sustainability

MDPI

Article

Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union

Jozef Andraško [1], Ondrej Hamuľák [2], Matúš Mesarčík [1], Tanel Kerikmäe [3] and Aleksi Kajander [3,*]

[1] Faculty of Law, Comenius University in Bratislava, Šafárikovo Námestie 6, 814 99 Bratislava, Slovakia; jozef.andrasko@flaw.uniba.sk (J.A.); matus.mesarcik@flaw.uniba.sk (M.M.)
[2] Faculty of Law, Palacký University Olomouc, Křížkovského 511/8, 771 47 Olomouc, Czech Republic; ondrej.hamulak@upol.cz
[3] Department of Law, Tallinn University of Technology, Ehitajate Tee 5, 12616 Tallinn, Estonia; tanel.kerikmae@taltech.ee
* Correspondence: aleksi.kajander@taltech.ee

Abstract: The article focuses on the issue of data governance in connected vehicles through a novel analysis of current legal frameworks in the European Union. The analysis of relevant legislation, judicial decisions, and doctrines is supplemented by discussions relating to associated sustainability issues. Relevant notions of autonomous vehicles are analyzed, and a respective legal framework is introduced. Although fully automated vehicles are a matter for the future, the time to regulate is now. The European Union aims to create cooperative, connected, and automated mobility based on cooperation between different interconnected types of machinery. The essence of the system is data flow, as data governance in connected vehicles is one of the most intensively discussed themes nowadays. This triggers a need to analyze relevant legal frameworks in connection with fundamental rights and freedoms. Replacing human decision-making with artificial intelligence has the capacity to erode long-held and protected social and cultural values, such as the autonomy of individuals as has already been in evidence in legislation. Finally, the article deals with the issue of responsibility and liability of different actors involved in processing personal data according to the General Data Protection Regulation (GDPR) applied to the environment of connected and automated vehicle (CAV) smart infrastructure. Based on a definition and analysis of three model situations, we point out that in several cases of processing personal data within the CAV, it proves extremely demanding to determine the liable entity, due to the functional and relatively broad interpretation of the concept of joint controllers, in terms of the possibility of converging decisions on the purposes and means of processing within the vehicles discussed.

Keywords: connected vehicles; autonomous vehicles; GDPR; sustainable data governance

Citation: Andraško, J.; Hamuľák, O.; Mesarčík, M.; Kerikmäe, T.; Kajander, A. Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union. *Sustainability* **2021**, *13*, 10610. https://doi.org/10.3390/su131910610

Academic Editors: Sandra Roger, Carmen Botella-Mascarell and David Martín-Sacristán

Received: 2 August 2021
Accepted: 11 September 2021
Published: 24 September 2021

1. Introduction

Introducing vehicles which perform some or all driving tasks onto public roads has been questioned by several legal institutions, particularly in the areas of liability [1,2], privacy, data protection [3,4], traffic law [5], type approval of vehicles [6,7], legal personality of autonomous systems [8], intellectual property rights [9,10], cyber security [11,12], and additional issues.

The concept of autonomous vehicles greatly influences the concept of smart cities and connected infrastructure, and as a result may aid road safety and ensure the comfort of participants in road traffic. Recent initiatives by the European Union (EU) in the field of creating intelligent transport systems, including the Cooperative Intelligent Transport Systems (C-ITS), cannot be underestimated [13,14] C-ITS will allow road users and traffic managers to share information and use it to coordinate their actions to improve the safety, comfort, and traffic efficiency. At the same time, connected vehicles process personal data necessary for the functioning of the ecosystem as a part of the C-ITS. The aim of the article

is thus to analyze data flow and data governance in autonomous vehicles from the point of view of the current legal framework. The special focus is on the data protection legislation in terms of access and the sustainable governance of personal data in specific user cases.

In summation, the questions "if existing legal frameworks are capable of effectively regulating automated vehicles, and if not, what would the appropriate legal framework look like? How can we ensure sufficient compliance? [15], presented at a University College London (UCL) workshop years ago, are still topical. The authors analyze the lege lata with the aim of gaining a holistic view of a rather complex issue, and highlight the problems that would pave the way to more efficient legislation in the field. As the lege lata has not necessarily been written with automated and autonomous vehicles in mind, analysis and interpretation of the existing legal frameworks required a significant original contribution on the part of the authors to both interpret and apply them to the topic in an appropriate manner. This type of difficulty was especially evident with older legal acts and regulations examined during the research. Thus, the final conclusions represent novel and original interpretations of the existing legal framework and its limitations.

The article highlights legal issues connected to automated mobility in light of the sustainability context. Furthermore, the complex analysis of roles and liabilities in data protection law based on model situations regarding automated mobility is absent from the literature and the official guidelines provided.

The first part of the article introduces the concept of autonomy per se in vehicles and specifies the relevant notions in connection with autonomous and connected vehicles. What is more, the legal framework of connected vehicles and C-ITS-related legislation is discussed at an EU level. Secondly, the role of autonomous vehicles in the system is explained, and sustainable data governance analyzed. The third part of the article deals with data protection issues of autonomous vehicles in light of the General Data Protection Regulation (GDPR) and responsibility/liability aspects.

Materials and Methods: Analyzing the Lege Lata

The focus of this paper was chosen as the existing legal framework of the European Union, owing to its declaration and commitment to an ambitious strategy for future mobility within the European Union utilizing connected and automated vehicles [16,17]. As a result, while the vehicles themselves may still be some time off in the future, the time for regulation is arguably now, so that shortcomings of the current legal framework may be resolved in time for their introduction.

In this vein, there is a need to further analyze legislation at the level of EU law that regulates the issue of autonomous vehicles, especially from the point of view of cybersecurity and personal data protection. In particular, we examine whether the legislation in place already imposes requirements on the security of automated or autonomous systems, so that they could become sufficiently secure in sustainable communication with other entities and that the integrity, confidentiality, and availability of information would not be compromised. In addition, the question of whether the legislation enables sustainable road infrastructure governance, e.g., in the form of intelligent traffic signs, and sufficiently regulates the issue of personal data protection and cybersecurity in the context of communication with vehicles is addressed.

Moreover, the article explores the current EU legal framework that is relevant for the social aspects relating to the concept of sustainable data governance for connected autonomous vehicles. In this context, the human rights legal framework applicable for EU Member States is included in addition, owing to its significance for social matters that can be argued to be within the scope of social aspects of sustainable data governance for connected autonomous vehicles. In this regard, the question of which social values are crucial for sustainable data governance of connected autonomous vehicles can reasonably be derived from the existing legal framework, and their potential implications analyzed.

2. Automated Systems and Autonomous Systems

"Automated vehicle", "autonomous vehicle", "self-driving vehicle", or "driverless vehicle" are terms that are most often associated with the concept of a vehicle where some or all driving tasks are performed by the vehicle itself. In particular, vehicle systems perform driving tasks which are the essence of vehicles capable of performing all or some of the driving tasks without intervention of the driver. The systems in question can be divided into automated and autonomous.

One way to distinguish between an autonomous system and an automated system is to focus on their ability to adapt, learn, and make decisions that are integrated into the system. Automated systems usually operate based on predefined parameters and are very limited in what tasks they can perform. On the other hand, an autonomous system learns to adapt to a changing environment and evolves as the environment changes. Data forming the basis for them learning is also beyond what was expected when the system was introduced [18].

The autonomy of the system cannot be perceived in terms of absolute independence and self-initiative. Most autonomous systems are dependent on humans for their tasks and activities. If we look at it from a different perspective, automated systems perform specific tasks with well-understood parameters that are known in advance. It is designed to perform a specific function repeatedly and efficiently. An autonomous system advises and helps define what is the right decision or action in an evolving environment, which is not predetermined [18].

A typical example of an autonomous system is an autonomous vehicle. According to Polčák, autonomous vehicles cannot be compared to classic cars from a legal point of view, especially given the fact that autonomous vehicles drive themselves. We find that for the case of autonomous vehicles, the analogy with the car should sooner not be used. Instead, it is better, and correct, to compare it with the software that manages such a system [8].

A specific example of an automated system is infrastructure and application-level compliance checks within a corporation's environment. These systems monitor compliance with a well-defined set of compliance standards and inform responsible institutions when systems do not comply. These systems can also perform well-defined actions to correct a problem, but this does not mean that they are autonomous. They are explicitly configured to take specific actions, giving the administrator confidence in what exactly is happening to their environment. These systems often indicate a problem so that the user or administrator can potentially solve the problem. It is an assistive technology that helps a person do their job but does not replace them [8].

An example of an autonomous system is network intrusion detection, searching for anomalies in otherwise normal network traffic. Autonomous systems are also used to search for zero-day exploits. The Roomba smart vacuum cleaner is a proper example of an autonomous system application. Its function is to clean the floor, but based on feedback from the surrounding environment, it decides where exactly to carry out the cleaning process. When approaching objects, it learns how to avoid them over time, and compiles a map of the space it is cleaning. The technology must constantly learn because furniture, other objects, and, perhaps, pets change the environment it operates in [8].

Autonomous systems cannot be identified merely as single-task software, for one sole task. Autonomous systems are programmed not only to perform certain activities, but also to learn to perform certain activities themselves. In other words, the essence of autonomous systems is not only the ability to exist and function autonomously but also to create their own codes (software) independently of their authors [8].

The autonomy of the system cannot be perceived in terms of absolute independence and self-initiative. Most autonomous systems are dependent on humans for their activities. The functioning of autonomous systems is largely influenced by the input data it obtains from its surroundings (e.g., incorrect traffic signs, outdated maps, etc.), based on which it learns and changes its behavior. Incorrect or harmful data may adversely affect functioning of an autonomous system. In this case, it is a so-called data poisoning attack. The driver of

an autonomous vehicle that uses autonomous systems cannot influence incorrect data that the autonomous system misinterprets.

The term "autonomous" has long been used in robotics and artificial intelligence research communities to refer to systems that have the ability and authority to make independent and self-sufficient decisions. Over time, this use has randomly expanded to include not only decision-making, but also functionality of the entire system, making it synonymous with automation.

In jurisprudence, autonomy also applies to the capacity for self-governance. In this sense, the term "autonomous" could be considered a noncorrect notion, as even the most advanced automated driving systems are not "self-driving". Automated driving systems tend to work based on algorithms, and follow user commands. For this reason, the SAE J3016:Sep 2016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (hereinafter referred to as the "SAE standard") does not use the term "autonomous" to describe driving automation [19] (Point 7.1.1.).

