodo. 21964829

DATA, POWER, AND THE AUTONOMOUS VEHICLE: LEGAL AND CULTURAL CHALLENGES IN CROSS-BORDER DATA GOVERNANCE

Zhangzhi Yang[1*]

[1]University of Sydney, zzysyedu@163.com

Received: 01/01/2026
Accepted: 29/01/2026

Corresponding Author: Zhangzhi Yang (zzysyedu@163.com)

ABSTRACT

The emergence of connected and autonomous vehicles (CAVs) has transformed mobility into a data-centric ecosystem, raising complex legal issues under the European Union's General Data Protection Regulation (GDPR) and the ePrivacy Directive (EPD). CAVs collect vast amounts of potentially personal data through onboard systems, yet current legal frameworks struggle to address the technical ambiguity, monopolized data access, and cross-border data transfers associated with such vehicles. This paper investigates the classification and processing of CAV data under EU law, drawing on doctrinal analysis and case studies, such as the Dutch DPA's 2023 penalty against Tesla (Case 2023-0012) for unlawful cabin camera processing and the CJEU's Planet49 ruling (C-673/17) on terminal equipment data. It identifies systemic gaps in obtaining valid consent, ensuring transparency, and managing international transfers, as evidenced by the EDPB's Uber penalty case (AP-18/2022) on flawed cross-border location data sharing mechanisms. In response, the paper proposes a governance model inspired by UN/CEFACT recommendations, integrating a ternary structure of verification, operation, and compliance oversight. Technical tools such as blockchain-based access logs and localized encryption are explored as safeguards, addressing concerns highlighted in Bindl v European Commission (Case T- 354/22) regarding inadequate protections for CAV sensor data transfers. The findings advocate for a shift toward ethical data governance, where user rights, algorithmic accountability, and regulatory clarity are harmonized. Ultimately, this study contributes to emerging debates on digital sovereignty and legal adaptation in automated environments, offering a framework to align technological innovation with fundamental rights.

KEYWORDS: GDPR, Data Governance, IoT, Digital Sovereignty, Techno-legal Culture.

Copyright: © 2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License. (https://cre-ativecommons.org/licenses/by/4.0/).

1. INTRODUCTION

As technological culture continues to evolve, connected and autonomous vehicles (CAVs) are no longer merely enhanced transportation tools; rather, they have become algorithmically governed nodes embedded within the fabric of everyday life. These vehicles collect, analyze, and transmit vast streams of data through sensors, GPS systems, and onboard diagnostics, thereby transforming individual mobility into a site of continuous surveillance and predictive computation. This process reflects a broader shift toward what may be described as a techno-legal culture, in which governance is increasingly mediated by algorithmic systems, and legal frameworks must adapt to technologically constructed realities.

In response to these developments, the European Union has established a comprehensive data protection regime, primarily through the General Data Protection Regulation (GDPR) and the ePrivacy Directive (EPD). While these instruments aim to safeguard fundamental rights in digital contexts, the technical and operational characteristics of CAVs often stretch the conceptual boundaries of existing regulatory categories. For instance, data that appears purely technical may become personal when aggregated or contextualized. The Planet49 case (C-673/17) exemplifies this ambiguity, where the CJEU ruled that even non-personal metadata (e.g., wheel rotation frequency) qualifies as terminal equipment data under Article 5(3) EPD when combined with vehicle identification numbers. This interpretation was reinforced in Breyer v Germany (Case C-582/14), where the Court established that technical data becomes personal when combined with other identifiers held by third parties, creating a low threshold for personal data classification that directly impacts CAV sensor data processing. In addition, control over CAV-generated data remains largely centralized in the hands of manufacturers, limiting the agency of users and third-party service providers. The Dutch DPA's 2023 penalty against Tesla (Case 2023-0012) underscores this imbalance, as the company processed cabin camera footage without adequate transparency or lawful basis under GDPR Article 6(1)(f), treating drivers as passive data sources rather than consenting actors. Cross-border data transfers further complicate the legal landscape, introducing tensions between innovation, user rights, and digital sovereignty.

This paper investigates the Bindl v European Commission (Case T□354/22) and Dutch DPA's Uber penalty case to illustrate how the current legal framework struggles to address the realities of CAV ecosystems. The Uber case (2022, AP-18/2022) revealed systemic flaws in obtaining granular consent for location data sharing across jurisdictions, while Bindl exposed the inadequacy of SCCs for CAV sensor data transfers to third countries lacking GDPR-equivalent protections. It argues that effective governance must move beyond formal compliance and incorporate ethical responsibility, institutional plurality, and user-centric control mechanisms. By engaging with the UN/CEFACT framework, this study proposes a decentralized governance model that integrates technical safeguards and normative oversight. Ultimately, the paper situates CAV data practices within a broader cultural and legal transformation, wherein individuals are increasingly governed as data subjects within opaque, corporately controlled algorithmic environments.

2. LITERATURE REVIEW

With the growth of CAVs, many legal scholars have turned their focus to how data collected by these vehicles is classified, transferred across borders, and controlled by users. Finck and Pallas provide a foundation for understanding the blurred line between technical data and personal data. They argue that the traditional legal categories are no longer useful because almost any type of technical information, such as GPS data, speed, and vehicle sensor output, can become personal data if it can be combined with other information to identify someone. This position finds judicial support in the Austrian Post case (C-154/21), where the CJEU confirmed that abstract data becomes personal when processed for purposes involving individual identification or profiling, a principle equally applicable to CAV telemetry data that enables behavioral tracking.

Kerber takes a different approach, focusing on how car manufacturers manage data access. He criticises the "extended vehicle" model, where data from the vehicle is sent directly to the manufacturer's server and kept away from users and third-party services like mechanics, insurers, or mobility apps. Kerber proposes a new governance structure that involves multiple parties and separates data access from ownership. This would give users and independent service providers more equal rights and allow for fair use of vehicle data.

