IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Dossier "Europe facing the digital challenge: obstacles and solutions"

The digital development of the European Union: data governance aspects of cooperative, connected and automated mobility[1]

Jozef Andraško
Comenius University

Ondrej Hamuľák
Palacký University Olomouc

Matúš Mesarčík
Comenius University

Date of submission: May 2021
Accepted in: November 2021
Published in: December 2021

Abstract

This article focuses on the issue of data governance in connected vehicles. Firstly, basic notions of autonomous vehicles are analyzed, and a legal framework is introduced. The European Union aims to create cooperative, connected, and automated mobility based on the cooperation of different inter-connected types of machinery. The essence of the system is data flow in connected vehicles, and the issue represents one of the heavily discussed themes in legal doctrine. Therefore, data governance is further discussed in the article. The final part of the article deals with the issue of responsibility and liability of different actors involved in the processing of personal data according to the General Data Protection Regulation applied to the environment of CAV smart infrastructure.

Keywords

connected vehicles; autonomous vehicles; GDPR; data governance

1. This paper was prepared on behalf of Jean Monnet Network Project 611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK "European Union and the Challenges of Modern Society".

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

El desarrollo digital de la Unión Europea: aspectos de gobernanza de datos de la movilidad cooperativa, conectada y automatizada

Resumen

Este artículo se centra en el tema de la gobernanza de datos en vehículos conectados. En primer lugar, se analizan las nociones básicas de vehículos autónomos y se introduce un marco legal. La Unión Europea tiene como objetivo crear una movilidad cooperativa, conectada y automatizada basada en la cooperación de diferentes tipos de maquinaria interconectada. La esencia del sistema es el flujo de datos en vehículos conectados y el tema representa una de las cuestiones tan discutidas en la doctrina legal. Por lo tanto, la gobernanza de datos se discute más a fondo en el artículo. La parte final del artículo trata sobre el tema de las responsabilidades y obligaciones de los diferentes actores involucrados en el procesamiento de datos personales de acuerdo con el Reglamento General de Protección de Datos aplicado al entorno de la infraestructura inteligente CAV.

Palabras clave

vehículos conectados; vehículos autónomos; RGPD; gobierno de datos

Introduction

The automatization of society may include the application of autonomous machines. Recently, special attention has been devoted to the development and use of autonomous vehicles. This is especially true when dealing with smart cities and connected infrastructure that may help with road safety and ensure comfort for travelers. Car manufacturers such as Tesla, Mercedes, Toyota, GM, Nissan, Volkswagen, and others have been testing autonomous vehicles for a long time, especially partially autonomous vehicles. However, from a legal point of view, the introduction and testing of autonomous vehicles is challenged by several legal institutions, particularly in the areas of liability, privacy, data protection, type-approval of vehicles, legal personality of autonomous systems, copyright rights, and further issues.[2]

This article focuses on the European Union (EU)'s recent initiatives in creating intelligent transport systems, including Cooperative Intelligent Transport Systems (C-ITS). C-ITS will allow road users and traffic managers to share and coordinate information in order to coordinate their actions to improve safety, comfort, and traffic efficiency. However, as a part of the C-ITS, connected vehicles process personal data necessary for the functioning of the ecosystem. The aim of this article is thus to analyze data flow and data governance in autonomous vehicles from a viewpoint of the current legal framework and related issues. The particular focus is on the data protection legislation in terms of access and governance of personal data in specific use cases.

The first part of the article introduces the concept of autonomy in vehicles and specifies relevant notions in connection with autonomous and connected vehicles. Furthermore, the legal framework of connected vehicles and C-ITS-related legislation at EU level is discussed. Secondly, the role of autonomous vehicles in the system is explained, and data governance is analyzed. The third part of the article deals with data protection issues of autonomous vehicles in the light of the personal scope of General Data Protection Regulation and liability.

1. Automated vehicles, autonomous vehicles, connected vehicles

Automated vehicles and autonomous vehicles are sometimes considered to be similar (DG GROW, 2017).

However, a distinction needs to be made between these two concepts. In general, autonomous vehicles can be described as "computer-controlled vehicles that are self-driven as they rely on several data resources to access the driving environment and to control the operation of the vehicle" (Collingwood, 2017). This would be the case of a fully automated vehicle that does not have a steering wheel or pedals. No driver input is required, and all vehicle occupants are considered as passengers. Autonomous vehicles are vehicles at level 5 of the SAE standard (SAE, 2016) and "rely solely on their on-board equipment to collect information, make decisions and inform tasks" (Frisoni *et al*., 2016).