Automated driving systems are defined as the hardware and software that are collectively capable of performing the entire dynamic driving tasks on a sustained basis, regardless of whether it is limited to a specific operational design domain; this term is used specifically to describe a level 3, 4, or 5 driving automation system [19] (Point 3.2).

The term "automated driving system" is also defined in the United Nations Economic Commission for Europe Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic as *"a vehicle system that uses both hardware and software to exercise dynamic control of a vehicle on a sustained basis"* [20].

2.1. Automation Levels

Automated vehicles are classified based on their level of automation. According to the SAE standard, automated cars are divided into six increasing levels of automation. These levels are considered as descriptive rather than normative, and technical rather than legal. In general, SAE levels primarily identify how the "dynamic driving task" is divided between a human and a machine. At level 0 (no automation), it is performed entirely by a human driver, and at level 5 (full automation), entirely by an automated driving system [21].

- Level 0 (no automation). The human driver performs all tasks associated with driving.
- Level 1 (driver assistance). The human driver controls the vehicle, but minor driving tasks are performed by the system. Examples: park assistant or cruise control.
- Level 2 (partial automation). The system, or more systems, handle the steering and speed of the vehicle while the human driver must monitor dynamic driving tasks and the surrounding environment at all times. Examples: the self-parking feature, lane-keeping system, emergency braking systems.
- Level 3 (conditional automation). Vehicles in level 3 and above are considered vehicles with automated driving systems. The vehicle monitors the driving environment through automated driving systems. The human driver does not need to monitor dynamic driving tasks but must be able to take control of the vehicle without notice at any time at all. The vehicles can make decisions themselves, e.g., the vehicle can see a slower moving vehicle in front and can decide whether to decelerate or overtake. Example: highway pilot.
- Level 4 (high automation). The vehicle can perform all driving tasks under some conditions (specific driving modes). The human driver can take control of the vehicle, in particular when conditions confuse predefined user cases (e.g., road works, road diversions, or when the human driver wishes to). Examples: urban mobility as taxi services and public transport services [22–24].
- Level 5 (full automation). No human driver is required. Automated driving systems handle all aspects of the driving task without the human needing to intervene in any scenarios at all. The vehicle does not need any pedals or a steering wheel. Automated driving systems make independent decisions. The vehicle can manage situations

when unpredictable events occur, or the physical environment changes. A suitable example here would consist of a full end-to-end journey [25] (pp. 4–5) [26].

2.2. Automated Vehicle and Autonomous Vehicle

In general, autonomous vehicles can be described as "computer-controlled vehicles that drive themselves by relying on a number of data resources to access the driving environment and to control the operation of the vehicle" [3]. However, not all vehicles equipped with technologies that can handle some or all driving tasks are considered autonomous vehicles.

Autonomous vehicles are able to make decisions independently of human intervention. Furthermore, autonomous vehicles rely on sensor data and artificial intelligence to interpret data, make decisions about vehicle operations, and adapt to changing conditions [27] (p. 3).

The necessity of using artificial intelligence in autonomous vehicles has also been emphasized by the author Ducuing, according to whom, in order to be able to delegate decisions in the field of vehicle operation to an autonomous vehicle, artificial intelligence must be used [7] (p. 189).

Autonomous vehicles are vehicles with systems that can handle all driving tasks under all conditions, automatically, in real time. In this case, we talk about full automation when the vehicle has no steering wheel or pedals. No driver input is required, and all occupants in a vehicle are considered passengers. Autonomous vehicles are vehicles at level 5 of the SAE standard [28] (p. 10).

On the other hand, the automated vehicle can be described as a vehicle using driving automation systems or automated driving systems that can handle some or all dynamic driving tasks within its operational design domain. The driver must be available, promptly, to take control of the vehicle.

Legal definitions of an autonomous vehicle or automated vehicle can be found in EU legislation [13,14,16,29], in the laws of EU Member States, or the United States. Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles and their trailers, and systems, components, and separate technical units intended for such vehicles, with regards to their general safety and the protection of vehicle occupants and vulnerable road users (hereinafter referred as "Regulation 2019/2144") [30], defines an automated vehicle as a motor vehicle designed and constructed to move autonomously for certain periods, without continuous driver supervision but in respect of which driver intervention is still expected or required [30] (Art. 3 (21)).

The regulation in question does not mention the concept of the autonomous vehicle, but rather a fully automated vehicle. In this regard, a fully automated vehicle means a motor vehicle that has been designed and constructed to move autonomously without any driver supervision [30] (Art. 3 (22)). Furthermore, automated vehicles and fully automated vehicles must comply with additional specific technical specifications set out in the Commission implementing act. The Commission implementing act will specify technical specifications that relate to: [30] (Art. 11 (1))

(a) *Systems to replace the driver's control of the vehicle, including signaling, steering, accelerating, and braking.*
(b) *Systems to provide the vehicle with real-time information on the state of the vehicle and the surrounding area.*
(c) *Driver availability monitoring systems.*
(d) *Event data recorders for automated vehicles.*
(e) *Harmonized format for the exchange of data, for instance, for multi-brand vehicle platooning.*
(f) *Systems to provide safety information to other road users.*

However, those technical specifications relating to driver availability monitoring systems [30] (Art. 3(23)) will not apply to fully automated vehicles [30] (Art. 11 (1)).

At European Member State level, on 21 July 2017, an amendment to the German Road Traffic Act (*Straßenverkehrsgesetz*-StVG) came into force regulating the subject of motor vehicles with highly or fully autonomous driving functions on German public roads.

Vehicles with highly or fully autonomous driving functions within the meaning of the German Road Traffic Act correspond to level 3 and level 4 of autonomous vehicles in terms of the autonomy of autonomous vehicles introduced in the SAE standard J3016: Sep 2016. Motor vehicles with highly or fully automated driving functions within the meaning of the German Road Traffic Act are those containing technical equipment which:

- "Is able to perform, after activation, the driving task-including longitudinal and lateral control-for the respective motor vehicle (vehicle control);
- Is able to comply with the traffic regulations applicable to the vehicle driving task during highly automated or fully automated driving;
- Can be manually overridden or deactivated by the driver at any time;
- Is able to recognize the necessity of manual vehicle control by the driver;
- Is able to visually, acoustically, tactilely, or otherwise perceivably notify the vehicle driver of the requirement to pass vehicle control to the driver with sufficient reserve of time ahead of passing control; and
- Notifies of use that is contrary to the system's description." [31]

The amendment to the German Road Traffic Act also introduces compulsory fitting of a black box to vehicles with highly or fully autonomous driving functions. In the event of an accident, the black box identifies whether the driver or system was controlling the vehicle at a given moment, and therefore clarifies whether the responsibility lies with the driver or potential manufacturer [31].

Automated and Electric Vehicles Act 2018—adopted in the United Kingdom, it does not define autonomous vehicles, but rather automated vehicles. An automated vehicle is a vehicle designed, or adapted to be capable, in at least some circumstances or situations, of safely driving itself that may lawfully be used when driving itself, at least in some circumstances or situations, on roads or in other public places in Great Britain.

2.3. Connected and Automated Vehicles

The full benefits of automated and autonomous driving, however, are realized when the vehicle is also capable of communicating with other vehicles and other objects, such as infrastructure, etc. In that regard, these vehicles are considered connected vehicles.

Connected vehicles can be described as vehicles equipped with wireless communication technologies that enable data transfer with other vehicles, infrastructures, or other networks [32] (p. 3).

In cases where automated vehicles are equipped with communications technology that enables data transfer with other vehicles, infrastructures, or other networks, the notion should rather be the connected and automated vehicle (hereinafter referred to as CAV) [32] (p. 3). Automated vehicles do not necessarily need to be connected, and connected vehicles do not require automation. However, connectivity will be a major enabler for driverless vehicles [16] (p. 4). For this article, we will use the term CAV or its plural (CAVs). If we want to highlight a fully autonomous vehicle, we will use the term autonomous vehicle.

The EU Communication on the road to automated mobility states: An EU strategy for mobility of the future. When vehicles become increasingly connected and automated, they will be able to coordinate their maneuvers, using active infrastructure support and enabling truly smart traffic management for the smoothest and safest traffic flows [16] (p. 4) CAVs rely on data that is created by their in-vehicle technologies, data that is sent from other vehicles or infrastructure, and traffic and infrastructure data sent from public authorities. CAVs must function properly to observe their conditions and surrounding environment. Different types of in-technologies are used in CAVs for these purposes. In general, there are three types: [11]

(a) Sensor technologies. Sensor technologies include radio detection and ranging (RADAR), light detection and ranging LiDAR), visible light communication (VLC), infrared systems [25] (p. 11), etc.
(b) Vision technologies. Vision technologies include high-definition (HD) cameras, stereo vision system (SVS) [33] (p. 15), etc.

(c) Positioning technologies. Positioning technologies include the Global Positioning System (GPS), radar cruise control, and radar-based obstacle detection (RBOD) [34] (pp. 186–193).

The technologies mentioned above communicate with other internal components of vehicles such as telematics and actuator by different networks. These networks include Flexray, ethernet networks, controller area network (CAN), etc. [11] (pp. 21–23).

CAVs rely on data that is sent from other vehicles, road infrastructures such as C-ITS stations or traffic lights or signs, or other traffic participants (cyclists, pedestrians). CAVs can also use data from devices used inside the vehicle such as smartphones, tablets, smartwatches, and personal computers. Different types of communication technologies, such as short-range communication technologies operating in the dedicated 5.9 GHz frequency bandwidth, as well as long-range technologies, 3G, 4G, or 5G mobile networks, can be used for these purposes. In that regard, the CAV is the connected entity that receives data from an external source and can share data that is recorded with a remote third party for various purposes. Based on participants in the communication, the concept of vehicle-to-everything includes:

- Vehicle-to-vehicle (V2V).
- Vehicle-to-infrastructure and vice-versa (V2I and I2V).
- Vehicle-to-mobile network (V2N) and infrastructure-to-mobile network (I2N).
- Vehicle-to-device (V2D).
- Vehicle-to-persons (V2P).

Various public authorities responsible for road traffic and road infrastructure create and can provide access to these data under certain conditions. Road traffic information and infrastructure data include dynamic speed limits, traffic rules, the location of stationary vehicles, road names, condition and availability of roads, length of roads, type of roads, road works warnings, number and positioning of traffic lights and signs, etc.

2.3.1. Type Approval

Before vehicles can be released to the market for use on public roads, the vehicle must be type-approved following set administrative procedures and technical requirements. No EU legislation explicitly regulates type approval of autonomous vehicles, but still permits introducing autonomous vehicles to the market only under certain conditions.

