EJPLT

Consideration of privacy aspects in the area of highly automated driving. An intention recognition use case

LIVIA AULINO
Ph.D. Candidate at the University Suor Orsola Benincasa of Naples
MARCEL SAAGER
M.Sc., Modelling & Software Engineer at Humatects GmbH
MARIE-CHRISTIN HARRE
HMI Engineer at Humatects GmbH
LEONARDO ESPINDOLA
Industrial Designer at Humatects GmbH[1]

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

Autonomous driving is increasingly becoming an issue in the development of modern vehicles. Above all, aspects such as safety and comfort are encouraging carmakers to embed highly automated driving in their latest developments. Due to the increasing complexity and the fact that it is often not clear how and for what purpose user data is processed, it is important to take a closer look at the legal and data protection aspects. For this purpose, a use case has been selected from the AutoMate project, on the basis of which current case law is to be applied in an exemplary manner.

Keywords Autonomous driving - Data processing - Data protection law - Human-Machine Interaction

Summary: Introduction. – 1. The Use Case: Intention Recognition. – 2. Related Work: Legal Aspects in the field of highly automated driving. - 3. Privacy Aspects in the underlying use case. – 3.1. First Phase: to set up whether the processing of the collected data falls within the scope of the GDPR. – 3.2. Second Phase: to apply GDPR regulation, if the data collected are not anonymous. – 3.3 How to ensure that the processing is in compliance with the GDPR. – 3.4. Third phase: to set up whether it is also necessary to collect a consent of data subjects. – 4. Data processing in AutoMate. – Conclusions.

Introduction.

The latest developments in the field of autonomous driving are progressing rapidly[2].

In order to make autonomous driving possible, many values must be recorded by sensors and processed by the automation system. Sensitive data is often collected in this process, which reflects information about the driver and his or her user behavior[3].

For this reason, it is particularly important to consider not only technical advances in the

[1] Livia Aulino wrote paragraphs n. 2 - 3 - 3.1 - 3.2 - 3.3 - 3.4; Marcel Saager wrote Introduction and paragraphs n. 1 - 4; Marie-Christin Harre wrote Introduction and paragraphs n. 1- 4; Leonardo Espindola designed Figure 1 and Use Case. This paper comes from the research activity carried out by PhD. candidate at University Suor Orsola Benincasa with members of Research center Humatects (*https://www.humatects.de*).

[2] J Janai, F Güney, A Behl, A Geiger, 'Computer Vision for Autonomous Vehicles: Problems, Datasets and State of the Art', (2020) in *Foundations and Trends® in Computer Graphics and Vision*, 12:1–3, 1,308.

[3] J Varghese, RG Boone, 'Overview of Autonomous Vehicle Sensors and Systems. Overview of Autonomous Vehicle Sensors and Systems' (2015).

field of autonomous driving, but also legal aspects. Examples for the applications of these systems range from software in the aviation domain over shipping to vehicles[4].

This paper will look at the legal aspects of recording and processing sensor data for autonomous driving in more detail: a use case from the "AutoMate" project is used for this purpose.

This use case will be described in the following paper. Afterwards, the legal aspects and in particular privacy aspects of the use case will be considered in detail. The paper concludes with an examination of the problems related to the collection and processing of data inside the vehicle, and with a proposed solution for the use case.

1. The Use Case: Intention Recognition.

The use case considered in this paper originates from the european project "AutoMate" (*www.automate-project.eu*). AutoMate aims at developing the so-called "TeamMate" car in which driver and automation have to be considered as team members who share the driving task and who are both responsible for the safety of driving[5]. The scenario deals with a use case in which the fictitious person named Peter drives along a narrow rural road in Manual Mode.

The scenario is exemplarily shown in Figure 1 on the left. Peter approaches a tractor, that causes limited visibility on the road. The TeamMate car detects a car approaching from the opposite lane.

Since Peter is not aware of the car, he decides to overtake, and the TeamMate car detects his intention. In order to avoid an imminent collision, the TeamMate car informs Peter about the approaching vehicle and warns him about the risky manoeuvre. This is shown in Figure 1 on the right side. Peter suddenly becomes aware of the risk, and he does not perform the overtake until it is safe[6].