2. See, e.g., CONSTANTINI *et al*. (2020). "Autonomous vehicles in a GDPR era: An international comparison". In: *Advances in Transport Policy and Planning*, vol. 5, pp. 191-213. KRONTIRIS, I. *et al*. (2020). "Autonomous Vehicles: Data Protection and Ethical Considerations". In: *CSCS '20: Computer Science in Cars Symposium*, no. 10. HACKER, P. (2017). "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things". In: *7 International Data Privacy Law*, pp. 266-286. APPT, S.; LIVESEY, N. (eds.) (2019). *Connected and Autonomous Vehicles. The Emerging Legal Landscape* [online]. London: Pinsent Masons. Available at: https://www.pinsentmasons.com/thinking/special-reports/connected-autonomous-shared-electric-vehicles. COLLINGWOOD, L. (2017). "Privacy implications and liability issues of autonomous vehicles". In: *Information & Communications Technology Law*, vol. 26, no. 1, pp. 32-45. DOI: https://doi.org/10.1080/13600834.2017.1269871. KERBER, W.; GILL, D. (2019). "Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation". In: *JIPITEC*, no. 10, pp. 244. DOI: https://doi.org/10.2139/ssrn.3406021. KERBER, W. (2018). "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data". In: *JIPITEC*, no. 9, pp. 310. SKIHO, K.; SHRESTHA, R. (2020). *Automotive Cyber Security Introduction, Challenges, and Standardization*. Singapore: Springer Nature. YEEFEN LIM, H. (2018). *Autonomous Vehicles, and the Law Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing. See more KASPER, A.; KRASZNAY, C. (2019). "Towards Pollution-Control in Cyberspace: Problem Structure and Institutional Design in International Cybersecurity". In: *International and Comparative Law Review*, vol. 19, no. 2, pp. 76-96 [online]. DOI: https://doi.org/10.2478/iclr-2019-0015.

On the other hand, automated vehicles are "vehicles that can replace the driver for some or all of the driving tasks" (DG GROW, 2017). However, the driver must be promptly available to take control of the vehicle.

Legal definitions of an automated vehicle can be found in the EU legislation.

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 (hereinafter referred as **"Regulation 2019/2144"**)[3] 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" (EUR-Lex-32019R2144, 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 driver supervision" (EUR-Lex-32019R2144, art. 3, 22).[4]

However, the full benefits of automated and autonomous driving are apparent when the vehicle can also communicate with other vehicles and other objects like infrastructure, etc. In this regard, these vehicles are considered connected vehicles.

Many vehicles are already considered connected devices. However, it is expected "that in the future they will also interact directly with each other and with the road infrastructure" (EUR-Lex-52016DC0766, p. 2).

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 (EUR-Lex-52018DC0283, p. 4).

Connected vehicles can be described as vehicles equipped with wireless communication technologies that enable data transfer with other vehicles, infrastructure, or other networks (BSI, 2020, p. 3).

Connected vehicles can "communicate with other vehicles, personal devices (e.g. smartphones) or the surrounding traffic infrastructure to collect information and perform driving tasks" (Frisoni *et al*., 2016, p. 19).

In cases in which automated vehicles are equipped with communications technology that enables data transfer with other vehicles, infrastructure, or other networks, we will refer to **the connected and automated vehicle (hereinafter CAV) (**BSI, 2020, p. 3).[5]

1.1 Intelligent transport systems

One of the practical examples where the vehicle may communicate within IoT is represented by the infrastructure of the intelligent transport systems. 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**") (EUR-Lex-32010L0040).

3. *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 (text with EEA relevance). PE/82/2019/REV/1.*
4. At the national legal order level, amendment to the German Road Traffic Act defines vehicles with highly or fully autonomous driving functions. Automated and Electric Vehicles Act 2018 adopted in the United Kingdoms does not define autonomous vehicles but rather automated vehicles (Regulation 2019/2144, art. 3, 22).
5. 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.

A high level of security for intelligent transport systems plays an important role in relation to autonomous vehicles. Autonomous and connected vehicles communicate with various intelligent transport systems for their operation. In these cases, data is received from an external source as well as recorded data are shared with a remote third party for various purposes.

From the point of view of communication between vehicles and road infrastructure, **cooperative intelligent transport systems** play an important role. These systems use technologies that allow road vehicles to communicate with each other and with the road infrastructure, including traffic signals. Commission adopted Proposal for a Delegated regulation supplementing the Intelligent transport systems directive concerning the deployment and operational use of cooperative intelligent transport systems (hereinafter referred to as the "Proposal for a delegated regulation") in March 2019 (EUR-Lex-C/2019/1789).[6]

In road transport, 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) (EUR-Lex-C/2019/1789, p. 1).

Cooperative intelligent transport systems services are a category of intelligent transport systems 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 or are not limited to exchanging messages with (a single) pre-defined station(s) (EUR-Lex-C/2019/1789, 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" (EUR-Lex-C/2019/1789, art. 2, 3).

According to Proposal for a 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 assemblies or as parts of larger assemblies (EUR-Lex-C/2019/1789, recital 15).

Each C-ITS station operator shall operate an information security management system under ISO/IEC 27001[7] and the additional requirements set out in point 1.3.1 of Annex IV of the Proposal for a delegated regulation (EUR-Lex-C/2019/1789, art. 27).

In connection with C-ITS stations, it is necessary to 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.