Granting approvals for motor vehicles, as well as systems for such vehicles, is regulated at the level of EU law by a regulation on approval and market surveillance of motor vehicles and their trailers, and of systems, components, and separate technical units intended for such vehicles [35] (hereinafter referred to as the "vehicle type-approval regulation"). The regulation on vehicle type approval assumed legal effect on 1 September 2020.

Technologies that are not covered by the vehicle type-approval regulation, such as the automatic control system, may be approved through the exemption procedure provided for in said regulation in Art. 39, regulating exemptions for new technologies or new concepts. In such cases, approval shall be granted based on a national ad hoc safety assessment, subject to authorization by the Commission. The Commission shall adopt implementing acts deciding on granting of the authorization. Pending the adoption of implementing acts, the national approval authority may grant preliminary EU type approval for a vehicle type, covered by the requested exemption. Prior authorization shall be valid only in the territory of the Member State of the approval authority concerned, but the approval authorities of other Member States may accept the EU preliminary type approval in their territory, provided they inform the approval authority granting the EU preliminary type approval in writing [35] (Art. 39).

The vehicle type-approval regulation does not specifically address the issue of personal data protection or cybersecurity [36]. According to recital 62, it is considered important that manufacturers take all necessary measures to ensure compliance with the rules on processing and transfer of personal data arising from the use of a vehicle. When using autonomous

and connected vehicles, where various automated driving systems or communication systems are used, personal data is processed and transmitted.

As there were different approaches to applying exemptions for new technologies or new concepts, the Commission issued guidelines on the exemption procedure for EU approval of automated vehicles ("the Guidelines") on 12 February 2019. The Guidelines aim to harmonize Member States' procedures for national ad hoc assessments of automated vehicles and to facilitate mutual recognition of such assessments, as well as to ensure fair competition and transparency. The Guidelines focus on automated vehicles that can drive themselves in a limited number of driving situations at automation levels 3 and 4 according to the SAE standard [37] (p. 1).

The Guidelines focus on personal data protection and cybersecurity in two parts. Firstly, the Guidelines deal with the issue of installation of event data recorders. In accordance with guidelines no. 23–27, automated vehicles should be equipped with an onboard device that records operational status of the automated driving system and the status of the driver to determine who was driving during an accident. This collected data makes it possible to determine liability in the event of an accident, and to assess whether the driver or vehicle responded correctly to the situation. Among this data, we can consider, e.g., the operating status of the automated driving system, driver status, environmental information, and vehicle control information. The onboard device must be able to store data securely, comply with EU data protection law, and be protected from manipulation while allowing national authorities access to such data. Based on experience gained, more specific requirements for data recording devices can be developed (recording time, retention time, for what purposes the data is used, standardized approach, way of handling personal data, etc.) [37] (p. 5).

The event data recorder is a new safety/security feature in-vehicle according to Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles and their trailers, and systems, components, and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users. Under Art. 3 (13) is the event data recorder a system with the only purpose of recording and storing critical crash-related parameters and information shortly before, during, and immediately after a collision. All motor vehicles will be equipped with an event data recorder when specific requirements will be met according to Art. 6 (4) (5). Detailed rules concerning the specific test procedures and technical requirements for event data recorder and other advanced vehicle systems will be regulated by Commission delegated acts.

The vehicle manufacturer is obliged to provide the following information in accordance with Guidelines:

(a) Type of stored data.
(b) Storage location.
(c) Storage duration.
(d) Means to ensure security and data protection.
(e) Access to the data [37] (p. 9)

In the section on cybersecurity, the Guidelines call for the vehicle to be designed to protect the vehicle against automated hacking, using state-of-the-art techniques, and to comply with EU data protection legislation. This includes, e.g., a manufacturer risk assessment, design measures, and adequate processes to avoid, mitigate, and respond to cyberattacks. Vehicle manufacturers should also adopt measures, such as those relating to software updates, etc., installed in automated vehicles necessary to ensure in-use cybersecurity over the vehicle's lifetime [37] (p. 5).

2.3.2. Intelligent Transport Systems

One of the practical examples where the vehicle can communicate with the Internet of Things (IoT), in particular, is the infrastructure of intelligent transport systems. Examples of applications of intelligent transport systems in road traffic transport include urban

and motorway traffic management and control systems, electronic toll collection, route navigation, etc. The deployment of intelligent transport systems is governed by a directive on the framework for the deployment of intelligent transport systems in the field of road transport and interfaces with other modes of transport (hereinafter "the intelligent transport systems directive") [38]. A high level of security for intelligent transport systems plays an important role in relation to autonomous vehicles. For their operation, autonomous and connected vehicles communicate with various intelligent transport systems. In these cases, data is received from an external source, and recorded data is also shared with remote third parties for various purposes.

In many cases, introduction and use of intelligent transport system applications and services will include processing of personal data. The issue of personal data protection and security is specifically regulated in Art. 10 of the intelligent transport systems directive, according to which processing of personal data must be carried out in accordance with both GDPR and the ePrivacy Directive [39]. Member States are also required to protect personal data against misuse, including unlawful access, alteration, or loss.

When using intelligent transport system applications, purpose limitation and data minimization principles should be applied, and anonymization should also be promoted as one of the principles to enhance the privacy of individuals [38] (Art. 10).

From the point of view of communication between vehicles and road infrastructure, cooperative intelligent transport systems play a crucial role. These systems use technologies that allow road traffic vehicles to communicate with each other and with the road infrastructure, including traffic signals. The Commission adopted a proposal for a delegated regulation supplementing the intelligent transport systems directive concerning deployment and operational use of cooperative intelligent transport systems (hereinafter referred to as the "Delegated regulation") in March 2019 [40].

In road transportation, cooperative intelligent transport systems usually include vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or infrastructure-to-infrastructure (I2I) communication and vehicle-to-pedestrian or cyclist communication (vehicle-to-everything, V2X) [40] (p. 1). Cooperative intelligent transport systems services are a category of intelligent transport system services based on an open network that enables a many-to-many or peer-to-peer relationship between stations of cooperative intelligent transport systems (hereinafter referred to as C-ITS stations). This approach means that all C-ITS stations can exchange messages securely with each other and are not limited to exchanging messages with (a single) predefined station(s) [40] (Recital 2). C-ITS stations are defined as *the set of hardware and software components required to collect, store, process, receive, and transmit secured and trusted messages to enable the provision of a C-ITS service* [38] (Art. 2(3)).

According to the Delegated regulation, C-ITS stations can be installed on vehicles, handheld, or alongside the road infrastructure, and are considered as products that can be placed on the market as standalone units and assemblies or as part of larger assemblies [40] (Recital 15). Under recitals 25 and 26 of the Delegated regulation, information relating to an identified or identifiable natural person should be processed in strict compliance with the principle of data minimization, only for purposes specified in the Delegated regulation. They should also only be stored as long as is necessary. The security requirements for pseudonymization set out in the Delegated regulation contribute to reducing risks of data misuse. End-users should be clearly and comprehensively informed of all relevant information regarding processing of their personal data in accordance with the GDPR.

The Delegated regulation deals in detail with the issue of security in Chapter V, which regulates the security of C-ITS stations. An EU system for managing security mandates for coordinated intelligent transport systems is being set up, which must meet the requirements of the certification policy (Annex III) and security policy (Annex IV), which sets out the requirements for information security management in coordinated intelligent transport systems [40] (Art. 23).

Each C-ITS station operator shall operate an information security management system under ISO/IEC 27001, and the additional requirements set out in point 1.3.1 of Annex IV

of the Delegated regulation [40] (Article 27). In connection with C-ITS stations, we must realize that even in the case of V2I communication, there will always be an exchange of messages between individual C-ITS stations. Therefore, for a vehicle to communicate with other C-ITS stations, such a station must be installed on the vehicle.

3. Sustainable Data Governance in CAV

CAVs can receive, produce, process, and transmit a huge amount of data. First of all, this data includes in-vehicle data that is produced via sensor technologies, vision technologies, positioning technologies, and within vehicle control units. More specifically, in-vehicle data include technical data about the vehicle (information about speed, acceleration, air temperature, fuel level, etc.), data about road traffic conditions, data about weather, data about driving behavior, and even data about the health status of the driver [6] (p. 247).

In-vehicle data helps to ensure correct operation of the vehicle, checks proper functioning, identifies and corrects errors, and refines and optimizes vehicle functions. This data can be used for different purposes, such as repair and maintenance, road safety and traffic management, fleet management, quality management, product development, and nonautomotive uses (e.g., car sharing, car rental, insurance) [41] (p. 3).

This data can be processed in the vehicle and, under some circumstances, exchanged via communication technology with other vehicles, infrastructures, and vehicle manufacturers. Secondly, CAVs can receive data from external sources (e.g., roadside units, other vehicles). Last, but not least, data imported (e.g., telephone contact lists, destinations for navigation) are produced by the driver and passengers (websites visited, online shopping preferences, etc.) are included.

Vehicle-generated data and data produced by the driver or passengers are valuable not only to vehicle manufacturers, but also for public authorities (e.g., road traffic data) and entities who would like to provide services to car users (e.g., automotive aftermarket services, online shopping providers, insurance companies, etc.) [6] (p. 248). Furthermore, vehicle-to-pedestrian (V2P) communication also forms an important part of communication mechanisms alongside vehicle-to-network (V2N) communication, known collectively as vehicle-to-everything (V2X) [42]. In addition, in general, there is a distinction between passenger car deployment paths and freight/urban mobility deployment paths, with the authors focusing mainly on the second direction [43].

CAV data creates new innovative services in the field of vehicle repair and maintenance (remote monitoring of vehicle operation, remote diagnostics, remote and predictive maintenance, and repair services), navigation services, parking apps, online shopping, or insurance services. However, access to in-vehicle data and the vehicle's own resources is required in order to provide these services. In some cases, access to real-time vehicle data is even required Access to in-vehicle resources includes IT systems, sensors, telematics systems, and the human-machine interface (dashboard). In cases of remote diagnostics, remote and predictive maintenance and repair services not only reading (downloading data) but especially writing data for updating or reconfiguring of software is necessary [6] (p. 248); [44].