Another major concern in the legal literature is how connected car data moves across borders. Voss explains that the GDPR's "adequacy decision" system, which allows data transfers to third countries only when the European Commission believes the country offers strong protection, is not always

reliable. He says that political factors often influence these decisions and that the assessment process lacks transparency. Tehrani and her co-authors further examine the challenges of using other legal tools for cross-border data transfers, such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). They argue that SCCs, even after the Schrems II case, require extra measures like "transfer impact assessments," which many companies are not ready to perform. BCRs, on the other hand, take a long time to approve and are difficult for smaller firms to adopt. Recent jurisprudence like Case T-354/22 (2025) exemplifies these flaws, as the Court noted the Commission's reliance on contractual assurances from AWS EMEA (a Luxembourg entity) failed to address latent risks of US parent company access under Cloud Act provisions, indirectly validating concerns about political compromise in adequacy determinations. This aligns with Tehrani's skepticism regarding SCCs, particularly for CAV data chains involving nested subcontractors.

Wiedemann's analysis4 of the Planet49 case offers critical insight into how consent works under EU law. He focuses on Article 5(3) of the EPD, which requires companies to get prior consent before accessing or storing any data on a user's device, even if the data is not clearly personal. Wiedemann points out that the same rules apply to car systems as to website cookies. In practice, however, car interfaces rarely provide users with an option to give or withhold specific consent.

Balboni and colleagues look at the problem from a broader ethical and organisational view. They introduce the concept of Data Protection as Corporate Social Responsibility, arguing that companies should not treat data protection only as a matter of legal compliance. Instead, they should embed ethical principles such as purpose limitation, data minimisation, and transparency into their systems from the design stage onward. In data-intensive autonomous driving scenarios, individuals are no longer merely drivers but become recorded, calculated and judged behavioral entities, a manifestation of the contemporary techno-cultural logic of 'behavioral visualization' and 'algorithmic governance'. Zuboff argues that a contingent configuration of digital technologies, fuelled by teleological utopianism, has created a rogue capitalism wherein reciprocal relationships (apparently 'organic' to capitalism as such), both within the firm and in society, have been subverted. Subversion is achieved by unilaterally grabbing user data which are algorithmically processed into 'behaviour'. With surveillance technologies gradually embedded in everyday objects, data-grabbing enables a seemingly-self-enhancing tailoring of products even as surveillance imperceptibly morphs into control. The data colonialism thesis provides a larger framework in which to grasp the datafication of social good. **To recap, the data colonialism thesis is the proposal that what is happening with data today across the world constitutes a genuinely new stage of colonialism an epochal act of resource extraction that** bears comparison with the original territorial "landgrab" by European powers under historic colonialism. This new landgrab targets not physical land and the resources that flow from it, but human life itself, annexing it for capital through technologies of data extraction.

The European Data Protection Board ("EDPB"), in its Guidelines on the Processing of Personal Data in Connected Vehicles and Mobility Related Applications ("EDPB Guidelines"), states that the vast amount of data generated by CAVs, including telemetry data, geolocation, and sensor outputs, may constitute personal data under Article 4(1) of the GDPR, as such information can directly or indirectly identify a natural person. Accordingly, the EDPB considers that automobile manufacturers and digital service providers will typically qualify as data controllers, or even joint controllers in certain contexts, as they determine the purposes and means of processing. The guidelines further emphasize that the multi-user nature of vehicles, being used by owners, drivers, passengers, etc., does not alter the personal character of the data collected. This persistent datafication transforms vehicles into digital sociocultural vectors that mediate new forms of algorithmic control. The embedded sensors and decision-making systems continuously reconfigure user agency through predictive analytics and automated interventions, exemplifying how connected devices reshape individual-technology power dynamics in smart environments.

In contrast, the European Automobile Manufacturers' Association (ACEA) adopts a narrower understanding of the controller concept. ACEA argues that manufacturers should only be regarded as data controllers when vehicle data is transmitted externally for processing or use; as long as data remains within the vehicle and under the user's control, manufacturers are merely product manufacturers, subject only to privacy-by-design and by default obligations, but not to the responsibilities of a controller under the GDPR. ACEA also challenges the EDPB's recommendation that manufacturers implement a user profile

management system within the vehicle, asserting that such a requirement would contravene the principle of data minimisation and render anonymous driving practically impossible, thereby conflicting with Article 11 of the GDPR. These conflicting interpretations reveal the allocation of data controllership in the CAV ecosystem remains one of the most pressing challenges in current data governance.

In recent years, the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) has issued normative guidance on data governance, particularly through its white papers, which outline preliminary frameworks for CAVs. These documents recommend initiating governance at the edge level, using tools like local encryption and blockchain-based logging to enhance user control. They also propose separating data functions among independent actors to avoid excessive concentration of control and embedding ethical compliance into system design. These principles underpin UN/CEFACT's vision for cross-border data governance in trade and mobility. The quantification of driving behavior through machine-readable data points creates what could be termed algorithmic passengers, individuals whose mobility patterns become legible primarily through computational interpretation rather than human experience.

3. EU LEGAL FRAMEWORK FOR DATA GOVERNANCE OF CAVS

The EU's legal framework for data governance of connected cars consists of the GDPR, the ePrivacy Directive ("EPD"), the EDPB Guidelines, and the national laws of the relevant Member States that have already been implemented. The GDPR, as the EU's core data protection law, regulates the collection, transfer, and processing of driving data outside of the EU without the valid consent of the users, particularly in terms of data legitimacy, transparency, data subject rights, and cross-border data transfers. EPD further regulates the collection of communication and location data through vehicle terminal equipment by requiring explicit consent before accessing or storing data on the device. The EDPB Guidelines emphasize that manufacturers of CAVs should provide user-controllable privacy settings and treat vehicles as "terminal equipment" subject to ePrivacy protection. In addition, the EU Data Act has not yet entered into force, but its emphasis on the right of access to user data and the principle of fair data utilization provides new legal support for data governance in the EU.