2. Data Governance in CAV

CAVs can receive, produce, process and transmit a huge amount of data. These data include:

1) in-vehicle data that are created by their in-vehicle technologies,
2) data that are sent from other vehicles or infrastructure,
3) traffic and infrastructure data sent from public authorities and
4) data imported (e.g. phone contact list, destinations for navigation) and produced by driver and passengers.

In-vehicle data are produced via sensor technologies, vision technologies, positioning technologies, and within vehicle control units. 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 behav-

6. Proposal for a delegated regulation available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282019%291789.
7. ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT. Several important standards have been adopted in the field of CAV. E.g. ISO 26262-1:2018 Road vehicles – Functional safety – Part 1: Vocabulary or Waste Heat Recovery System Thermal Management J3173_202002. For more standards see: https://www.connectedautomateddriving.eu/standards/standards-collection/.

ior, data about the health status of the driver (Kerber & Gill, 2019, p. 247).

Firstly, in-vehicle data help to ensure the proper operation of the vehicle, checks its proper operation and 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 and product development, non-automotive usage (e.g, car sharing, car rental, insurance) (ACEA, 2016, pp. 3).

These data can be processed in the vehicle and under some circumstances exchanged via communication technologies with other vehicles, infrastructure, vehicle manufacturers.

Secondly, CAVs rely on data that is sent from **other vehicles**, **road infrastructures** like C-ITS stations or traffic lights or signs, or other traffic participants (cyclists, pedestrians). For these purposes, different types of communication technologies like short-range communication technologies that operate in the dedicated 5.9 GHz frequency band, as well as long-range technologies 3G, 4G, or 5G mobile networks can be used. In that regard, CAV is the connected entity that receives data from an external source and can share data that are recorded with a remote third party for various purposes. Based on the participants in the communication the notion 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 some requirements. 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 work warnings, number and position of traffic lights and signs, etc.

Last but not least, **data imported** (e.g. phone contact list, destinations for navigation) and **produced** by driver and passengers (visited websites, online shopping preferences, etc.) are included.

Vehicle-generated data and data produced by driver or passengers are valuable not only for 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, insurance, etc.) (Kerber & Gill, 2019, p. 248).

2.1. Access to in-vehicle data concepts

From a **technical point of view**, there are different concepts for **access to in-vehicle data**. First of all, **the extended vehicle concept** is widely used by many vehicle manufacturers. The extended vehicle concept allows accessing vehicle data via different types of interfaces depending on the purpose for which access is sought. In this regard, vehicle manufacturers have exclusive, direct, full, and privileged control of data on their proprietary server and to whom access to data will be granted. Transferred data are usually in filtered and aggregated form. Access to vehicle data and their use will require a 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) (ACEA, 2016, p. 45).

Secondly, **the shared data server** concept is based on the idea that a neutral entity has control of the server and can grant non-discriminatory access to vehicle data. The data made available to the shared data server will be of the same quality as the data available on the vehicle manufacturer's proprietary server. However, vehicle manufacturers decide which data will be transferred from their proprietary server to the shared server.

Thirdly, **on-board application platform**. In this technical solution, the vehicle is considered as a platform where data are stored in the vehicle. The car owner will decide whom to grant access to in-vehicle data to and who is allowed to provide services directly to car users. This platform should support different functionalities directly from the HMI (Kerber, 2018, p. 1).

At the EU level, access and use of in-vehicle data are heavily discussed, 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 specific purpose for the use of the data.

Current EU legal regulation of access to vehicle generated data deals with access to vehicle OBD information[8] and vehicle repair and maintenance information[9] rather than general access to vehicle-generated data or data produced by vehicle users. Vehicle manufacturers are obliged to provide independent operators[10] with unrestricted, standardized, and non-discriminatory access to vehicle OBD information and vehicle repair and maintenance information. However, it must be understood that independent operators do not have remote access to in-vehicle data and resources but rather have access to the results of the diagnostic services. Thus, independent operators are not allowed to provide their repair and maintenance services.

The issue of data access has been widely discussed by Kerber and other commentators (Kerber, 2018; Kerber & Frank, 2018; Kerber & Gill, 2019; Tombal, 2019). Kerber discusses two solutions for the access of data processed within CAV – right to data portability in the Article 20 GDPR and introduction of a new property-like right to access (Kerber, 2018). However, these solutions might not fit the requirement of data access entirely. Firstly, right to data portability is strictly limited in terms of legal grounds and data itself. Article 20 GDPR does not apply to aggregated personal data. Right to portability may be seized only in case of data provided by data subjects or observed by the controller.[11] Additionally, the right in question is limited when personal data is processed on 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.[12] Secondly, the introduction of binding property-like right on machine generated data has not been recommended by the European Commission.[13]

The issue of access is not relevant in cases where the entity is the controller of personal data as it is processing data on its behalf and under its own accountability and liability.

In order to achieve the goal of full automation, it will be necessary to provide easier access to in-vehicle data. In this regard, it will be necessary to define categories of data that can be made available. Furthermore, the purpose for which it is used, and whether such data are used for public interest or commercial interest, must be taken into account.