From a technical point of view, there are different concepts for accessing in-vehicle data. Firstly, the extended vehicle concept is used widely, by many different vehicle manufacturers. The extended vehicle concept allows access to vehicle data via different types of interface, depending on the purpose for which access is sought. The initial concept in question includes onboard diagnostic (OBD) interfaces, where data for diagnosis and repair purposes can be accessed. Secondly, vehicle data can be accessed via a web interface for third-party services. Data generated in-vehicle is transferred via a secure and encrypted communication channel (e.g., mobile telecom network) to a proprietary external server of the vehicle manufacturer. In this regard, vehicle manufacturers have exclusive, direct, full, and privileged control of data on their proprietary server and over who is granted access to the data. Transferred data is usually in a filtered and aggregated form. Vehicle manufacturers also have privileged, direct access to the driver's dashboard (human–machine interface, HMI). Access to vehicle data and using it will require a business-

to-business (B2B) agreement between the service provider and vehicle manufacturer. Last, but not least, the extended vehicle concept includes an ad hoc communication interface under the responsibility of the vehicle manufacturer (e.g., transfer of data for purposes of intelligent transport systems) [41] (pp. 3–5); [14] (p. 45).

Secondly, the shared data server concept is based on the idea that a neutral entity controls the server and can grant nondiscriminatory access to vehicle data. Data made available to the shared data server will be of the same quality as data available on the vehicle manufacturer´s proprietary server. However, vehicle manufacturers will decide which data will be transferred from their proprietary server to the shared server. The vehicle manufacturer is privileged to display services to the consumer directly via vehicle HMI [41] (pp. 3–5) [14] (p. 205).

Thirdly, onboard application platforms. With this technical solution, the vehicle is considered as a platform where data is stored in the vehicle. The car owner must decide who to grant access to in-vehicle data to, and who is allowed to provide services directly to the user of the car. This platform should support different functionalities directly from the HMI [44] (p. 313).

Vehicle manufacturers are strictly against the onboard application platform, because of security and safety concerns that may arise by granting a third party uncontrolled access to vehicle data and resources. In this regard, vehicle manufacturers are willing to grant access to specific vehicle data to third parties, based on a B2B contract, once strict requirements for data security and product safety are met [41] (pp. 3–5) [14] (pp. 5–7).

At an EU level, access to and uses of in-vehicle data are frequently under discussion, especially as a part of a cooperative intelligent transport system platform. The Commission´s final report on access to in-vehicle data and resources defined five guiding principles that should apply to access to in-vehicle data and resources. According to one of these principles, the vehicle user (data subject) decides if data can be provided and to whom, including the concrete purpose for using the data. Another principle states that all service providers should be in an equal, fair, reasonable, and nondiscriminatory position to offer services to the vehicle's user [14] (p. 150)

Current EU legal regulation of access to vehicle-generated data deals with access to OBD vehicle information [16] (Art. 3(49) and vehicle repair and maintenance information [16] (Art. 3(49)), rather than general access to vehicle-generated data or data produced by vehicle users. Vehicle manufacturers are obliged to provide unrestricted, standardized, and nondiscriminatory access to vehicle OBD information and vehicle repair and maintenance information to independent operators [16] (Art. 3(45)) Nondiscriminatory access also applies to remote diagnostic services used by vehicle manufacturers and authorized dealers and repairers. However, this must be interpreted so that independent operators do not have remote access to in-vehicle data and resources, but, rather, have access to the results of diagnostic services. Therefore, independent operators are not allowed to provide repair and maintenance services. Additionally, information will be presented in an easily accessible manner in the form of machine-readable and electronically processable datasets [16] (Art. 61(1)).

The issue of data access has been widely discussed by Kerber and other commentators [6,44–46]. Kerber discusses two solutions for access to data processed within a CAV—the right to data portability in Article 20 GDPR, and introduction of a new property-like right to access [44] (pp. 326-327). However, these solutions might not entirely fit the data access requirement. Firstly, the right to data portability is strictly limited in terms of legal grounds and the data itself. Article 20 GDPR does not apply to aggregated personal data. Right to portability may be taken up only in case of data provided by data subjects or observed by the controller [47] (p. 10). Additionally, the right in question when personal data is processed is limited by legal grounds of consent or performance of contracts. If the provider of CAV processes personal data on the legal ground of legitimate interests (e.g., for the purposes of maintenance, development, or other purposes), the right to data portability does not apply [48] (Art. 20(1)) [49]. Kerber also adds technical feasibility of

data as a problem that may further hinder application of Article 20 GDPR [44] (pp. 326–327) Secondly, introducing a binding property-like right for machine-generated data has been not recommended by the European Commission [50].

However, the issue of access is not relevant in cases where the entity is the controller of personal data, as it processes data on its own behalf and under its own accountability and liability. The only applicable case of access, thus, shall be where public authority exercises powers in the public interest to investigate traffic incidents or maintain C-ITS.

In order to achieve the goal of full automation, it will be necessary to provide easier access to in-vehicle data. In this regard, we shall need to define categories of data that can be made available. Furthermore, the purpose for which it is used and whether these data are used for public or commercial interests must be considered.

Sustainable Social Data Governance for Connected Autonomous Vehicles

Future-oriented sustainable smart cities often incorporate connected autonomous vehicles as a central part of their vision of becoming sustainable [27] (p. 1), and, as such, the concept of sustainability becomes interconnected with vehicles as a result of the association. However, in the field of smart cities, the concept of "sustainability" often goes beyond purely environmental concerns such as more efficient energy usage and less pollution, but rather there are additional significant social and cultural aspects to sustainability [51] (p. 3); [52,53]. Consequently, when discussing the sustainability of connected autonomous vehicles, the "social" and "cultural" sustainability aspects that relate to data associated with such vehicles and go beyond the scope of protecting privacy should not be overlooked as it may otherwise be overshadowed.

Sustainability in this social context has been considered as including social and cultural values [54] (pp. 5–6). In this context, there are several aspects of connected autonomous vehicle data that are relevant, which, if left unaddressed, may erode arguably important social and cultural values by replacing human decision-making with artificial intelligence (AI). Perhaps chief among them, besides privacy, is autonomy, which is relevant in the context of connected autonomous vehicles and has been described as an "underdog", due to a lack of consideration [55]. Not only is it relevant in the sense of the individual having freedom to determine the course of their life and make their own ethical, religious, and moral decisions, but additionally in terms of an individual having the right to not be subject to purely automated decision-making for significant life-altering decisions.

The connection here being that, while the international law(s), which can be argued to constitute the right to autonomy in the face of AI, were not written with automation in mind, their combination could be considered to produce such a right. Autonomy can be defined at an individual level as actions "endorsed by the self", which includes acting in accordance with one's own values [56] (p. 32). This applies in the context of autonomous vehicles, as inevitably the autonomy of a self-driving vehicle may present a threat to the personal autonomy of an individual in cases of life-and-death decisions, which would effectively be automated. In such life-and-death situations, fundamental philosophical questions relating to ethics, religion, and opinion arise. The rights to hold opinions and manifest beliefs are already protected under, for example, the Universal Declaration of Human Rights Articles 18 and 19, or Articles 9 and 10 of the European Convention on Human Rights (ECHR), thereby implying by extension a right to manifest them in the context of life-and-death decisions relating to autonomous vehicles.

Consequently, for the purposes of this article, the right to autonomy in the context of autonomous vehicles can therefore be considered as deriving from the combined effect of the right to hold opinions, religious and ethical beliefs, and to manifest them through choices, rather than to be purely subject to decisions reached by AI on matters that have a significant effect on the individual. This definition, while it narrows the concept of "autonomy" significantly, is a necessary limitation in the scope of this article as it limits the discussion to what is directly derivable from the existing legal framework. Were this limitation not put in place, the resulting conclusions would not have the solid foundation

of the relatively uncontroversial interpretation of the existing ECHR rights as above, i.e., that a right to hold opinions and manifest beliefs exists. While such a right to autonomy in the face of AI decision-making, such as is found in autonomous vehicles, does not exist directly, it is not reasonable to envision that a "sustainable" data governance model for autonomous vehicles would ignore these fundamental rights and values. For if the user of the autonomous vehicle cannot, for example, manifest the opinion or belief that their vehicle should primarily protect (or sacrifice) the user, it is difficult to envision this as a sustainable model, as it would significantly erode fundamental and established social and cultural values that are incorporated into human rights laws.

Moreover, this modern derivation of the right to autonomy is perhaps not as abstract as it may appear, as it is already somewhat included in the current EU legal framework, albeit in a different context than autonomous vehicles, but arguably the underlying principle is the same. The right to not have decisions based solely on automatic processing which produce legal effects, or are likewise significant, is already included in the GDPR in Article 22 (1). Therefore, at its core, Article 22 is intended to protect individuals from having their life's direction altered solely by automated decision-making, at least within the scope of the GDPR. Considering that, if being denied a loan by AI is considered significant enough to be specifically mentioned as a life-changing decision [48] (Recital 71), it is unreasonable to suggest that the decision to sacrifice the occupants of an autonomous vehicle would not similarly be such a "significant" decision. As a result, it is logical to suggest that this and similar provisions are there to sustain the concept of autonomy for individuals in a world that is changing, by giving automated decision-making increasing authority and with increasingly grave consequences. Moreover, initiatives already exist that call for the fundamental right of humans to make major decisions [57]. Therefore, considering such concerns in the context of autonomous vehicles to make them more sustainable is arguably warranted.

This lack of "social" and "value" sustainability in data governance of autonomous vehicles is already perceptible to some extent. For example, there are already declarations by (future) manufacturers of autonomous vehicles that they will have made life-and-death decisions for the owner [58]. This already implies that due consideration has not been given to the concept of autonomy of the user or occupant, as they are deprived of the possibility to manifest their beliefs and opinions. Furthermore, this implies the need to definitively "translate" and apply the human rights, which can be collectively said to constitute a right to autonomy in the face of autonomous decision-making, specifically to the context of autonomous vehicles, since presently the connection appears too abstract, as it has already been ignored. Considering that this is a question of risks to life and limb that may determine the course of a person's life, the right for everyone to determine their preferences should not be glossed over or ignored, owing to its potentially grave ramifications.

Hence, the preservation and thus, "sustainability" of social values, such as the autonomy of individuals, needs to be considered in data governance of autonomous vehicles. Proceeding with the right to maintain one's autonomy even when using an autonomous vehicle, the data governance implications of preserving such social values becomes increasingly apparent. For example, as has been mentioned previously, autonomous vehicles will reduce the number of accidents, but nevertheless they will not eliminate them entirely as there will still be occasions where accidents will happen [59] (pp. 89–90). This is inevitable due to physics, as, for example, when an object, animal, or person appears in the path of the vehicle inside its braking distance, leaving no room to avoid hitting something else, an accident will happen, regardless of who or what is driving.