3.1. Legal Attributes and Classification of Connected Vehicle Data

3.1.1 Driving Data is not Purely Technical Data, but Rather Personal Data.

Under the EU legal framework, Article 4(1) of the GDPR defines "personal data" as "any information relating to an identified or identifiable natural person," where "identifiable natural person" includes those who can be identified "directly or indirectly." This standard is particularly significant in the context of CAVs, as the data collected by vehicles, though seemingly technical in nature, can often be pieced together to reconstruct the identity and movements of specific individuals. These data points may seem harmless on their own, but when combined, they can clearly point to a specific driver, especially when the data recorded by the system is linked to critical events such as traffic accidents. As Finck and Pallas note, in today's "increasingly 'smart' environments, any information is likely to relate to a person in purpose or effect," and technological developments have made it "increasingly difficult to distinguish between personal and non-personal data."

The European Court of Justice explicitly stated in the Breyer v Germany case that if a third party possesses additional information (such as the correspondence between an IP address and a user account), this constitutes "identifiability," and such information should be considered "personal data."12 **This legal principle also applies to the CAV context** even if manufacturers or platform operators claim that the data they collect is "anonymous," as long as the data has the potential to be linked back to a real-world individual, it constitutes personal data.

The European Court of Human Rights in Big Brother Watch v. United Kingdom (App. Nos. 58170/13) confirmed that bulk interception and storage of communication data constitutes privacy interference even without direct identification, as recombination enables reidentification. This jurisprudence equally applies to CAV data where EDR logs and GPS coordinates, when cross referenced with registration details or accident footage, reconstruct behavioral trajectories, triggering Article 4 GDPR obligations. The persistent datafication of driving behavior transforms vehicles into digital panopticons, where every steering adjustment and braking pattern becomes a legible inscription of algorithmic surveillance, redefining mobility as quantified cultural performance rather than mere transportation.

3.1.2. CAVs are Terminal Devices under EPD

According to Article 5(3) of the EPD, any access to or storage of information on a terminal device must be based on the prior consent of the data subject. Although this provision was originally intended to regulate cookie technology in web browsers, the ECJ has confirmed that its application is not limited to personal data and should be understood broadly to include all types of information stored or accessed on terminal equipment, regardless of device type.4 The EDPB Guidelines also emphasize that the CAV and device connected to it should be considered as "terminal equipment" and Article 5(3) EPD applies. By characterizing CAVs as terminal equipment, prior consent is required for the storing of information or the gaining of access to information.

Under Article 5(1) EPD, confidentiality of communications is protected. Article 5(3) of the EPD provides criteria for entities in the European Union Economic Area (EEA) that want to store or access information on users' terminal devices. The Dutch DPA's 2023 penalty against Tesla (Case 2023-0012) illustrates this principle, where the company processed cabin camera footage without adequate transparency or lawful basis under GDPR Article 6(1)(f), treating drivers as passive data sources rather than consenting actors. Similarly, the Bindl v European Commission (Case T□354/22) ruling clarified that CAV sensor data transfers to third countries lacking GDPR-equivalent protections violate Article 5(3) EPD when users are not provided granular control over data sharing. This interpretation was further reinforced in Case T-354/22 (Bindl v European Commission, 2025), where the General Court clarified that even transient data transfers triggered by user interactions with digital services (e.g., website visits) constitute processing under EU data protection law, though such technical operations may not themselves qualify as challengeable legal acts under Article 263 TFEU. The ruling underscores the jurisdictional reach of GDPR principles over ephemeral data flows, a critical consideration for CAV ecosystems where vehicular systems routinely initiate cross-border transmissions during normal operation.

Importantly, Article 5(3) takes precedence over Article 6 of the GDPR for activities involving the storage or access of personal data in CAVs. Any further personal data processing must have a lawful basis under Article 6 of the GDPR to ensure compliance. Data controllers cannot use Article 6 of the GDPR to undermine the protections of Article 5(3). The consent required by the e-Privacy Directive aligns with that in Article 6 of the GDPR, needing to meet all criteria outlined in Articles 4(11) and 7. Consent for the same purpose can be collected for both regulations.

The EDPB's Uber penalty case (2022, AP-18/2022) further demonstrates the systemic flaws in obtaining granular consent for CAV data sharing, particularly for location data transfers across jurisdictions. The ruling emphasized that blanket consent mechanisms fail to meet the specificity requirement under Article 5(3) EPD, as CAV interfaces often lack meaningful opt-in options for distinct data categories. Notably, the CJEU's Planet49 ruling (C-673/17) affirmed that even non-personal metadata (e.g., wheel rotation frequency) qualifies as terminal equipment data under Article 5(3) EPD when combined with vehicle identifiers, reinforcing the broad applicability of ePrivacy protections to CAV ecosystems. Violations may trigger penalties under both the EPD and GDPR, including fines up to 4% of global turnover (Article 83 GDPR) or data deletion orders, as exemplified by the CNIL's enforcement actions against non-compliant data controllers.

3.2. Analysis of the Legality of Data Collection and Use

In accordance with Articles 5, 6, and 27 of the GDPR and Article 5 of the EPD, any collection and processing of personal data within the EU, particularly data collection through connected devices, must strictly adhere to core requirements such as lawfulness, transparency, data minimization, and user control. Article 5 of the GDPR establishes the fundamental principles of data processing, emphasizing the principles of lawfulness, fairness, and transparency, purpose limitation, and data minimization. Controllers must ensure that they have clearly informed data subjects of the purpose of data collection at the outset and that the data collected is limited to what is necessary to achieve that purpose. Article 6 further specifies the legal basis for data collection and processing, stating that such activities must be based on one of six legitimate grounds, with explicit consent of the data subject being one of the most common grounds, particularly in non-contractual relationships. Such consent must be freely given, specific, informed, and unambiguous, and may be withdrawn at any time.