8. According to art. 3 (49) of the Vehicle type approval regulation, vehicle OBD is information defined as "the information generated by a system that is on board a vehicle or that is connected to an engine, and that is capable of detecting a malfunction, and where applicable, is capable of signalling its occurrence by means of an alert system, is capable of identifying the likely area of malfunction by means of information stored in computer memory, and is capable of communicating that information off-board".
9. Under art. 3 (48) of the Vehicle type approval regulation vehicle repair and maintenance information "means all information, including all subsequent amendments and supplements thereto, that is required for diagnosing, servicing, and inspecting a vehicle, preparing it for roadworthiness testing, repairing, re-programming, or re-initializing of a vehicle, or that is required for the remote diagnostic support of a vehicle or the fitting on a vehicle of parts and equipment, and that is provided by the manufacturer to his authorized partners, dealers, and repairers or is used by the manufacturer for the repair and maintenance purposes".
10. Under art. 3 (45) of the Vehicle type approval regulation, an independent operator is "a natural or legal person, other than an authorized dealer or repairer, who is directly or indirectly involved in the repair and maintenance of vehicles, and includes repairers, manufacturers, or distributors of repair equipment, tools or spare parts, as well as publishers of technical information, automobile clubs, roadside assistance operators, operators offering inspection and testing services, operators offering training for installers, manufacturers and repairers of equipment for alternative-fuel vehicles; it also means authorized repairers, dealers, and distributors within the distribution system of a given vehicle manufacturer to the extent that they provide repair and maintenance services for vehicles in respect of which they are not members of the vehicle manufacturer's distribution system".
11. EUROPEAN DATA PROTECTION BOARD (2019). 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, p. 10.
12. GDPR, art. 20 (1). See GRAEF, I.; HUSOVEC, M.; PURTOVA, N. (2018). "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law". In: *German Law Journal*, vol. 19 no. 6, pp. 1359-1398.
13. See e.g. EUR-Lex-52017DC0009. *Building a European data economy*.

3. Data Protection and Liability in CAV

Based on our above findings, the development, testing and use of CAV entail the processing of a vast amount of data including personal data. As noted by the Dutch Automobile Association ANWB "apart from the automotive industry nobody really knows what data are being collected, stored and shared" (ANWB, 2015). Therefore, we will refer to the extensive work of ACEA on processing of data concerning CAVs.

ACEA distinguishes between various types of data processed by CAV. The first category includes pure technical data related to the vehicle e.g. serial number of vehicles components, version of the software or diagnostic trouble codes. The second category of processed data consists of personal data related to the data subjects, namely usage 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 (European Automobile Manufacturers Association, 2020, p. 6). It is of the essence to note that ACEA conclusions noting that not every piece of data processed within CAV shall be considered as personal data, is not correct. GDPR requires precise testing of reasonable probability when it comes to the identifiability criterion, therefore triggering the application of GDPR in cases where there is a legal reasonable possibility of identification. In practice, this means that the notion of personal data shall be interpreted in a very broad and extensive manner. Due to the extensive interpretation of the notion of personal data, technical data of CAV may be classified as personal data as well.

Another pressing issue that shall be briefly mentioned in this context is the power of the respective data protection authorities to act, considering transborder processing of personal data. Although the principle of one-stop-shop reflects the role of the so-called leading supervisory authority to act in most cases (GDPR, art., 56), several exceptions were recently confirmed by the CJEU.[14] These findings are also relevant considering CAVs transferring personal data to third countries and potential legal claims filed in the EU member states.

3.1. Personal scope of GDPR

Organizations processing personal data fall under the provisions of the EU data protection law represented by GDPR (EUR-Lex- 32016R0679). It is of the essence to establish to whom and under what circumstances data protection laws apply.

Historically, requirements of compliance with data protection laws apply to controllers and processors processing personal data on data subjects. Controllers are entities that solely or jointly determine purposes and means of processing personal data (GDPR, art. 4, 7) and are primal carriers of responsibility for compliance with data protection rules (Van Alsenoy, 2012, p. 25). On the other hand, processors process personal data on behalf of controllers (GDPR, art. 4, 8).

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 (GDPR, art. 4, 1). The recipient is defined broadly as any "natural or legal person, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not" (GDPR, art. 4, 9). Public authorities accessing data in the course of their public tasks are excluded from the definition but may be classified as third parties (GDPR, art. 4, 10).[15]

CAVs represent a robust ecosystem of processing data via various significant processing parties.[16] Guidelines issued by the European Data Protection Board (European Data Protection Board, 2020a) provides the first authoritative interpretation on the classification of various players involved in the data processing of CAVs. Typical data

14. Decision of the CJEU from 15 June 2021 in Case C645/19 Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit.
15. 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 authorised to process personal data".
16. See EUROPEAN DATA PROTECTION BOARD (2020). "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, p. 7-8.