Therefore, it is not reasonable to ignore the need for the user to determine the actions of the autonomous vehicle based on their ethics, religion, and other preferences. Obviously, such preferences must be declared before the accident; consequently, it becomes logical that each user ought to be able to make their preferences known to the vehicle once they are inside. For now, the conundrum of what to do in the presence of multiple passengers

will be ignored, as it distracts from the focus of attention, and we shall assume there is one person inside or that the owner's wishes prevail. Nevertheless, such preferences must be arguably either be recorded permanently in the vehicle's electronic system or the user must enter them each time.

In either case, considering the very personal and difficult nature of whatever preference the user decides on, it is obvious that the decision should be private to the utmost. This is evidenced by the disconnect between individuals' own unwillingness to purchase "self-sacrificing" utilitarian autonomous vehicles versus their comfort with other people purchasing them [59] (p. 91).This implies that there is a conflict between self-preservation and morality, which could manifest in a societal condemnation of "selfish" individuals who made the choice of self-preservation after an accident, even if it is likely many of the condemners would have made the same choice. Consequently, to prevent such predictable condemnation, the vehicle's data governance should be designed to take this into account. Moreover, the situation is ever more complex, considering traffic with CAVs would imply that there are multiple vehicles with perhaps conflicting preferences sharing the road. As such, at least on the V2V level, it would make sense that nearby cars communicate this to each other, which may raise the challenges of ensuring the confidentiality and security of such user choices and preferences.

Furthermore, research has been conducted in respect of the "trolley question" for autonomous vehicles through, for example, the "Moral Machine" [60], which has been criticized for its methodology as being simplistic and focused on characteristics of the "target" [61] (pp. 287-288). For example, the "scenarios and therefore answers are based on differences in characteristics such as gender, age and social status" [59] (p. 92). Hypothetically, if autonomous vehicle decision-making was to be based on the results of experiments, such as "Moral Machine", the result would be problematic not only from a GDPR perspective, but also the human right perspective. If the AI controlling the autonomous vehicle would make the decision on "who to sacrifice" based on the characteristics mentioned above, we must argue this violates the nondiscrimination required, for example, by Article 14 of ECHR, as effectively it would selectively limit the right to life based on certain parameters [61] (p. 290).

However, such a decision-making process arguably would not be technically unfeasible, making the situation even more concerning. For example, considering that a CAV would have a wide array of sensors and a capability to communicate with various devices (V2X), as well as a need to share data anyway, this, combined with existing technology such as facial recognition, could enable a CAV to form a "value matrix" of its surroundings, including other vehicles and pedestrians [59] (p. 105). Consequently, the obstacle to such decision-making in CAVs is not technical, but rather ethical and, potentially, legal, although in the absence of a specific case law or legislation it is not possible to conclusively state that, for example, Article 14 of ECHR would prevent such discriminatory decision-making.

Therefore, it is important that sustainable data governance of the CAV take this into account already at a design stage, to remove the possibility of AI making "unsustainable" choices from the societal and ethical point of view. This could involve, for example, not incorporating the aforementioned facial recognition that could be used to make discriminatory directional choices for the vehicle and preventing introduction of such software later on by the user to the vehicle, thus preventing such data from being collected or considered. As a result, it is important that data governance of CAVs be designed from the beginning to be "sustainable", in the sense that it preserves existing societal and cultural values and ensures that the beliefs and opinions of the user of the CAV are respected.

Consequently, from the point of view of designing sustainable data governance for CAVs, it is crucial that the current legal framework's social values, both explicit and implicit, be considered. Although the right to autonomy in the face of automated decision-making may, strictly speaking, be an emerging right for CAVs, as currently it is found in the GDPR regarding data protection, it is already indirectly required by existing human rights that aim to preserve the autonomy of human beings. Furthermore, as the focus

of this article is on existing law and, as such, the social values considered above were limited to what can reasonably be derived from the existing legal frameworks, there may be a multitude of diverse local societal and cultural values, that must be considered for sustainable data governance in CAVs, that were not included in the scope of this article. Therefore, when considering the concept of "sustainability", as already understood for smart cities in terms of social values, similar considerations ought to be made for connected autonomous vehicles.

4. Data Protection and Liability in CAV

Based on our findings above, the development, testing, and use of CAVs entail processing a vast amount of data, including personal data. The European Automobile Manufacturers' Association (ACEA) differs among various types of data processed by CAVs. The first category includes purely technical data relating to the vehicle, e.g., serial numbers of vehicle components, version of software, or diagnostic fault codes. The second category of data processed consists of personal data relating to the data subjects, namely user statistics, use of entertainment services, or contractual and financial data. The third category relates to the environment of the CAV—external temperature, pedestrians, or other license plates captured by sensors or cameras [62] (p. 6). It is of essence to note that ACEA's conclusions noting that not every piece of data processed within a CAV shall be considered as personal data is not correct. GDPR requires a precise test of reasonable probability when it comes to identifiability criterion, therefore triggering application of GDPR in cases where there is a reasonable legal possibility of identification. In practice, this means that the notion of personal data shall be interpreted in a very broad and extensive manner. Although technical data in a CAV may be classified as nonpersonal data at first glance, such assumptions do not always need to be substantiated.

Personal data is often important when it comes to one of the most frequently discussed issues of a CAV—liability for damages caused by (partly) autonomous vehicles. This part of the article deliberates on the legal framework for processing personal data in the EU, represented by the GDPR and related issues of personal scope and liability. Model user cases are provided to distinguish between different actors involved in processing personal data within a CAV, and potential issues are analyzed.

4.1. Personal Scope of GDPR

Organizations processing personal data clearly fall under the provisions of EU data protection law represented by the GDPR [48], but different stakeholders may need to follow specific rules, traditionally, requirements of compliance with data protection laws apply to controllers and processors processing personal data about data subjects. Controllers are entities that, solely or jointly with others, determine purposes and means of processing personal data [48] (Art. 4(7)), and are primary bearers of responsibility for compliance with data protection rules [63] (p. 25). The entity is classified as a controller when five elements are fulfilled [64] (p. 9). Firstly, the controller shall have a determinative influence (or control) [64] (pp. 10–11) [63] (p. 30) over data processing, and this control may stem from explicit legal competence, implicit legal competence, or factual influence [64] (pp. 10–12).

Secondly, the controller shall exercise the determinative influence over purposes and means of processing. In other words, the controller is the entity specifying the "why" and "how" of processing operations [64] (pp. 13–15) Thirdly, influence shall be exercised by one or more entities classifying as controllers. The institution of joint controllers has emerged during the interpretation of "jointly" from the definition of controller in Directive 95/46/EC [64] (pp. 12–13), and joint controllers are now explicitly provided for in the GDPR. We must note that interpretation of the notion of joint controllers is still a part of academic debate and practice. The relationship of joint controllers shall be based on factual circumstances [64] (p. 17). It is detrimental to analyze whether joint participation in determining the means of purposes has been involved in processing operations. Joint participation may take the form of joint decisions or converging decisions [65] (pp. 18–19).

The fourth condition relates to the status of the controller, as the controller may be a natural or legal person, public authority, agency, or other body. The definition is thus not reserved for organizations, but a natural person processing personal data may also qualify as a controller [64] (p. 10). The fifth condition represents the fact that control shall be exercised over the processing of personal data [64] (pp. 15–16).

On the other hand, processors process personal data on behalf of controllers [48] (Art. 4(8)). Two basic building blocks form part of the definition of a processor. Firstly, it must be a separate entity from the controller [64] (p. 24). Secondly, processing operations by the processor must be conducted on behalf of the controller [64] (pp. 24–45). This relationship is best described as a form of delegation where a controller determining the purposes and means of processing outsources processing operations to another entity—the processor.

GDPR further includes the definition of other actors of data processing—recipients, third parties, and data subjects. Data subjects are persons whose personal data are processed [48] (Art. 4(1)). The recipient is defined broadly as any "natural or legal person, public authority, agency or another body, to which personal data is disclosed, whether a third party or not." [48] (Art. 4(9)). Public authorities accessing data due to their public tasks and roles are excluded from the definition. Lastly, third parties represent "a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data." [48] (Art. 4(10)).

When it comes to CAVs, these represent a robust ecosystem of data processing via various significant processing parties [65] (pp. 7–8). Guidelines issued by the European Data Protection Board (EDPB) [65] provide the first authoritative interpretation of classification of various players involved in data processing for CAVs. Typical data subjects are passengers in CAV, and the owner or driver himself. Additionally, the ACEA recognizes more types of data subjects, namely subscribers of services, users of services, and individuals close to the vehicle, though challenging identifiability of some categories for manufactures [62]. Examples of controllers include insurance companies, providers of CAV´s services, or manufacturers of the vehicle processing data for maintenance and development. EDBP's demonstrative lists of processors consist of manufacturers of specific vehicle components processing personal data on behalf of manufacturers. Commercial partners providing specific services shall be considered recipients [65] (p. 9). Public authorities or law enforcement agencies are explicitly recognized in the guidelines as third parties [65] (p. 9). However, it shall be noted that the reality of processing personal data is far more complex and it would cause blurring to classify them rigorously based on the guidelines [62] (p. 3). After all, concepts of controllers and processors are dynamic and shall always be assessed based on the factual circumstances.

4.2. Liability in GDPR

Defining roles and, therefore, also the scope of liabilities is often no easy task. We must highlight that this "binary" setting of the roles for processing operations does not fit with practice in networked environments using new technologies [66] (p. 72).

Article 82 (1) GDPR establishes the basis for liability for damages: "Any person who has suffered material or nonmaterial damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." Three elements of liability may be derived from the provision: (i) unlawfulness, (ii) damage(s), and (iii) causality [66] (pp. 493–495). The element of unlawfulness is fulfilled by any infringement of the GDPR. In terms of damages, the GDPR also explicitly mentions material and nonmaterial damages in the pertinent article. Examples of material damages may include dismissal from employment, nonexecution of contracts, or altering clauses or provisions of contracts based on unlawful processing of personal data. Nonmaterial damages may include negative public exposure, anxiety, or discrimination [67] (p. 495). As a final element of the liability regime in GDPR, causality between unlawful actions of a competent entity and damages must exist [48] (Art. 82(1)).