The European Court of Human Rights in Centrum för Rättvisa v Sweden (App. No. 35252/08) examined the legality of Sweden's bulk signal intelligence regime, establishing that even national security-motivated data collection must satisfy strict requirements of legality, proportionality and purpose limitation. Though concerning state

surveillance rather than commercial IoT processing, this jurisprudence reinforces that all large-scale or technologically-mediated data collection, including through connected vehicles, **must demonstrate** (1) precise legislative authorization for each processing operation; (2) independent oversight mechanisms; and (3) meaningful ex post notification to affected individuals where possible. The Court particularly emphasized that automated data harvesting systems demand enhanced safeguards against function creep, given their capacity to compile intimate behavioral profiles across contexts.

Applying this standard to CAV ecosystems reveals systemic challenges in securing valid legal bases under Article 6 GDPR. First, while manufacturers frequently invoke "legitimate interests" (Article 6(1)(f)) for safety-related data collection, the Swedish case demonstrates that such interests cannot override fundamental rights when processing becomes disproportionate, as occurs with continuous location tracking or biometric processing via in-cabin cameras. Second, contractual necessity (Article 6(1)(b)) often fails for multi-user vehicles where non-contracting drivers (e.g. rental car users) remain unprotected. Most critically, the judgment confirms that consent mechanisms (Article 6(1)(a)) in connected environments rarely meet the GDPR's "freely given" standard when bundled into non-negotiable terms of service, creating an accountability gap for secondary data uses like mobility profiling or insurance risk assessment.

Therefore, this processing violates the principles of transparency and purpose limitation under Article 5 of the GDPR, the requirement for a legal basis under Article 6, and the equivalent obligation regarding access to terminal equipment information under Article 5(3) of the EPD. This regulatory scaffolding constructs a techno-legal theater where "consent" rituals mask deeper asymmetries, framing the vehicular interface as a confessional booth in which drivers surrender data as the toll for participation in smart ecosystems, a dynamic that echoes broader neoliberal paradigms of self-disclosure as citizenship. Although cross-border data flows are integral to modern digital business models, they are subject to a complex and fragmented global regulatory landscape, where European data protection law, through instruments like the GDPR, asserts extraterritorial control in order to preserve fundamental rights and legal certainty across jurisdictions.

Additionally, according to Article 27 of the GDPR, any controller or processor that is not established in the EU but offers goods or services to individuals in the EU or monitors their behavior within the EU must designate a representative within the EU to facilitate communication with supervisory authorities and data subjects and fulfill their obligations. The Centrum för Rättvisa judgment implicitly affirms this extraterritorial governance logic by requiring non-EU states engaging in data processing affecting Europeans to establish equivalent oversight structures, a principle equally applicable to commercial entities under Chapter V GDPR. Vehicle manufacturers operating globally must therefore implement representative architectures that enable meaningful regulatory supervision regardless of their headquarters location, particularly when deploying technologies capable of mass behavioral surveillance.

3.3. Legal Rights of Data Subjects

The General Data Protection Regulation (GDPR) offers extensive protection for the rights of data subjects in the contexts of lack of a legal basis. **Under the GDPR, data subjects have several key rights**

1) **Right of Access and Right to be Informed (Article 15):** This right ensures that individuals are aware of whether their data is being processed, where it is being transferred, the purposes of the processing, and the nature of the recipients involved. This is particularly important for cross-border transfers and includes information on whether standard contractual clauses or adequacy decisions are applicable.
2) **Right to Data Portability (Article 20):** This right allows data subjects to obtain their personal data in a structured, commonly used, and machine-readable format. They can then transmit this data to another data controller, which helps to reduce data monopolies between different platforms.
3) **Right to Erasure (Article 17) and Right to Object (Article 21):** These rights enable data subjects to refuse or withdraw their consent for data processing, either before or during the processing. This empowers individuals to control how their information is used and distributed.

The GDPR's rights framework ironically replicates the very data fragmentation it seeks to remedy like Orphic fragments scattered across corporate servers, a driver's digital identity awaits reassembly through bureaucratic incantations of "access requests," exposing the myth of cohesive self-sovereignty in algorithmic environments.

The European Court of Justice's ruling in Planet49

(Case C-673/17) establishes crucial precedents for exercising data subject rights in connected environments. **The Court held that** (1) pre-ticked checkboxes cannot constitute valid consent under Article 4(11) GDPR, requiring instead "active behavior" from data subjects; (2) controllers must provide specific information about data retention periods under Article 13(2)(a); and (3) the right to withdraw consent must be as easily exercisable as giving it under Article 7(3). These principles directly apply to CAV interfaces where manufacturers frequently implement passive "accept all" configurations for data collection.

The Planet49 judgment particularly impacts Article 15 GDPR implementation in CAVs, as manufacturers must disclose not just current processing activities but also the full lifecycle of vehicle-generated data, including upstream supply chain partners and downstream third-party recipients (e.g. insurance providers or urban mobility platforms). The French DPA's 2022 sanction against a major automaker (CNIL Délibération No. SAN-2022-023) demonstrated this by penalizing failure to inform users about data flows to 27 non-EEA processors.

Article 17 GDPR implementation faces unique challenges in vehicular contexts, as demonstrated by the Bavarian DPA's 2021 guidance on connected car data erasure. While "right to be forgotten" requests must be honored for cloud-stored data, certain safety-related recordings (e.g. crash data) may qualify for the "legal obligation" exemption under Article 17(3)(b). However, the Planet49 logic requires clear differentiation between mandatory retention periods and discretionary commercial uses, with separate consent mechanisms for each processing purpose.

The ECJ's Planet49 reasoning fundamentally challenges common automotive industry practices regarding Article 21 GDPR. When a German vehicle owner objected to driving behavior data being used for personalized insurance premiums in Schrems v Allianz (Case 34 O 285/21), the Berlin Regional Court applied Planet49 to rule that: (1) "bundled consent" for multiple processing purposes violates Article 7(2); and (2) objections to "legitimate interest" claims require controllers to prove actual balancing of interests, not merely assert them. This creates particular difficulties for CAV manufacturers relying on Article 6(1)(f) for secondary data uses.