subjects will be passengers of the CAV and an owner or a driver himself. Additionally, 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 manufacturers (European Automobile Manufacturers Association, 2020, p. 6). Examples of controllers include insurance companies, providers of CAV's services or manufacturers of the vehicle processing data for maintenance and development. EDPB's demonstrative lists of processors consist of manufacturers of specific vehicle components processing personal data on behalf of the manufacturers. Commercial partners providing specific services shall be considered recipients (European Data Protection Board, 2020a, p. 9). Public authorities or law enforcement agencies are explicitly recognized by the guidelines as third parties (European Data Protection Board, 2020a, p. 9). However, it shall be noted that the reality of processing personal data is far more complex and it would be confusing to classify them strictly based on the guidelines.[17] The role of data protection authorities shall be emphasized as the authorities will deal with the question in practice. The question of correct attribution of roles and liabilities shall be proposed by data protection authorities considering different processing scenarios and providing a guidance shall not be avoided. For example, considering the guidelines on the processing of personal data in CAVs published by French data protection authority in 2018 (Commission Nationale de l'Informatique et des Libertés, 2018), the analysis of attribution of roles is generally missing in the paper.

3.2. Liability in the GDPR

Defining roles and liabilities is often not an easy task. It must be highlighted that this "binary" setting of the roles of processing operations does not fit the practice in networked environments using new technologies (Kuner, 2017, p. 72). Questions of liability shall be differentiated from issues related to accountability and general responsibility of compliance with GDPR. In general, controllers and processors may face severe sanctions including administrative penalties provided by GDPR in case of non-compliance. However, in this part the primary focus is on liability for damages as the area represents insightful use cases in terms of attributing of roles according to GDPR. This is without prejudice to the possibility of the sanctioning controllers or processors by data protection authorities.

Article 82 (1) the GDPR establishes the basis for liability of damages: "Any person who has suffered material or non-material 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 (Kuner, 2017, pp. 493-495):

1) unlawfulness,
2) damage(s), and
3) causality.

The element of unlawfulness is fulfilled by any infringement of GDPR. In terms of damages, GDPR also explicitly mentions material and non-material damages in the pertinent article. As a final element of the liability regime in GDPR, the causality between unlawful actions of a competent entity and damages shall exist (GDPR, art. 81, 1).[18] CAV processing personal data and causing damages as a result e.g. by preventable unauthorized access of a third party, would fall under the liability regime of the GDPR.

Controllers and liability

As an introductory note, it shall be noted that a "strict" liability regime remains applicable to controllers. The latter is confirmed in 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

17. Similarly, EUROPEAN AUTOMOBILE MANUFACTURERS ASSOCIATION (2020). "ACEA comments EDPB guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", p. 3.
18. "Any person who has suffered material or non-material 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" (GDPR, art. 81, 1).

principle of accountability (GDPR, art. 5, 2).[19] The aforementioned in practice might mean that when the data subject offers evidence of unlawful processing activity, the burden of proof is shifted towards the controller to demonstrate compliance with GDPR (Van Alsenoy, 2016, p. 283). Defining roles concerning CAVs is of fundamental importance and it is suggested that CAVs manufacturers or operators will generally fall under the notion of the controller and related liability regime.

The controller may only escape liability in case 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".

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 GDPR. Obligations for the processor may stem directly from GDPR[20] or from the contract concluded with the controller in compliance with Article 28 (3) GDPR. As per the fact that the processor always acts on behalf of the controller, deviating from the lawful instructions of the controller or data processing agreement form the background for liability of processors.

The legislation provisions a proportional liability regime for processing operations where a processor is involved. However, GDPR provides the option for the processor to be held liable for "the entire damage in order to ensure effective compensation of the data subject" (GDPR, art. 82, 4). Damage may be attributed to the processor only under the condition that the processor's activities during the processing of personal data caused damage and actions related to the damages were either contrary to the 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, GDPR does not contain any threshold when it comes to the degree of responsibility therefore in theory the processor may be held liable for the whole amount of the damage (GDPR, art. 82, 4, supra note 108).[21] This factor is especially relevant when it comes to CAVs as many components processing personal data may be provided by suppliers acting as processors. In case of traffic accidents e.g. caused by insufficient security measures of the component and compromising personal data, processors may be held liable in the sense of the aforementioned liability regime.

Joint controllers and liability

GDPR explicitly recognizes the concept of joint controllers (GDPR, art. 26, 1).[22] Joint controllers shall determine their responsibilities concerning compliance with GDPR in a transparent manner. In terms of liability, it shall be highlighted that based on the wording of GDPR every joint controller may be held liable for damage in the entirety. It is worth noting that Article 83 GDPR does not contain specific rules on allocating fines among joint controllers in case of breach 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 cases Wirtschaftsakademie and Fashion ID further discussed in the next part. Both of the aforementioned decisions reflect the complexity of the correct determination of entities in light of the personal scope of GDPR. What is more, CJEU applies the principle of "effective and complete protection"[23] in light of fundamental rights and freedoms, therefore, aiming to ensure the protection of all potential data subjects affected by the processing of personal data by various parties. As