4.2.1. Controllers and Liability

We must note that a "strict" liability regime continues to apply for controllers. The latter is confirmed by Article 82 (2) GDPR: *"Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation."* It is important to highlight that the GDPR strengthens the principle of accountability [48] (Art. 5(2)). This principle requires controllers to demonstrate compliance with the regulation in two ways. First, by fulfilling more formal obligations, e.g., maintaining records of processing personal data, or drafting and publishing a privacy policy or internal data protection documentation (security policy or internal data protection policy). Second, by implementing appropriate organizational and technical measures into data protection practice, e.g., identity management, procedures for notifying personal data breaches, or introducing a different level of access to personal data for specific employees [68] (pp. 49–82). In practice, the above may mean that when the data subject offers evidence of unlawful processing activity, the burden of proof shifts towards the controller to demonstrate compliance with GDPR [69] (p. 283).

The controller may escape liability only in cases of "events beyond control." Article 82 (3) GDPR stipulates that "A controller shall be exempt from liability . . . if it proves that it is not in any way responsible for the event giving rise to the damage." Some authors even suggest that the wording "in any way" represents narrowing this exception [70] (p. 58).

4.2.2. Processors and Liability

Though specific obligations and liability of processors are not presented in Directive 95/46/EC, EU legislators took the step forward and regulated the issue in the GDPR. Obligations for the processor may stem directly from the GDPR (e.g., obligation to maintain records of processing activities based on the Article 30 GDPR, notification obligation about the personal data breach to the controller according to the Article 33 (2) GDPR, or appointment of data protection officer per Article 37 GDPR) [48] (Art. 30, 33(2), 37) or from the contract concluded with the controller in compliance with Article 28 (3) GDPR. As the processor always acts on behalf of the controller, deviating from lawful instructions of the controller or data processing agreement form the background to liability for processors.

The legislation provisions are a proportional liability regime for processing operations where a processor is involved. This conclusion arises from Article 82 (2) GDPR: *"A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."* However, the GDPR provides the option for processors to be held liable for *"the entire damage in order to ensure effective compensation of the data subject."* [48] (Art. 82(4). We should note that the mere involvement of the processor in processing personal data shall not mean that a processor may be held liable wholly or partially for the damage [69] (p. 285). Damages may be attributed to the processor only under the condition that the processor´s activities during processing of personal data caused damage, and actions related to the damages were either contrary to obligations under the GDPR, or controller´s instructions. If this is the case, the processor may be held liable for damages. On the other hand, the GDPR does not contain any threshold when it comes to the degree of responsibility, therefore, at least in theory, the processor may be held liable for the whole amount of the damage [64] (pp. 12–13). Even more, the controller has an option to redress—compensation from the processor if it is established that the processor was in breach of the GDPR, or acted outside of the scope of the controller´s instructions [48] (Art. 82(5)) In terms of defenses and types of eligible damages, the same rules apply as for controllers.

4.2.3. Joint Controllers and Liability

The GDPR explicitly recognizes the concept of joint controllers [48] (Art. 26(1)). Joint controllers shall determine their responsibilities concerning compliance with GDPR in a transparent manner. In terms of liability, we must highlight that, based on the wording of the GDPR, every joint controller may be held liable for the damage in the entirety. It

is worth noting that Article 83 GDPR does not contain specific rules on allocating fines among joint controllers, in cases of breaches of GDPR.

Joint controllership and joint liability issues have been under the scrutiny of the Court of Justice of the European Union (CJEU) recently in the cases of Wirtschaftsakademie and Fashion ID, following the basic premise established by Google Spain. In the case of *Google Spain* [71], the Court of Justice of the European Union in Luxembourg (CJEU) noted regarding data protection issues (including liability) for search engines and original publishers of news that: *" . . . the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities,* ***powers, and capabilities****, that the activity meets the requirements of Directive 95/46."* [71] (Para. 38). The CJEU emphasized that meeting data protection obligations shall be analyzed through the lens of the "powers and capabilities" of the controller. Although the case concerns a specific entity processing personal data (search engine), the CJEU seems to allow interpretation of responsibilities in an exceptional manner, opening the door to avoid liability.

Wirtschaftsakademie [72] concerned operating a fan page on Facebook and correct classification of the provider of the social network (Facebook) and operator of the fan page (Wirtschaftsakademie). The cornerstone of the deliberation of the court was to establish whether, and to what extent, the operator of the fan page determines purposes and means of processing of personal data jointly with Facebook.

The Luxembourg court noted at the beginning of their judgment that, although not every user of Facebook shall automatically be considered to be a controller, the specific situation of the operator of a fan page derives from the fact that *"by creating such a page, allows Facebook to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account."* [72] (Para. 35). The CJEU also noted that the operator of the fan page has a margin of appreciation as to determining targeting filters (selecting the audience) and criteria for how the statistics are created [72] (Para. 36). Based on these conclusions, the Court established that Facebook and the operator of a fan page are joint controllers. However, the CJEU highlighted the importance of analyzing the state of processing as different controllers may be involved at various stages on the various levels, therefore *"the level of responsibility of each of them must be assessed concerning all the relevant circumstances of the particular case."* [72] (Para. 43). Doctrine characterized the decision as to the switch from macroscopic to microscopic view of processing of personal data [73] (p. 48) However, the court still did not address some of the crucial considerations of joint controllership, such as mechanisms for allocating responsibilities or the relationship between determining purposes *and* means of processing [73] (p. 49).

A similar outcome lies within the conclusions of the Fashion ID case [74]. The dispute involved a situation where a web page provider (Fashion ID—online clothing retailer) embedded the "Like" social plugin on its website from the social network Facebook. The issue at question was that every time a visitor visits the web page of the online clothing retailers, the web transmits data about visitors to Facebook regardless of the existence of an account on the social network. The Court again acknowledged the broad interpretation of the notion of controller following the decision in Wirtschaftsakademie. Joint determination of purposes and means have been found at the origin of processing operations (collection and disclosure) [74] (Paras. 79-81). Different liability may be attributed to various actors during personal data processing, taking different stages of processing into account [74] (Para. 71).

Both the decisions above reflect the complexity of the correct determination of entities in light of the personal scope of GDPR. What is more, the CJEU applies the principle of "effective and complete protection" [73] (pp. 40–41) in light of fundamental rights and freedoms, therefore, aiming to ensure protection of all potential data subjects affected by processing personal data by various parties.

4.3. Defining the Roles and Liabilities

Three regimes of data sharing within CAVs are analyzed. Based on these, different conclusions regarding roles and liabilities under GDPR may be derived from the situations addressed.

The first situation occurs when a CAV is connected to the Internet, including processing data by providers of essential and entertainment applications (vehicle to the Internet (V2I)). Two possible user cases can be characterized within this situation—(i) connection to essential services for functioning of the CAV, e.g., GPS navigation, and (ii) connection to entertainment services, e.g., streaming services. Processing data whilst connected to the essential CAV services will be perceived as a relationship between the data subject (a driver or owner of a vehicle) and a controller (provider of the essential service). However, an issue may arise considering the relationship between the provider of the CAV and a provider of the essential service. Determining this kind of processing relationship as a simple controller–processor relationship has been rendered obsolete by recent decisions of the Court of Justice of the European Union mentioned above.

Therefore, it is of the essence to revise understanding of these concepts, especially in terms of liability. It seems that the key principle guiding the relationship is the principle of full and effective protection of data subjects and microscopic evaluation of processing operations [72] (Para. 43). After assessing the details of processing operations between the provider of the CAV and the provider of the essential services, one may conclude that in some cases joint controllership is in place. Additionally, for origination of joint controllership, no explicit joint determination of means and purposes is required. It is sufficient if converging decisions occur, with a tangible impact on determination [64] (p. 18). It is, therefore, possible that in the case of guidance of a CAV by the provider of the service required, the requirement of converging decisions to determine the purposes and means of processing would be met. As enshrined in the EDPB, the mutual benefit of processing parties is also of the essence [64] (p. 18). As a result, joint controllership would ensue. Liability in a given case should be determined for the specific case and specific circumstances. The second case is the connecting the CAV to entertainment services. We believe that this is the case of the data subject and a controller (provider of the entertainment), while the provider of a CAV shall not have stricto sensu access to data processing within this operation, as this is not necessary for functioning of the CAV.

The second situation consists of communication between two CAV vehicles (vehicle-to-vehicle (V2V)) for preventing road traffic accidents. In our opinion, processing data for this purpose shall be subject to proper anonymization [75], and processed data shall consist of nonpersonal data, relating to the distance between vehicles or other technical data. In this case, identifying the data subject will not be possible and the GDPR would no longer apply. Furthermore, such an approach would be in line with the law on data protection, by design and by default [76].

The second situation relates to connection of a CAV to other devices within the Internet of Things infrastructure (vehicle to the Internet of Things (V2IoT)). Again, we may discuss two model situations in this context—(i) connection to cooperative–intelligent transportation system (C-ITS) and (ii) use of data for tort proceedings by public authorities. The first modality is data processing between vehicles and C-ITS, where the purpose lies in the cooperation between the CAV provider and the road infrastructure to prevent accidents and to ensure compliance with road traffic regulations. Communication between vehicles is not excluded in this case [77]. When discussing connections to C-ITS, the question of status and liability in terms of the GDPR arises again. Is this the case for having separate controllers or joint controllership? In our opinion, it is again possible that in light of recent CJEU case law, practice will have to assess this relationship as joint controllers. We base this conclusion on two arguments. According to the first argument, both controllers have a common purpose materialized in faultless road traffic. This purpose is detrimental to the provider of C-ITS (state or self-governments), as well as being economically inevitable and important to the provider of a CAV, for without respecting traffic laws it would

be impossible to obtain profits for the sale of CAVs. At the same time, providers use interconnected infrastructure to communicate with each other. Again, this may be the case of converging decisions about purposes and means of personal data processing.

The second argument in favor of classification of these entities as joint controllers is the decision of the CJEU in Wirtshaftsakademie. In this case, it was the operator of the fan page on the social network that fitted its processing activities within the boundaries provided by the social network (e.g., in the form of advertising targeting specifications or statistics) and subsequently both entities benefited from the processing of data. Analogously, a similar situation may arise when the provider of the CAV "deploys" the vehicle within C-ITS. From our point of view, this solution is not ideal, as it would require a comprehensive review of the relationship between providers of CAVs and operators of the infrastructure, as required by Article 26 of GDPR. Right now, it is impossible to predict how the judiciary and practice will deal with this issue.

The second modality within the third regime is use of data by public authorities for purposes when conducting administrative or criminal proceedings. Therefore, public authorities shall be classified as recipients and separate controllers of data. Concerning this situation, reference can be made to the German regulation, which explicitly regulates access and use of data from the so-called black boxes for autonomous vehicles [78] (Art. 63).