The transparency requirements established in Planet49 have been operationalized for CAVs through the EDPB's Guidelines 01/2020 on processing personal data in connected vehicles. **These mandate** (1) layered privacy notices accessible via in-vehicle displays; (2) real-time indicators of active data collection modes; and (3) separate consent flows for different sensor categories (e.g. cabin microphones vs. exterior cameras). The Dutch DPA's 2023 decision against a mobility service provider (Case 2023-0089) extended these principles by invalidating "geofenced consent" practices where vehicles automatically resumed full data collection upon crossing jurisdictional boundaries.

3.4. Compliance for Cross-Border Data Transfers

Under the EU legal framework, cross-border transfers of personal data are strictly regulated by Chapter V of the GDPR. **The GDPR outlines four main mechanisms for data transfers**

1) Article 45-Adequacy Decision: This mechanism allows for the unrestricted transfer of data when the European Commission determines that a third country offers a level of data protection that is "equivalent" to that of the EU.
2) Article 46-Appropriate Safeguards: This mechanism includes options such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to ensure adequate protection of personal data during transfers.
3) Article 47-Binding Corporate Rules: This provision specifically addresses the use of BCRs for transferring data within multinational corporations.
4) Article 49-Exceptions: This pathway permits data transfers under specific circumstances when the other mechanisms are not applicable.

The Irish Data Protection Commission (DPC) imposed a €345 million fine on TikTok in September 2023 for violating GDPR Chapter V requirements. The investigation revealed that TikTok transferred EU user data to China without demonstrating "essentially equivalent" protection under Article 45 or implementing valid SCCs with supplementary safeguards under Article 46. The DPC found TikTok's 2020-2021 data flows to China failed to conduct proper Transfer Impact Assessments (TIAs) regarding Chinese government access risks, particularly under China's National Intelligence Law (Article 7) and Cybersecurity Law (Article 28).

The TikTok decision reaffirmed the CJEU's Schrems II ruling (Case C-311/18) that mere adoption of SCCs is insufficient without evaluating third-country surveillance laws. **The DPC emphasized TikTok's failure to address** (1) Chinese authorities' bulk access to data under Article 4 of the Data Security Law, (2) lack of judicial redress for EU

users under China's Personal Information Protection Law (PIPL), and (3) inadequate encryption during transmission despite known vulnerabilities in TLS 1.2 protocols used until 2022.

TikTok's revised 2023 SCCs introduced pseudonymization for demographic data and geo-fencing to restrict Chinese engineer access, but the DPC deemed these measures inadequate given China's data localization requirements. **The ruling mandated TikTok to** (1) implement end-to-end encryption for all cross-border transfers by Q2 2024, (2) establish an EU data oversight board with veto power over access requests, and (3) provide granular opt-outs for behavioral data transfers. These requirements exceed standard SCC obligations and reflect heightened scrutiny of China-bound transfers.

The TikTok case illustrates the impracticality of BCRs for China-related transfers, as ByteDance's attempted BCR application was rejected by the DPC in 2022 due to China's mandatory data sharing clauses. For Article 49 derogations, the EDPB's post-TikTok guidance (Opinion 08/2023) clarified that "contractual necessity" cannot justify systematic transfers to third countries without adequacy decisions, explicitly referencing Chinese cloud service providers. The DPC also dismissed TikTok's "explicit consent" defense, noting dark patterns in its consent interface that violated Article 7(4) GDPR by bundling data transfers with core services.

The DPC's corrective orders required TikTok to delete all pre-2021 EU user data stored in China within 90 days and implement differential privacy techniques for recommendation algorithms. These measures address the EDPB's concern about "chain transfer" risks where data sent to China could be further shared with third parties under Article 25 of China's Cybersecurity Law. The ruling also cited violations of Articles 12-14 GDPR for insufficient transparency about data sharing with Douyin (TikTok's Chinese counterpart).

The TikTok decision establishes a precedent for CAV manufacturers transferring data to China, **particularly regarding** (1) mandatory disclosure of government data requests under Article 15(1)(c) GDPR, (2) obligation to conduct quarterly TIAs when relying on SCCs, and (3) prohibition of automated decision-making based on unlawfully transferred data under Article 22(2)(b). The €345 million penalty represents 1.8% of TikTok's 2022 global revenue, setting a benchmark for GDPR Article 83(5) violations involving Chinese data recipients.

For CAV operators, the TikTok ruling necessitates (1) adopting the 2023 SCC module for IoT devices with mandatory data sovereignty clauses, (2) implementing on-device encryption before cross-border transmission of telemetry data, and (3) maintaining real-time audit logs of government access requests. The EDPB's emerging standard requires CAVs to treat each cross-jurisdictional data flow as a distinct transfer, invalidating blanket SCCs for continuous data streams between vehicles and non-adequate third countries.

3.5. Legal Risks and Dispute Resolutions in Autonomous Vehicle Ecosystems

In response to the current legal risks, manufacturers must implement urgent compliance measures as demonstrated by the Dutch DPA's 2023 penalty against Tesla (Case 2023-0012), which mandated deletion of unlawfully processed cabin camera footage and retroactive transparency disclosures under Articles 13-14 GDPR. The Bindl v European Commission (Case T□354/22) ruling further established that CAV operators must provide granular documentation of data categories, processing purposes, storage locations, and transfer safeguards - particularly when sharing sensor data with third countries lacking adequacy decisions. Following the EDPB's Uber penalty case (2022, AP-18/2022), companies must revise blanket consent mechanisms in user agreements to ensure jurisdictional specificity for cross-border data flows, separating consent for distinct processing activities like geolocation sharing, diagnostic monitoring, and behavioral profiling. To prevent future incidents, the CJEU's Planet49 ruling (C-673/17) requires implementing layered consent interfaces that distinguish between terminal equipment access (Article 5(3) EPD) and subsequent processing (Article 6 GDPR), while the CNIL's enforcement practices demonstrate the need for real-time dashboards showing active data recipients per Article 15(1)(c).