This use case was selected because it can be addressed highly autonomously driving and it can be investigated to what extent and whether user data is collected and processed.

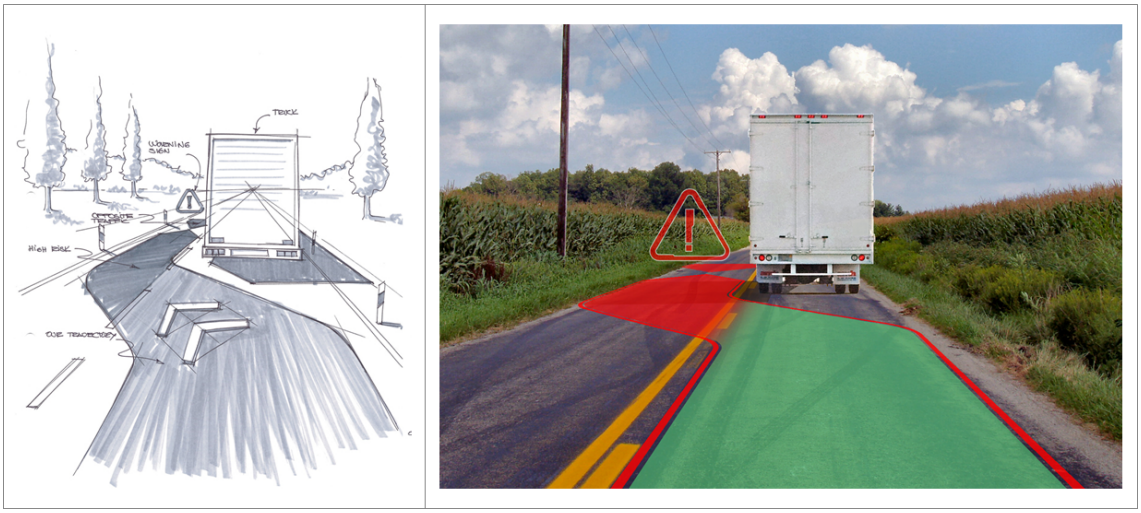

Fig.1: The Scenario.

[4] V Ilková - A Ilka, 'Legal aspects of autonomous vehicles - an overview' (2017) *Proceedings of the 2017 21st International Conference on Process Control* (Strbske Pleso 2017), 6-9, 428,433.

[5] AutoMate: Automation as accepted and trusted TeamMate to enhance traffic safety and efficiency, Website: *www.automate-project.eu*.

[6] MR Endsley, 'Situation Awareness in Future Autonomous Vehicles: Beware of the Unexpected' in *Proceedings of the 20th Congress of the International Ergonomics Association* (IEA 2018).

The Use Case considered here is situated in highly automated driving. This means in *highly automated driving* the vehicle has its own intelligence that plans ahead and can take over the driving task from humans in most situations.

Human and machine control the vehicle together, but the human driver can determine at any time to what extent he or she or the artificial intelligence takes over tasks. Examples of this are ESP and ABS. In contrast to that, *driving assistance systems* must be delimited.

They are additional modules in vehicles that are intended to support the driver in certain situations. The control is not relinquished. The focus is on safety and driving comfort. One example of this is the parking aid, which can support the driver in the process with the help of acoustic feedback.

The SAE International, Society of Automotive Engineers, defines further levels of driving modes, which will be described in the following. *Partial Driving Automation* is defined as advanced driver assistance systems that can take over steering and acceleration, for example.

Nevertheless, the human driver can intervene from the driver's seat at any time and take total control of the vehicle.

With *Full Driving Automation*, the vehicle takes over the entire dynamic driving task. Human attention and situational awareness are no longer necessary. There are currently no fully automated vehicles for normal road traffic[7].

2. Related Work: Legal Aspects in the field of highly automated driving.

The success of autonomous driving will depend on the ability to create a solid human-machine team as well as on the quality of interaction, communication and cooperation. This cooperation fully exploits the potential of automation to improve human life.

The interface also provides legal information the driver needs and precisely on: privacy and data protection (security of the data processed; lawfulness of processing; ownership); shared control (visual icons that tell the user the possibility of a risk); support and mutual learning.

The interfaces should not only content the legal and ergonomic technical needs but should also consider the experience and quality of the interaction. These should be understandable and easy to use.