5. Conclusions

Although fully automated vehicles are sooner a matter for the future, connected and partially automated vehicles present current legal issues due to their fast development and actual deployment. The EU aims to provide CAV manufacturers a sound legal basis and environment and become the leader in regulatory innovations and attract economic stimulation. It is of the essence to note, that development of C-ITS is also backed by legislation and connectivity, and inclusion of CAVs within the system is one of the cornerstones of future smart and connected mobility.

However, the transformation to "smart" mobility should be accomplished in a sustainable manner, similar to other such "smart" developments such as smart cities. In the context of smart cities, sustainability has been considered to include social and cultural values, which, considering the interconnectedness of autonomous vehicles to the smart city, therefore arguably extends to autonomous vehicles. The replacement of human decision-making by artificial intelligence has the capacity to erode long-held and protected social and cultural values, such as the autonomy of an individual. There is already some evidence to suggest that (future) manufacturers of autonomous vehicles are already planning to ignore such values, despite them being derivable from existing legal frameworks, such as various human rights instruments and Article 22 (1) of GDPR. As a result, the scope of current research was limited to the most fundamental and readily derivable social and cultural values that are immediately obvious, with a literal and uncontroversial interpretation of instruments incorporating internationally recognized fundamental rights such as those found in the ECHR. Therefore, there may well be additional social and cultural rights that require a more in-depth, contextualized, and purposeful analysis to be uncovered, that may be threatened by the shift to autonomous vehicles, and, as such, represent a potential direction for future research. Consequently, it is important to bring this seemingly overlooked aspect of sustainability to the reader's attention, associated with data governance of autonomous vehicles, before they deprive individuals of their autonomy for example, and the opportunity to manifest their beliefs and choices in life-and-death situations.

Furthermore, exploring the meaning of sustainable data governance for the decision-making of the vehicle itself ought to be carried out prior to their introduction, to avoid significant negative effects for many stakeholders. For example, if decision-making of the AI controlling an autonomous vehicle should selectively limit the right to life, contrary to Article 14 of the ECHR, the results would be undesirable for both the vehicle manufacturer and those individuals unfairly "targeted" by such automated decision-making. Consequently, the importance of making data governance sustainable from a social and cultural

perspective prior to introduction of connected autonomous vehicles is considerable for many of the stakeholders affected by their introduction.

Processing of data and related data governance is fundamental to the development and use of CAVs. As discussed in the article, manufacturers of CAVs are quite reluctant to allow access to data for third parties. The current legislative provisions ensure access to maintenance and repair data only for independent operators. However, further access rights may be overridden by independent controllers of personal data due to their controllership rights. Moreover, this places constraints on, and limits, current research, as the nature of the processed data in CAVs is only truly known by the automotive industry; therefore, as a result, any research at the present moment is hampered and obstructed by what information is available to the public and, as such, conclusions drawn may not be representative of the full extent of the situation for CAV data.

In terms of the position of various actors in processing personal data in a CAV, we primarily discussed the current interpretation of the concepts of the controller, processor, and their liability in the sense of recent CJEU case law. Based on the definition and analysis of three model situations, we pointed out that in several cases of processing personal data within the CAV, it is extremely demanding to determine the liable entity, due to the functional and relatively broad interpretation of the concept of joint controllers in terms of the possibility of converging decisions on purposes, and means of processing within vehicles under discussion. A constant microscopic view of processing operation through the lens of the CJEU is not the most appropriate and sustainable method for defining relationships concerning CAVs. It is therefore possible that the future will bring very complicated legal questions with no simple and positive consequences in terms of processing personal data in cases where the respective EU legislative acts have not been harmonized and simplified.

Therefore, in summation, the main results and conclusions drawn from our analysis of the existing European Union legal frameworks with regards to CAVs are as follows:

- Data governance and processing of data are fundamental to the development and use of CAVs; however, manufacturers are reluctant to allow access to third parties.
- The current legislative environment ensures access only in limited cases, such as maintenance and repair.
- The transformation to connected autonomous vehicles must be conducted in a sustainable manner, to avoid erosion of legally protected social and cultural values.
- The current legal framework makes it extremely demanding to establish the liable entity in matters relating to processing of personal data.
- The present method of using the CJEU to define relationships between personal data processing and CAVs is not sustainable for the future.

In conclusion, our research has identified numerous issues relating to the sustainable governance of CAVs that warrant further examination in the fields of data protection and fundamental rights, as well as ensuring access to data. As a result, it is evident that there are numerous directions for future developments of this research which we have highlighted through our analysis and resulting conclusions. The article demonstrates that the current legal framework of the EU with regards to CAVs is not able to provide a definitive answer to all issues under discussion, surrounding the development and eventual introduction of CAVs. Moreover, this article has identified threats to fundamental values enshrined in law, for example, the ECHR, which have already begun to emerge and are likely to exacerbate if left unaddressed as the development and introduction of connected autonomous vehicles continues. Therefore, it is imperative that the regulators safeguard internationally well-established fundamental values when addressing the legal issues surrounding CAVs to ensure sustainable reforms that will form a solid foundation for realizing the EU's vision of a cooperative, connected, and automated mobility.

Author Contributions: Conceptualization, J.A., O.H. and T.K.; methodology, M.M., writing—original draft preparation, J.A., O.H., T.K., M.M. and A.K.; writing—review and editing, A.K.; supervision, J.A.; project administration, O.H.; funding acquisition, T.K. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was prepared as part of the cooperation within Jean Monnet Network "European Union and the Challenges of Modern Society" (611293-EPP-1-2019- 1-CZ-EPPJMO-NETWORK). O.H. and T.K. participated on the works on the paper within the implementation of the project no. 20-27227S "The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union" funded by the Czech Science Foundation (GAČR).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Schellekens, M.H.M. Self-driving cars and the chilling effect of liability law. *Comput. Law Secur. Rev.* **2015**, *31*, 506–517. [CrossRef]
2. Collingwood, L.; Bartolini, C.; Tettamanti, T.; Varga, I. Critical features of autonomous road transport from the perspective of technological regulation and law. *Transp. Res. Procedia* **2017**, *27*, 791–798.
3. Collingwood, L. Privacy implications and liability issues of autonomous vehicles. *Inf. Commun. Technol. Law* **2017**, *26*, 32–45. [CrossRef]
4. Hacker, P. Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things. *Int. Data Priv. Law* **2017**, *7*, 266–286. [CrossRef]
5. Prakken, H. On the problem of making autonomous vehicles conform to traffic law. *Artif. Intell. Law* **2017**, *25*, 341–363. [CrossRef]
6. Kerber, W.; Gill, D. Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation. *JIPTEC* **2019**, *10*, 244–256. [CrossRef]
7. Ducuing, C.; Vedder, A.; Schroers, J.; Valcke, P. Towards an Obligation to Secure Connected and Automated Vehicles "by Design"? In *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure*; Intersentia: Cambridge, UK, 2019; pp. 183–213.
8. Polčák, R. Odpovědnost Umělé Inteligence a Informační útvary bez Právní Osobnosti. Bulletin Advokace 11/2018. Available online: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2018/BA_11_2018_web.pdf (accessed on 6 July 2021).
9. Yong, W.; Hongxuyang, L. Copyright protection for AI-generated outputs: The experience from China. *Comput. Law Secur. Rev.* **2021**, *42*, 105581.
10. Barfield, W.; Pagallo, U. *Research Handbook on the Law of Artificial Intelligence*; Edward Elgar Publishing: Cheltenham, UK, 2018; pp. 411–535.
11. Kim, S.; Shrestha, R. *Automotive Cyber Security. Introduction, Challenges, and Standardization*; Springer: Singapore, 2020; 216p.
12. Schellekens, M. Car hacking: Navigating the regulatory landscape. *Comput. Law Secur. Rev.* **2016**, *32*, 307–315. [CrossRef]
13. European Commission. European Strategy on Cooperative Intelligent Transport Systems. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0766 (accessed on 26 August 2021).
14. European Commission. Access to In-Vehicle Data and Resources. Available online: https://ec.europa.eu/transport/sites/default/files/2017-05-access-to-in-vehicle-data-and-resources.pdf (accessed on 26 August 2021).
15. Eriksson, L.; McConnachie, S.; Autonomous Vehicles. What Can Social Science offer? University College London & Catapult College London. Available online: https://s3-eu-west-1.amazonaws.com/media.ts.catapult/wp-content/uploads/2018/08/06093018/00498_Autonomous-Vehicles_What-can-Social-Science-Offer_A5-Booklet-009.pdf (accessed on 6 July 2021).
16. EU Commission. COM/2018/283 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions on the Road to Automated Mobility: An EU Strategy for Mobility of the Future. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0283 (accessed on 13 September 2021).
17. Andraško, J.; Mesarčík, M.; Hamuľák, O. The regulatory intersections between artificial intelligence, data protection and cyber security: Challenges and opportunities for the EU legal framework. *AI Soc.* **2016**, *36*, 623–636. [CrossRef]
18. Matteson, S. Autonomous Versus Automated: What Each Means and Why It Matters. Motor Vehicle Type Approval Regulation, 10 (2019) JIPITEC 244. Available online: https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/ (accessed on 6 July 2021).
19. SAE J3016: Sep 2016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for on-Road Motor Vehicles.
20. United Nations Economic Commission for Europe Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic. Available online: https://unece.org/transport/publications/resolution-deployment-highly-and-fully-automated-vehicles-road-traffic (accessed on 25 August 2021).