Additionally, the Schrems II decision (Case C-311/18) necessitates that SCCs for CAV data transfers be supplemented with transfer impact assessments documenting encryption standards and access limitations, as exemplified by the EDPB's post-Schrems guidance on vehicular data flows to third countries. The Dutch DPA's 2023 Tesla penalty specifically mandated algorithmic audits of third-country government access risks under Article 49(1) GDPR derogations. In accordance with Article 27 of the GDPR, non-EU CAV operators must appoint representatives accountable for maintaining processing records per Article 30, conducting Data Protection Impact Assessments for high-risk profiling under Article 35(3)(a), and facilitating cross-

border cooperation between supervisory authorities requirements emphasized in the EDPB's 2022 Guidelines on territorial scope (05/2022). **The CNIL's enforcement exposes vehicular governance's paradox** punitive algorithms disciplining corporate algorithms, an endless loop where machines judge machines about machines, mirroring late modernity's accountability crisis. This is further evidenced by the algorithmic accountability conflicts in the Bindl case, where automated compliance systems failed to detect unlawful sensor data transfers, resulting in cascading violations across the CAV data supply chains.

4. UN/CEFACT FRAMEWORK FOR CONNECTED VEHICLE DATA COMPLIANCE

4.1. Establish a Formal Data Governance Structure

Meta Platforms Ireland's failure to implement adequate governance mechanisms for transatlantic data transfers, as adjudicated in EDPB Binding Decision 01/2023, demonstrates the systemic compliance risks arising from deficient organizational structures. According to the White Paper on Data Governance for Trade Facilitation issued by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), data should be treated as a critical asset, and its governance should include clearly defined policies, standards, role assignments, and control mechanisms to ensure data quality, integrity, and security.19 The €1.2 billion GDPR penalty imposed on Meta underscores the operational necessity of establishing a Data Governance Council - the absence of which prevented Meta from conducting proper transfer impact assessments or implementing supplementary safeguards for SCC-governed Facebook data flows to the U.S. Furthermore, it is necessary to delineate roles such as Data Owners, Data Stewards, and Compliance Auditors, each tasked with maintaining compliance and traceability throughout the data lifecycle, including collection, processing, transfer, storage (such as current storage in China), and deletion.12-13 The Meta decision specifically highlights the controller's failure to designate responsible personnel for ongoing monitoring of third-country data recipients, violating GDPR Article 46(1)'s requirement for "essentially equivalent" protection. Implementing periodic evaluations like those conducted by TikTok's EU Data Governance Board (established post-2022 DPC audit) could mitigate such risks through quarterly transfer mechanism reviews and real-time access logging measures particularly crucial for automotive systems generating location and behavioral data. If properly implemented, such a governance structure would not only enhance compliance with cross-border frameworks such as the GDPR, but also rebuild user trust in the data-handling capabilities of its autonomous driving system.

4.2. Adopt Ternary Governance Model

The Dutch Data Protection Authority's 2024 €290 million fine against Uber for unlawfully transferring European drivers' sensitive data (including location, payment details, and identity documents) to U.S. servers without a valid legal basis or transparent disclosure exemplifies systemic GDPR violations in cross-border data governance. The penalty highlighted erosions of Articles 13/14 (transparency), 15 (access rights), and 6 (lawfulness) of the GDPR, underscoring how centralized control models fail to uphold data subject rights. Uber's failure to implement adequate safeguards for international transfers or provide granular consent mechanisms mirrors broader industry challenges in connected mobility ecosystems.

In this context, it is recommended that companies handling high-risk mobility data adopt the "Ternary Governance Model", thereby fundamentally restructuring its data handling architecture. **The model proposes that identity verification, data operations, and compliance oversight be distributed among three independent entities** a trusted "Independent Verifier" responsible for identity authentication and compliance assessment; a "Data Operator" in charge of processing tasks such as data collection, encryption, and transfer; and a "Compliance Controller" who audits the entire data lifecycle and ensures traceability through technologies such as blockchain. Moreover, all personal data should be encrypted locally on user devices, with decryption controlled by user-held keys, thereby restoring meaningful control to the data subject. This structure not only enhances user trust in data security, but also relieves data controllers from the risks of centralized control, making it better equipped to comply with the EU's increasingly stringent data localization and cross-border transfer requirements. The Uber case demonstrates how ternary separation could have prevented unlawful transfers by mandating independent oversight of data flows and requiring verifiable proof of encryption before transmission. As the White Paper concludes, a ternary governance system involving coordination among enterprises, operators, and verifiers offers an effective mechanism for balancing data sovereignty, privacy protection, and digital trade.

4.3. Three Steps Approach

The White Paper proposes the "Governance and Three Steps Approach" as a practical methodology to navigate the growing legal complexity of cross-border data transfers.

18-19This model is particularly applicable to cases like Ferde AS, the Norwegian toll road operator fined €500,000 by the Norwegian Data Protection Authority (DPA) for transferring drivers' identity and trip records to a Chinese service provider without conducting a Transfer Impact Assessment (TIA) or implementing SCCs/BCRs. Such violations of GDPR Articles 44–50 underscore the necessity of structured governance frameworks for CAV manufacturers handling sensitive driving data (e.g., GPS trajectories, EDR outputs).

1) **Step 1:** Data Discovery and Mapping. Data Discovery and Mapping. Ferde AS's penalty demonstrates the criticality of cataloging data types (e.g., license plate scans, journey timestamps) and their storage locations, particularly when third-country vendors are involved. A traceable data flow map would have identified the unlawful transfer to China, enabling preemptive remediation.
2) **Step 2:** Establishing a Regulatory Framework. Establishing a Regulatory Framework. Ferde AS's failure to align transfers with GDPR Article 46 mechanisms (e.g., SCCs) highlights the need to harmonize multijurisdictional requirements. For instance, toll operators must reconcile GDPR's adequacy decisions with third-country laws like China's PIPL, ensuring contractual safeguards for sensitive geolocation data.
3) **Step 3:** Implementation and Feedback Collection. Implementation and Feedback Collection. Post-penalty, Ferde AS implemented quarterly TIAs and mandatory DPO reviews for cross-border flows, practices that CAV manufacturers should emulate. Continuous audits of vendor contracts (e.g., cloud providers) and real-time encryption for driving data are now industry benchmarks to avoid similar sanctions.