Therefore, the design of interfaces requires a multidisciplinary approach that combines law, design and technology. This approach ensures that information is provided in a legal manner and in compliance with technical and HMI requirements.

In this perspective it is believed that the legal design[8] methodology is the most suitable in the design of sensor systems of autonomous driving, in order to guarantee their self-awareness. This methodology represents a possible remedy to the communication deficit of legal information provided in the car.

In fact, the solution can be seen in the opportunity to design human machine interfaces, which - also through a signalling acoustic, visual or tactile - provide legal information clearly

---

[7] SAE Standards News: J3016 automated-driving graphic update, Website: *https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.*

[8] The notion of legal design was coined by Margaret Hagan. Legal design is the application of human-centred design to the world of law, in order to promote the usability and comprehensibility of legal instruments, and in particular contracts. Legal design is a method of creating legal services, focusing on their usability, utility and involvement. It is an approach with three main resource groups - process, mentality and mechanics - to be used for legal professionals. These three resources can help conceive, build and test better methods of legal action, which will involve and empower both legal professionals and individuals. The design phases of this methodology are: framing the situation; focusing on the type of user/consumer; developing ideas; understanding and prioritizing; developing a prototype; testing. See M. Hagan, 'Law by Design' (Retrieved March 2018), in *www.lawbydesign.co/en/home/*

and unambiguously on the autonomous vehicle. This in order to guarantee a security by design and to ensure support and mutual learning between the car and the user.

Incorporating legal regulations into the design phase can improve - or automate - their ex ante application. Thus, the problem of technological development that often hinders the regulatory efforts of legislators can be prevented. It might seem like a complex change, but it is actually easier to adopt adequate protection solutions from the start than to apply privacy considerations after a project is fully developed

The use case in question needs an in-depth study on the processing of data operated by the TeamMate car.

3. Privacy Aspects in the underlying use case.

The reference legislation is General Data Protection Regulation (Reg. UE 679/2016 – GDPR)[9], which has been in force since 2018 in all EU member States. It applies in any case where data processing in the context of connected vehicles[10] involves processing personal data of individuals.

Additionally to regulations provided by the GDPR, we can find other standards in the "ePrivacy" directive (2002/58/EC, as revised by 200/136/EC), a directive that is aimed to discipline all those actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA).

But, even if it is true that most of the "ePrivacy" directive provisions (art. 6, art. 9, etc.) is tailored for and only applies to providers of publicly available electronic communication services and providers of public communication networks, however we can find a general provision in the art. 5 of the ePrivacy directive. In fact, it does not only apply to electronic communication services but also to every entity that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed.

As a predictable result, a connected vehicle, and every device connected to it, shall be considered as a terminal equipment (just like a computer, a smartphone or a smart TV) and, following this statement, provisions of art. 5 ePrivacy directive must apply where relevant.

A number of issues need to be analysed in relation to the use case in question.

The first concerns establishing whether the processing of the data collected falls within the scope of the GDPR.

3.1. First Phase: to set up whether the processing of the collected data falls within the scope of the GDPR.

First of all, it is necessary to clarify what is meant by personal data.

Recital 26 of GDPR states that *the principles of data protection should apply to any information*

[9] The General Data Protection Regulation No. 2016/679, hereinafter GDPR (General Data Protection Regulation) is the European legislation on privacy and protection of personal data. It was published in the European Official Journal on 4 May 2016, and entered into force on 24 May 2016, but its implementation took place on 25 May 2018. Its main purpose was to harmonise the rules on the protection of personal data within the European Union.

[10] According to the European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, adopted on 28 January 2020, the connected vehicle definition has to be understood as a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle to assist drivers is included in the scope of this document since they contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data with the vehicle.

concerning an identified or identifiable natural person[11].

Most data associated with connected vehicles will include technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). At present, the EDPB[12] has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations.

More specifically the personal data could be processed inside the vehicle, exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or collected within the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.

Also, the Article 4 of GDPR states that 'personal data' is *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Therefore, non-anonymous data fall within the scope of the GDPR.

So if the data used in the AutoMate project were completely anonymous and not attributable in any way, neither directly nor indirectly to a natural person, then the GDPR does not apply.

Consequently, there is no need to release the privacy information and collect consent to data processing.