19. This principle in sum requires controllers to demonstrate compliance with the regulation in two ways. First by fulfilling more formal obligations e.g. maintaining personal data processing records, drafting and publishing privacy policy or internal data protection documentation (security policy or internal data protection policy). Secondly by implementing appropriate organizational and technical measures into data protection practice e.g. identity management, procedures for notification of personal data breaches, or introducing a different level of access to personal data for specific employees.
20. E.g. obligation to maintain records of processing activities based on Article 30 GDPR, notification obligation on the personal data breach to the controller according to the Article 33 (2) GDPR, or appointment of data protection officer per Article 37 GDPR.
21. What is more, the controller has an option to redress – compensation from the processor if it is established that the processor was in breach of GDPR or act out of the scope of the controller's instructions.
22. GDPR reads: "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers" (GDPR, art. 26, 1).
23. See e.g. Mahieu, Van Hoboken & Asghari, 2019, pp. 40-41.

many different parties may be involved in data processing of CAVs, joint controllership shall not be excluded as a possibility for classification of actors processing personal data. However, as noted above, attributing responsibility and liability within joint controllers may be a Sisyphus task as GDPR does not contain specific rules on the matter.

3.3. Defining the roles and liabilities

Three regimes of data sharing within CAV shall be analyzed. Based on these situations, different conclusions regarding roles and liabilities under GDPR may be derived.

"The first situation" shall occur when CAV is connected to the Internet including the processing of data by providers of essential and entertainment applications (V2I – Vehicle to the Internet). Within this situation it is possible to characterize two use cases:

1) connection to the essential services for the functioning of the CAV e.g. GPS navigation and
2) connection to entertainment services e.g. streaming services.

Processing of data during the connection to the essential CAV services shall be perceived as a relationship between the data subject (a driver or an owner of the 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 is obsolete due to the recent decisions of the Court of Justice of the European Union mentioned above. Therefore, it is of the essence to revise the 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 the processing operations.[24] After assessing the details of the processing operations between the provider of the CAV and the provider of the essential services, one may conclude that in some cases joint controllership originates. Additionally, for the origination of joint controllership, the explicit joint determination of means and purposes is not the requirement. It is sufficient if converging decisions with a tangible impact on the determination occur (European Data Protection Board, 2020b, p. 18). Therefore, it is possible that in the case of CAV guidance by the provider of the necessary service, the requirement of converging decisions to determine the purposes and means of processing would be met. As enshrined by EDPB, the mutual benefit of the processing parties is of the essence as well (European Data Protection Board, 2020b, p. 18). As a result, joint controllership would arise. Liability in a given case should be determined in specific cases and specific circumstances. The second case is the connection of 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 CAV shall not have access *in strictu senso* to data processing within this operation, as it is not necessary for the functioning of the CAV.

"The second situation" consists of the communication between two CAV vehicles (V2V – Vehicle to Vehicle) for the prevention of traffic accidents. In our opinion processing of data for this purpose shall be subject to proper anonymization[25] and processed data shall consist of non-personal data related to the distance between vehicles or other technical data. In this case, identifiability of the data subject shall not be possible and GDPR would not be applicable. Furthermore, such an approach would be in line with the data protection by design and by default (European Data Protection Board, 2019).

"The second situation" relates to the connection of CAV with other devices within the Internet of Things infrastructure (V2IoT – Vehicle to the Internet of Things). Again, we may discuss two model situations in this context:

1) connection to cooperative – intelligent transportation system (C-ITS) and
2) 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 ensure compliance with road traffic regulations. Communication between vehicles is not excluded in

24. Decision of the CJEU from 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case n., C210/16, § 43.
25. See Data Protection Working Party (2014). *Opinion 05/2014 on Anonymisation Techniques*, article 29.

this case (Žolnerčíková, 2020, pp. 129-152). When discussing the connection C-ITS, the question of status and liability in terms of GDPR arises again. Is this the case of separate controllers or joint controllership? In our opinion, it is again possible that in the light of the recent case law of the CJEU, practice will have to assess this relationship as joint controllers. We base this conclusion on two arguments. The first argument is that 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 economically inevitable and important to the provider of CAV, as without respecting traffic laws it would be impossible to gain 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 the 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 fits his processing activities within the boundaries provided by the social network (e.g., in the form of ad 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 CAB and operators of the infrastructure as required by Article 26 of the GDPR. At present, it is impossible to predict how the judiciary and practice will deal with this issue.

The second modality within the third regime is the use of data by public authorities for purposes of conducting administrative or criminal proceedings. Public authorities shall be classified as recipients and separate controllers of data. Concerning this situation, the reference may be made to German regulation, which explicitly regulates the access and use of data from the so-called black boxes for autonomous vehicles (Czarnecki, 2017, § 63a).

Conclusions

Fully automated vehicles are a matter of the future. However, connected and partially automated vehicles are a current legal issue due to their development and deployment. The EU aims to provide a CAVs manufacturers sound legal environment and become the leader in regulatory innovations and attract economic stimulations. It is of the essence to note that the development of C-ITS is also backed by the legislation and connectivity and the inclusion of CAVs within the system is one of the cornerstones of future smart and connected mobility.