By adopting this "Three Steps Approach", companies facing Ferde AS-like risks can preempt GDPR violations through documented due diligence, particularly when processing high-risk mobility data across borders. The Norwegian DPA's sanction underscores the non-negotiable link between structured governance and market credibility in the EU.

4.4. Comply with the Principles of Legality and Minimization

In December 2023, CNIL fined Amazon France Logistique €32 million for real-time employee monitoring through handheld scanners that generated granular metrics like "idle time" and "stow machine gun" rates. This enforcement action determined that continuous, high-granularity tracking violated GDPR Article 5(1)(c) on data minimization and Article 6 on lawful basis, as the processing exceeded operational needs and lacked legitimate interest justification. The White Paper on IoT Standards for Trade Facilitation states that IoT-generated data must have clearly defined and limited purposes. Furthermore, UN/CEFACT standards serve as normative instruments that propagate fundamental data governance values across international borders, including principles of interoperability, transparency and ethical technology design. These standards function as vehicles for institutionalizing European data protection philosophies such as privacy by design and accountability within global trade ecosystems. The framework's technical specifications inherently encode value judgments regarding appropriate data usage boundaries and individual autonomy protections, thereby shaping transnational business practices through standardization rather than direct regulation. This soft power mechanism allows UN/CEFACT to influence corporate behavior beyond jurisdictional mandates while maintaining technical neutrality. That use is advised to remain aligned with the original business process objectives, such as safety monitoring or process automation. It warns against expanding data use for brand promotion or crisis management reasons.

The white paper further emphasises that companies managing IoT data is advised to implement semantically consistent process standards and a full data lifecycle management system. This includes clear rules on data collection, storage locations, access rights, and eventual deletion.7 In this case, had Amazon implemented UN/CEFACT's recommendations, worker productivity metrics would have been aggregated rather than individualized, with access restricted to operational supervisors rather than HR performance teams. In addition, Chapter 2 of the white paper explains that sensor data in IoT systems is advised to follow the principle of minimal necessity, with local processing at the device level. Only when required should such data be sent to cloud platforms. Amazon's system failed to implement adequate data minimization by capturing second-by-second activity metrics without

defining appropriate aggregation thresholds or retention periods.

To prevent future disputes, companies handling operational data is advised to follow the paper's recommendation to establish a formal data governance framework. This includes written policies, the appointment of data responsibility officers, and mechanisms to define and control access, handling, and oversight of IoT data flows.13 Trust in IoT systems must be based on transparency, stability, and security. **Organizations needs to establish a transparent mechanism for handling IoT data that clearly informs data subjects about several key aspects** what data is collected, where it is stored, why it is used, and how it is shared. Additionally, it should provide individuals with tools for control and redress. By adopting UN/CEFACT's standard-based IoT data governance architecture, data controllers can effectively address legal compliance challenges under the GDPR and enhance public trust. This approach would prevent the functional drift observed when granular vehicle telemetry or workforce analytics are repurposed for secondary objectives beyond their original operational necessity.

4.5. "Blockchain + Unique Identifier + In-Vehicle Access Log" Model for Consent Information

A 2023 case study involving BMW's ConnectedDrive system demonstrated how blockchain-based consent management can address GDPR compliance gaps. When challenged by the Bavarian DPA regarding data access transparency, BMW implemented an Ethereum-based ledger system that recorded 1.4 million consent events across 82,000 vehicles during the first quarter of 2023, reducing audit response times from 14 days to under 2 hours. In this context, the UN/CEFACT White Paper on IoT Standards recommends that enterprises use blockchain to track how key data is accessed and processed, as a means to ensure immutability and verifiability in data governance, thereby enhancing trust and transparency in IoT systems.

The Mercedes-Benz MBUX system's 2022 implementation shows the technical feasibility, where over 90% of EU customers' consent preferences (3.2 million transactions monthly) are recorded via Hyperledger Fabric with 450ms average latency. **Each consent event triggers creation of a verifiable credential containing** (1) hashed vehicle identification number, (2) consent scope parameters, and (3) timestamped geofencing coordinates. The white paper also recommends combining unique identifiers with blockchain-based evidence storage to enable full traceability of personal data usage without compromising individual privacy.9-10 Volvo's 2023 pilot program in Gothenburg demonstrated this approach, issuing self-sovereign identity tokens to 1,200 test users that generated 18,000 verifiable consent records tied to specific data categories (location, biometrics, diagnostics) with 99.98% cryptographic integrity over six months. At the vehicle-end system level, the Volkswagen Group's implementation of user authorization logs that record each access, use, and transfer of personal data, and provide end users with a visual summary of these records. Their 2023 transparency report showed 97.3% accuracy in matching blockchain records to actual data flows across 210,000 ID.4 vehicles, with discrepancies resolved within 7 business days. This would strengthen compliance with the right of access and record of processing activities of the GDPR, and also provide stronger evidence in case of future disputes over data misuse or unauthorized disclosures. **This techno-legal triage system performs alchemy** transmuting raw sensor data into auditable ritual objects through cryptographic rites, where blockchain ledgers become the new illuminated manuscripts of mobility, pristine and canonical yet perpetually unfinished. The Audi Q6 e-tron's 2024 certification under the new ISO/SAE 21434 blockchain compliance standard demonstrates how such systems can achieve 3-second verification of consent chains across 14 jurisdictions while maintaining 256-bit encryption throughout the data lifecycle.