3.2. Second Phase: to apply GDPR regulation, if the data collected are not anonymous.

More generally, the paper examines the case in which the data collected and processed were not anonymous but were equipped with any information "*attributable directly or indirectly to a natural person*", in this case, the GDPR applies.

In this regard, the Articles 1[13] and 4,1[14] paragraph states that in the Regulation there are

---

[11] Recital 26 of GDPR: *The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.*

[12] European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, adopted on 28 January 2020.

[13] Article 1 of GDPR: *1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.*

[14] Article 4,1 of GDPR: "*personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

the rules relating to the processing of personal data, that means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

For example, the data that can be traced through some encryption (e.g. if the user is identified with a number) are not anonymous.

Consequently, if the data were pseudonymous, it is necessary to understand whether data processing is ongoing.

In particular, according to the recital 18[15] and article 2,2, c)[16], the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. This includes the case where the vehicle collects personal data, but is not passed on to third parties. In this case, the data are processed only for personal purposes. Therefore, it is not a processing for which the principles of the GDPR apply, as provided for in recital 18 and art. 2 of the same Regulations.

It is different if the data are not processed exclusively by the owner of the vehicle, but in some way by a third party. In this case it falls within the concept of treatment, as laid down in Article 4, paragraph 2[17].

Once it is established that there is an ongoing processing, then it is necessary to understand who are the subjects of the processing. More specifically:

- The data subject is the natural person owning personal data. So the data subject is not only the owner of the vehicle, but it is also anyone who provides their personal data, using the vehicle. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle[18].
- The data controller, according to article 4, 7 of GDPR is *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*, that take place in connected vehicles.

Data controllers can include service providers that process vehicle data to send the driver

---

15 Recital 18 of GDPR: *"This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities".*

16 Article 2 of GDPR - Material scope: "*1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: a) in the course of an activity which falls outside the scope of Union law; b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; c) by a natural person in the course of a purely personal or household activity; d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. 3.No data shall be adapted to the principles and rules of this Regulation in accordance with Article 98. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal. 4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive*".

17 Article 4,2 of GDPR: *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

18 As it was identified by European Data Protection Board, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, adopted on 28 January 2020.

traffic-information, eco-driving messages or alerts regarding the functioning of the vehicle, insurance companies offering "Pay As You Drive" contracts, or vehicle manufacturers gathering data on the wear and tear affecting the vehicle's parts to improve its quality[19].

In addition, it is necessary to understand whether the processing complies with the principles of the GDPR. The data of data subjects could be collected and processed also by more than one third party and in this case, it will be necessary to establish the role of these subjects.

Therefore, it will be necessary to determine whether it is:

- Joint controllers are two or more controllers jointly that determine the purposes and means of processing (art. 26 of the GDPR[20]). In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information as referred to in art. 13 and 14 GDPR.
- Or a data processor who manages the data in the interests of the data controller. According to the article 4,8 the 'processor' is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

E.g. the data could be collected and processed not only by the vehicle manufacturer but also by a third party (e.g. a research centre) which is responsible for the development of vehicle technologies. As another example, in several cases, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, the art. 28 GDPR sets out obligations of data processors.

For this reason, it is important to establish the roles of the various entities also in order to guarantee the rights of the data subjects and to provide the related information.

3.3 (Cont.) How to ensure that the processing is in compliance with the GDPR.

For the processing is in compliance with the GDPR it is necessary that:

- the data controller must provide the information to the data subjects. The article 12 of the GDPR provides that the data controller adopts appropriate measures to provide the data subject with all the information referred to in articles 13[21] and 14

---

[19] *Ibidem.*

[20] Article 26 of GDPR - Joint controllers: "*1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects. 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject. 3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers*".

[21] Article 13 of GDPR: Information to be provided where personal data are collected from the data subject. "*1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they

and in the communications pursuant to arts. 15 to 22 and to the art. 34 relating to processing in a concise, transparent, intelligible and easily accessible form, with simple and clear language, in particular in the case of information specifically intended for minors[22].