21. International Transport Forum and Corporate Partnership Board. Automated and Autonomous Driving Regulation under uncertainty. Available online: https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf (accessed on 6 July 2021).
22. Abdulrazzaq, L.R.; Abdulkareem, M.N.; Yazid, M.R.M.; Borhan, M.N.; Mahdi, M.S. Traffic Congestion: Shift from Private Car to Public Transportation. *Civ. Eng. J.* **2020**, *6*, 1547–1554. [CrossRef]
23. Severino, A.; Curto, S.; Barberi, S.; Arena, F.; Pau, G. Autonomous Vehicles: An Analysis both on Their Distinctiveness and the Potential Impact on Urban Transport Systems. *Appl. Sci.* **2021**, *11*, 3604. [CrossRef]
24. Gorbunova, A.D.; Anisimov, I.A. Assessment of the Use of Renewable Energy Sources for the Charging Infrastructure of Electric Vehicles. *Emerg. Sci. J.* **2020**, *4*, 539–550. [CrossRef]
25. Lim, H. *Autonomous Vehicles and the Law Technology, Algorithms and Ethics*; Edward Elgar Publishing: Cheltenham, UK, 2018.
26. Skeete, J. Level 5 autonomy: The new face of disruption in road transport. In *Technological Forecasting and Social Change*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 134, pp. 22–34.
27. Lim, H.; Taeihagh, A. Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies* **2018**, *11*, 1062. [CrossRef]
28. European Union Agency for Cybersecurity. Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. 2019. Available online: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving/ (accessed on 25 August 2021).
29. European Commission. Ethics of Connected and Automated Vehicles. Available online: https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search (accessed on 26 August 2021).
30. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on Type-Approval Requirements for Motor Vehicles and Their Trailers, and Systems, Components, and Separate Technical Units Intended for Such Vehicles, as Regards Their General Safety and the Protection of Vehicle Occupants and Vulnerable Road Users, Amending Regulation (EU) 2018/858 of the European Parliament and of the Council and Repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166. Available online: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32019R2144 (accessed on 13 September 2021).
31. German Road Traffic Act. Available online: https://www.gesetze-im-internet.de/stvg/ (accessed on 14 September 2021).
32. BSI: Connected and Automated Vehicles—Vocabulary BSI Flex 1890 v3.0:2020-10. Available online: https://edisciplinas.usp.br/pluginfile.php/5810443/mod_resource/content/3/GLOSSARIO%20%20-%20Connected%20and%20Automated%20Vehicles%20bsi-flex-1890-v3-2020-10%20%281%29.pdf (accessed on 14 September 2021).
33. Kala, R. On-Road Intelligent Vehicles. In *Motion Planning for Intelligent Transportation Systems*; Elsevier: Amsterdam, The Netherlands, 2016.
34. Fulu, W.; Long, C.; Yongqing, G.; Mingtao, C. Car-following Behavior Analysis of Left-turn Vehicles at Signalized Intersections. *Civ. Eng. J.* **2020**, *6*, 186–193.
35. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the Approval and Market Surveillance of Motor Vehicles and Their Trailers, and of Systems, Components, and Separate Technical Units Intended for Such Vehicles, Amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and Repealing Directive 2007/46/EC. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0858 (accessed on 13 September 2021).
36. Kasper, A.; Krasznay, C. Towards Pollution-Control in Cyberspace: Problem Structure and Institutional Design in International Cybersecurity. *Int. Comp. Law Rev.* **2019**, *19*, 76–96. [CrossRef]
37. EU Commission. Guidelines on the Exemption Procedure for the Eu Approval of Automated Vehicles. Available online: https://ec.europa.eu/docsroom/documents/34802 (accessed on 6 July 2021).
38. Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the Framework for the Deployment of Intelligent Transport Systems in the Field of Road Transport and for Interfaces with Other Modes of Transport. Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040 (accessed on 13 September 2021).
39. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications). Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (accessed on 13 September 2021).
40. EU Commission. Document C(2019)1789 Delegated Regulation Supplementing Directive 2010/40/EU with Regards to the Deployment and Operational Use of Cooperative Intelligent Transport Systems. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282019%291789 (accessed on 13 September 2021).
41. ACEA Position Paper Access to Vehicle Data for Third-Party Services. Available online: https://www.acea.auto/files/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf (accessed on 6 July 2021).
42. Elliot, D.; Keen, W.; Miao, L. Recent advances in connected and automated vehicles. *J. Traffic Transp. Eng.* **2019**, *6*, 109–131. [CrossRef]

43. Gruyer, D.; Orfila, O.; Glaser, S.; Hedhli, A.; Hautière, N.; Rakotonirainy, A. Are Connected and Automated Vehicles the Silver Bullet for Future Transportation Challenges? Benefits and Weaknesses on Safety, Consumption, and Traffic Congestion. *Front. Sustain. Cities* **2021**, *2*, 1–24.
44. Kerber, W. Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data. *JIPITEC* **2018**, *9*, 1–33.
45. Kerber, W.; Frank, J. Data Governance Regimes in the Digital Economy: The Example of Connected Cars. 2018. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064794 (accessed on 25 April 2021).
46. Tombal, T. GDPR as a Shield to a Data Sharing Remedy? Available online: https://law.haifa.ac.il/images/ASCOLA/Tombal.pdf (accessed on 7 July 2021).
47. European Data Protection Board. Guidelines on the Right to Data Portability. Adopted on 13 December 2016. As last Revised and Adopted on 5 April 2017. 16/EN WP 242 rev.01. Available online: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (accessed on 13 September 2021).
48. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regards to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119. 4 May 2016, pp. 1–88. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 13 September 2021).
49. Graef, I.; Husovec, M.; Purtova, N. Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. *Ger. Law J.* **2018**, *19*, 1359–1398. [CrossRef]
50. EU Commission Building a European Data Economy. 10 January 2017. COM(2017) 9 fin. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A9%3AFIN (accessed on 13 September 2021).
51. Paskaleva, K.; Evans, J.; Martin, C.; Linjordet, T.; Yang, D.; Karvonen, A. Data Governance in the Sustainable Smart City. *Informatics* **2017**, *4*, 41. [CrossRef]
52. Toli, A.M.; Murtagh, N. The Concept of Sustainability in Smart City Definitions. *Front. Built Environ.* **2020**, *6*, 1–10. [CrossRef]
53. Campisi, T.; Severino, A.; Al-Rashid, M.; Pau, G. The Development of the Smart Cities in the Connected and Autonomous Vehicles (CAVs) Era: From Mobility Patterns to Scaling in Cities. *Infrastructures* **2021**, *6*, 100. [CrossRef]
54. Taeihagh, A.; Lim, H.S.M. Towards Autonomous Vehicles in Smart Cities: Risks and Risk Governance. In *Towards Connected and Autonomous Vehicle Highways*; Springer: Cham, Switzerland, 2021; pp. 169–190.
55. Ethics Dialogue. The Underdog in the AI Ethical and Legal Debate: Human Autonomy. Available online: www.ethicsdialogues.eu/2019/06/12/the-underdog-in-the-ai-ethical-and-legal-debate-human-autonomy/ (accessed on 30 June 2021).
56. Calvo, R.A.; Peters, D.; Vold, K.; Ryan, R.M. Supporting Human Autonomy in AI Systems: A Framework for Ethical Enquiry. In *Ethics of Digital Well-Being*; Springer: Cham, Switzerland, 2020; Volume 140, pp. 31–54.
57. Jeder Mensch. The 6 European Fundamental Rights. Available online: www.jeder-mensch.eu/informationen/?lang=en&fbclid=IwAR2tVh9JqX_IXf0i1uigZIkThiumKIUiMfTqEupyk-PAj57gWjQnTz_Cwys (accessed on 30 June 2021).
58. Morris, D. Mercedes-Benz's Self-Driving Cars Would Choose Passenger Lives over Bystanders. Available online: Fortune.com/2016/10/15/mercedes-self-driving-car-ethics/ (accessed on 30 June 2021).
59. Etienne, H. The dark side of the 'Moral Machine' and the fallacy of computational ethical decision-making for autonomous vehicles. *Law Innov. Technol.* **2021**, *13*, 85–107. [CrossRef]
60. Moral Machine. Moral Machine. Available online: www.moralmachine.net/ (accessed on 13 September 2021).
61. Kochupillai, M.; Lutge, C.; Poszler, F. Programming away Human Rights and Responsibilities? "The Moral Machine Experiment" and the Need for a More "Humane" AV Future. *NanoEthics* **2020**, *14*, 285–299. [CrossRef]
62. European Automobile Manufacturers Association. ACEA Comments. European Data Protection Board Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. April 2020. Available online: https://www.acea.auto/files/ACEA_comments_EDPB_guidelines_1-2020.pdf (accessed on 13 September 2021).
63. Van Alsenoy, B. Allocating responsibility among controllers, processors, and everything in between: The definition of actors and roles in Directive 95/46/EC. *Comput. Law Secur. Rev.* **2012**, *28*, 25–43. [CrossRef]
64. European Data Protection Board. Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 1.0. Adopted on 2 September 2020. Available online: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en (accessed on 13 September 2021).
65. European Data Protection Board. Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. Version 1.0 Adopted on 28 January 2020. Available online: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-12020-processing-personal-data_en (accessed on 13 September 2021).
66. Kuner, C. *European Data Protection Law—Corporate Compliance and Regulation*, 2nd ed.; Oxford University Press: New York, NY, USA, 2003.
67. Cordeiro, A.M. Civil Liability for Processing of Personal Data in the GDPR. *Eur. Data Prot. Law Rev.* **2019**, *5*, 492–499. [CrossRef]
68. Alhadeff, J.; Van Alsenoy, B.; Dumortier, J. The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In *Managing Privacy through Accountability*; Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo, H., Eds.; Palgrave Macmillan: London, UK, 2012; pp. 49–82.
69. Van Alsenoy, B. Liability under EU Data Protection Law. *JIPITEC* **2016**, *7*. Available online: https://www.jipitec.eu/issues/jipitec-7-3-2016/4506 (accessed on 13 September 2021).

70. LaRouche, P.; Peitz, M.; Purtova, N. Consumer Privacy in Network Industries—A CERRE Policy Report, Centre on Regulation in Europe. 2016. Available online: https://cerre.eu/wp-content/uploads/2016/01/160125_CERRE_Privacy_Final.pdf (accessed on 13 September 2021).
71. Decision of the CJEU from 13 May 2014, Google Spain SL a Google Inc. v Agencia Española de Protección de Datos (AEPD) a Mario Costeja González. Case n. C-131/12. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (accessed on 13 September 2021).
72. Decision of the CJEU from 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case n., C-210/16. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210 (accessed on 13 September 2021).
73. Mahieu, R.; Van Hoboken, J.; Asghari, H. Responsibility for Data Protection in a Networked World. On the question of the Controller. Effective and Complete Protection"and its Application to Data Access Rights in Europe. *JIPITEC* **2019**, *10*, 39–59. [CrossRef]
74. Decision of the CJEU from 29 July 2019, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV. Case n. C-40/17. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0040 (accessed on 13 September 2021).
75. Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. Available online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (accessed on 13 September 2021).
76. European Data Protection Board. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Available online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (accessed on 13 September 2021).
77. Žolnercikova, V. Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly. *Rev. Pro Právo A Technol.* **2020**, *21*, 129–152. [CrossRef]
78. Czarnecki, K. English Translation of the German Road Traffic Act Amendment Regulating the Use of "Motor Vehicles with Highly or Fully Automated Driving Function". 2017. Available online: https://www.researchgate.net/publication/320813344 (accessed on 25 April 2021).