Data processing and related data governance is fundamental to the development and use of CAV. As discussed in the article, manufacturers of CAVs are quite reluctant to allow access to data for third parties. The current legislation provisions ensure access only to maintenance and repair data for independent operators. However, further access rights may be overridden by independent controllers of personal data due to their controllership rights.

In terms of the position of the various actors in the processing of personal data in a CAV, we primarily discussed the current interpretation of the concepts of the controller, processor, and their liability with regards to the recent case law of the CJEU. Based on the definition and analysis of three models, we have pointed out that in several cases of personal data processing within the CAV, it is extremely demanding to determine a 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 discussed vehicles. A microscopic view of processing operation through the lens of the CJEU is not the most appropriate solution for the definition of relationships concerning CAVs. It is therefore possible that the future will lead to very complicated legal questions with no simple or positive consequences with regard to the processing of personal data.

Acknowledgements

This paper was prepared on behalf of Jean Monnet Network Project 611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK "European Union and the Challenges of Modern Society". This paper represents the shorter preliminary version of the study published in a special issue of Sustainability (vol. 13, no. 19) on Vehicular Communications for Sustainable Mobility and Transportation. For details see: ANDRAŠKO, J.; HAMUĽÁK, O.; MESARČÍK , M.; KERIKMÄE, T.; KAJANDER, A. (2021). Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union. Sustainability, vol. 13, 10610. https://doi.org/10.3390/su131910610. The present version covers approximately 40% of the later comprehensive study.

References

ACEA (2016). "Access to vehicle data for third-party services". In: *ACEA Position Paper*, pp. 3 [online]. Available at: https://www.acea.auto/files/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf

ANDRAŠKO, J.; HAMUĽÁK, O.; MESARČÍK, M.; KERIKMÄE, T.; KAJANDER, A. (2021). "Sustainable Data Governance for Cooperative, Connected and Automated Mobility in the European Union". In: *Sustainability*, vol. 13, no. 19, p. 10610. DOI: https://doi.org/10.3390/su131910610

ANWB (2015). "Onderzoek naar verzamelen, opslaan, gebruiken en verzenden van data door auto's" [online]. Dutch Automobile Association. Available at: https://www.anwb.nl/binaries/content/assets/anwb/pdf/auto/connected-car/my-car-my-data---adac---fia-test-data-in-auto.pdf

BSI (2020). "Connected and automated vehicles. Vocabulary BSI Flex 1890 v3.0:2020-10". In: *BSI* [online]. Available at: https://www.bsigroup.com/globalassets/localfiles/en-gb/cav/bsi-flex-1890-v3-2020-10.pdf

COLLINGWOOD, L. (2017). "Privacy implications and liability issues of autonomous vehicles". In: *Information & Communications Technology Law*, vol. 26, no. 1, pp. 32-45. DOI: https://doi.org/10.1080/13600834.2017.1269871

Commission Nationale de l'Informatique et des Libertés (2018). "Connected vehicles: a compliance package for a responsible use of data" [online]. Available at: https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data

CORDEIRO, A. B. M. (2019). "Civil Liability for Processing of Personal Data in the GDPR". In: *European Data Protection Law Review*, no. 4.

CZARNECKI, K. (2017). "English Translation of the German Road Traffic Act Amendment Regulating the Use of Motor Vehicles with Highly or Fully Automated Driving Function". In: *ResearchGate* [online]. Available at: https://www.researchgate.net/publication/320813344 [Accessed: 25 April 2021].

DG GROW (2017). "GEAR 2030: High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union. Final Report". In: *DocsRoom European Commission* [online]. Available at: https://www.europarl.europa.eu/cmsdata/141562/GEAR%202030%20Final%20Report.pdf.

EUROPEAN AUTOMOBILE MANUFACTURERS ASSOCIATION (2020). "ACEA comments EDPB guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", p. 6.

EUROPEAN DATA PROTECTION BOARD (2019). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

EUROPEAN DATA PROTECTION BOARD (2020a). *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.

EUROPEAN DATA PROTECTION BOARD (2020b). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Version 1.0. Adopted on 02 September 2020.

FRISONI, R. *et al*. (2016). "Research for TRAN Committee. Self-Piloted Cars: The Future of Road Transport?". In: *European Parliament Think Tank* [online]. Available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2016)573434

GERMANY. Road Traffic Act. Federal Law Gazette I, last amended by Article 6 of 17 August 2017, p. 3202.

KALA, R. (2016). *On-Road Intelligent Vehicles. Motion Planning for Intelligent Transportation Systems*. Oxford: Butterworth-Heinemann, pp. 536.

KASPER, A.; KRASZNAY, C. (2019). "Towards Pollution-Control in Cyberspace: Problem Structure and Institutional Design in International Cybersecurity". In: *International and Comparative Law Review*, vol. 19, no. 2, pp. 76-96 [online]. DOI: https://doi.org/10.2478/iclr-2019-0015

KERBER, W. (2018). "Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data". In: *JIPITEC*, no. 9, pp. 310.