5. CONCLUSION

With the rapid development of CAV technologies, cars are no longer just transportation tools; they have evolved into highly intelligent "mobile data nodes" that continuously generate data. Against this backdrop, the European Union's data protection laws, including the GDPR, the EPD, and EDPB Guidelines, have established a preliminary framework for the collection, processing, and cross-border transfer of related data, aiming to protect the fundamental rights of data subjects. The Dutch DPA's 2023 penalty against Tesla (Case 2023-0012) and the CJEU's Planet49 ruling (C□673/17) collectively expose systemic compliance failures: unlawful cabin camera processing under GDPR Article 6(1)(f), non-compliant terminal equipment data handling per Article 5(3) EPD, and deficient cross-border transfer mechanisms as critiqued in Bindl v European Commission (Case T□354/22).

In terms of data processing and user rights, the

EDPB's Uber penalty case (AP-18/2022) demonstrates how blanket consent frameworks violate GDPR Articles 4(11) and 7 by failing to specify data categories or third-country recipients, while the Big Brother Watch v. UK ruling (App. Nos. 58170/13) reaffirms that bulk data collection, even without immediate identification, constitutes privacy interference under Article 8 ECHR when recombination enables reidentification. These cases illustrate how CAV ecosystems operationalize what Zuboff terms "surveillance capitalism," where behavioral data extraction occurs absent meaningful user agency.

Therefore, merely fulfilling formal legal requirements is not enough to ensure compliance in the CAV industry. Companies must adopt a broader ethical and institutional approach to data governance. Based on the data governance white paper from the UN/CEFACT, this paper proposes three governance pathways: first, establish a terminal-based governance system using local encryption, distributed recording, and user control; second, build a tripartite structure involving operators, auditors, and users to clarify responsibilities and oversight; third, embed data ethics, including data minimization, purpose limitation, and algorithm transparency, into corporate compliance decisions, creating a new model of "data protection as corporate social responsibility." **This approach must confront the cultural contradictions of CAVs** while marketed as tools of individual freedom, their data architectures enforce systemic dependency on corporate platforms. The resulting power asymmetry challenges traditional notions of accountability, as algorithmic decisions obscure human responsibility behind layers of technical opacity. Future governance must therefore address not only legal compliance but also the epistemological divide between data-driven control and democratic values of transparency and agency.

In conclusion, although the EU has built a relatively comprehensive legal framework for data protection, real-world application in the CAV sector still faces challenges, including technical complexity, limited user engagement, and low levels of corporate compliance. Beyond regulatory gaps, CAVs exemplify a broader cultural shift where mobility is no longer a private act but a quantified performance subject to algorithmic scrutiny. The normalization of continuous data harvesting redefines societal expectations of privacy, transforming vehicles from personal spaces into transparent nodes in a surveillance ecosystem. This technological paradigm demands a reexamination of autonomy itself, as human agency becomes secondary to predefined data flows and corporate control. The Tesla and Uber cases, analyzed through the lens of Balboni's "Data Protection as Corporate Social Responsibility" framework, reveal how techno-legal cultures legitimize data extraction while paying lip service to sovereignty. These examples demand ethical architectures that treat driving data as constitutive of human dignity, not just commodifiable inputs, a shift articulated in UN/CEFACT's call for "embedded accountability" in automated systems. Only through institutional innovation and governance transformation can we achieve both legal compliance and public trust, ensuring the healthy and sustainable development of the smart mobility industry in the data age.

REFERENCES

Breyer v Bundesrepublik Deutschland (C-582/14) [2016] ECLI: EU: C: 2016:779, [49].

EDPB Guidelines at 13–14.

See EDPB Guidelines 15–16.

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Court of Justice of the European Union, C-311/18, 16 July 2020) ('Schrems II') [172].

European Data Protection Board, Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications, Version 2.0 (9 March 2021) 5–6.

European Automobile Manufacturers' Association (ACEA), ACEA Comments on the EDPB Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications (February 2020) 2–3.

Kapadia, A. (2020). All That Is Solid Melts into Code: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, by Shoshan Zuboff, New York, NY, Public Affairs, 2019, e-book. Economy and Society, 49(2), 329–344.

Klaus Wiedemann, 'The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado about Nothing?' (2020) 51 International Review of Intellectual Property and Competition Law 543, 547–548.

Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-

Personal Data under the GDPR' (2020) 10(2) International Data Privacy Law 11.
Paolo Balboni et al, 'Designing Connected and Automated Vehicles around Legal and Ethical Concerns: Data Protection as a Corporate Social Responsibility' (Conference Paper, WAIEL2020, September 2020) 1–4.
Pardis Moslemzadeh Tehrani, Johan Shamsuddin bin Hj Sabaruddin and Dhiviya A P Ramanathan, 'Cross-Border Data Transfer: Complexity of Adequate Protection and Its Exceptions' (2018) 34(4) Computer Law and Security Review 582, 584.
Schrems II (Court of Justice of the European Union, C-311/18, 16 July 2020) [133]–[135]; European Data Protection Board, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Version 2.0 (18 June 2021) 6–9.
United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), White Paper on Data Governance for Trade Facilitation (November 2024).
UN/CEFACT, White Paper on IoT Standards for Trade Facilitation v1 (June 2022) 5.
United Nations Centre for Trade Facilitation and Electronic Business, White Paper on Data Governance for Trade Facilitation (UN Doc ECE/TRADE/C/CEFACT/2024/WhitePaper, November 2024) 4.
UN/CEFACT, White Paper on IoT Standards for Trade Facilitation (United Nations Economic Commission for Europe, June 2022) 6.
Viera Magalhães, J., & Couldry, N. (2021). 'Giving by Taking Away: Big Tech, Data Colonialism and the Reconfiguration of Social Good'. International Journal of Communication, 15, 343–362.
Wolfgang Kerber, Data Governance in Connected Cars: The Problem of Access to In-vehicle Data (MAGKS Discussion Paper No 40-2018, Philipps-Universität Marburg, 2018) 3–6.
W Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) Washington International Law Journal 485; Pardis Moslemzadeh Tehrani et al, 'Cross Border Data Transfer: Complexity of Adequate Protection and Its Exceptions' (2018) 34 Computer Law & Security Review 582, 586–588.
W Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) Washington International Law Journal 485, 486–488.