KERBER, W.; FRANK, J. S. (2018). "Data Governance Regimes in the Digital Economy: The Example of Connected Cars" [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064794 [Accessed: 25 April 2021]

KERBER, W.; GILL, D. (2019). "Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation". In: *JIPITEC*, no. 10, pp. 244 [online]. Available at: https://www.jipitec.eu/issues/jipitec-10-2-2019/4917

KUNER, CH. (2007). *European Data Protection Law. Corporate Compliance and Regulation*. 2nd. ed. Oxford: Oxford University Press.

LAROUCHE, P.; PEITZ, M.; PURTOVA, N. (2016). "Consumer Privacy in network industries. A CERRE Policy Report". In: *Centre on Regulation in Europe*.

MAHIEU, R.; HOBOKEN VAN, J.; ASGHARI, H. (2019). "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". In: *JIPITEC*, no. 39. DOI: https://doi.org/10.2139/ssrn.3256743

MATTESON S. (2020). "Autonomous versus automated: What each means and why it matters". In: *Tech Republic* [online]. Available at: https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/ [Accessed: 25 April 2021].

OECD/ITF (2015). "Automated and Autonomous Driving: Regulation under uncertainty" [online]. Available at: https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf [Accessed: 25 April 2021]

SAE (2016). *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, J3016_201609 [online]. Available at: https://www.sae.org/standards/content/j3016_201609/

SKIHO, K.; SHRESTHA, R. (2020). *Automotive Cyber Security. Introduction, Challenges, and Standardization* [online]. Singapore: Springer. DOI: https://doi.org/10.1007/978-981-15-8053-6

TOMBAL, T. (2019). "GDPR as shield to a data sharing remedy?". *ASCOLA 2020 Conference* [online]. University of Namur - CRIDS/NaDI. Available at: https://law.haifa.ac.il/images/ASCOLA/Tombal.pdf.

VAN ALSENOY, B. (2012). "Allocating responsibility among controllers, processors, and 'everything in between': the definition of actors and roles in Directive 95/46/EC". In: *Computer Law and Security Review*, no. 28 [online]. DOI: https://doi.org/10.1016/j.clsr.2011.11.006

VAN ALSENOY, B. (2016). "Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation". In: *JIPITEC*, no. 7, pp. 271 [online]. Available at: https://www.jipitec.eu/issues/jipitec-7-3-2016/4506

VAN ALSENOY, B.; DUMORTIER, J. (2012). "The accountability principle in data protection regulation: origin, development and future directions". In: GUAGNIN, D. *et al*. (eds). *Managing Privacy Through Accountability*. London: Palgrave Macmillian.

YEEFEN LIM, H. (2018). *Autonomous Vehicles, and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, p. 4-5.

ŽOLNERČÍKOVÁ, V. (2020). "Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly". In: *Revue pro právo a technologie*, no. 21, pp. 129-152 [online]. DOI: https://doi.org/10.5817/RPT2020-1-6

Legal resources

Decision of the CJEU from 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case n. C210/16.

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.

Decision of the CJEU from 29 July 2019, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV. Case n. C40/17.

EUR-Lex-32002L0058. *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)*.

EUR-Lex-32010L0040. *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*.

EUR-Lex-32016R0679. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. OJ L 119, 4.5.2016, p. 1-88.

EUR-Lex-32018R0858. *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 (Text with EEA relevance)*. PE/73/2017/REV/1. OJ L 151, 14.6.2018, p. 1-218.

EUR-Lex-32019R2144. *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 (Text with EEA relevance)*.

EUR-Lex-52016DC0766. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*.

EUR-Lex-52018DC0283. *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*.

EUR-Lex-C/2019/1789. *COMMISSION DELEGATED REGULATION (EU) .../... supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems*.

Recommended citation

ANDRAŠKO, Jozef; HAMUĽÁK, Ondrej; MESARČÍK, Matúš (2021). "The digital development of the European Union: data governance aspects of cooperative, connected and automated mobility". *IDP. Internet, Law and Politics E-Journal*. No. 34. UOC [Accessed: dd/mm/aa]
http://dx.doi.org/10.7238/idp.v0i34.387494

About the authors

JUDr. Jozef Andraško, Ph.D.
Assistant professor
Institute of the Information Technology Law and Intellectual Property Law
Comenius University in Bratislava, Faculty of Law
jozef.andrasko@flaw.uniba.sk

JUDr. Ondrej Hamuľák, Ph.D.
Senior lecturer
Faculty of Law, Palacký University Olomouc, Czech Republic
ondrej.hamulak@upol.cz

JUDr. Matúš Mesarčík, Ph.D., LL.M
Assistant professor
Institute of the Information Technology Law and Intellectual Property Law
Comenius University in Bratislava, Faculty of Law
matus.mesarcik@flaw.uniba.sk