- the rights of data subjects must be guaranteed and precisely: right of access by the data subject; rectification and erasure; right to rectification; right to erasure ('right to be forgotten'); right to restriction of processing; notification obligation regarding rectification or erasure of personal data or restriction of processing; right to data portability; right to object and automated individual decision-making; right to object; automated individual decision-making, including profiling.
- In addition, the data controller must provide adequate security measures to ensure the protection and safeguard of the right processing.

In fact, according to the article 5, par. 1, lett. f) of GDPR[23], the security of the entire processing must be guaranteed, not just the data as a final product. Furthermore, article 32[24] establishes some fundamental principles on security measures, specifying that they must be adapted to the individual situation. In particular, security measures are divided into two categories: organizational measures and technical measures (such as pseudonymisation and encryption of personal data and security requirements)[25].

---

have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information".

[22] IA Caggiano, '*Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*' (2018) *Familia* 3,23.

[23] Article 5, par. 1, lett. f) of GDPR: "*Personal data shall be: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

[24] Article 32 of GDPR - Security of processing: "*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of* personal *data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for* regularly *testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law*".

[25] F Pizzetti, *Privacy ed il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/48 al nuovo Regolamento europeo*, (Giappichelli 2016) 153.

The European regulation takes an approach based on risk assessment rather than user protection. Therefore, a correct risk analysis of the processing of personal data is appropriate in order to implement adequate security measures[26].

Consequently, in case of data processing, the information had to be provided and must be guaranteed the rights of the data subject, by articles 15 to 22.

In general, the data controller must also act in accordance with the principles of "privacy by design and privacy by default" introduced by the GDPR[27]. According to these principles it would be appropriate to provide that the technologies underlying the connected vehicles are made (from the design phase) in such a way as to minimize the collection of personal data and to ensure that the data subjects, in addition to being adequately informed, to be able to easily change any setting associated with the personal data.

In this regard it should be noted that, at the national level, the German Federal Data Protection Act of 1990, predating the GDPR, already came close to this principle. In fact, the third section of the law, named "*Datenvermeidung und Datensparsamkeit*"[28] (deletion of data and data economy), established to design information systems with the aim of processing as little personal data as possible. Furthermore, it stated that personal data must be pseudonymised or anonymized as far as reasonable in relation to the desired level of protection.

3.4. Third phase: to set up whether it is also necessary to collect a consent of data subjects.

The paper will present what the legal basis of the data processing is.

Processing shall be lawful only if and to the extent that at least one of the following applies provided by article 6[29].

---

[26] Art. 32, par. 2, lists some types of risk: accidental or unlawful destruction or loss of data; modification; unauthorized disclosure; accidentally or illegally or not authorized access.

[27] G D'Acquisto - M Naldi, *Big Data e Privacy by Design* (Giappichelli 2017).

[28] § 3a Datenvermeidung und Datensparsamkeit - Bundesrepublik Deutschland Bundesdatenschutzgesetz a.F. (Expired on May 25, 2018 due to the law of June 30, 2017 (Federal Law Gazette I p. 2097) § 3a) in *https://dejure.org/gesetze/BDSG_a.F./3a.html.*

[29] Article 6 of GDPR states that: the processing is lawfulness if: *(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (b) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX. 3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific. 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been*

In particular, in the case of the processing of data that are necessary for the operation of the vehicle, consent does not need to be collected, because the legal basis of the processing falls under art. 6, let. b., as necessary for the performance of the contract.

In case the processing for a purpose other than that for which the personal data have been collected is not based on the consent of data subject, according to the article 6, par. 4,

the controller have to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected. Precisely the controller shall to take into account: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Moreover, there is the case in which the data are collected, also in automated form, for the development of technologies similar to those purchased and used by the data subjects.

For example, through big data systems, such data could be collected to develop further technologies. In this case, depending on whether the requirements of art. 6, par. 4, you may need to seek consent to collect additional data unrelated to the purpose of the contract.

In other cases, when the purpose is completely unrelated to the purpose for which they were collected (e.g. for marketing purposes or for advertising), the consent of the data subject needs to be collected[30].

As well as when sensitive data are processed, IE those indicated in art. 9[31]. This even when

---

collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

[30] On the point see: L Gatt, R Montanari, IA Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali', (2017) II *Politica del diritto* 363 ff.; MC Gaeta, 'La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi' (2018) 1 Dir. inf. e informatica, 147 ff.; MC Gaeta, 'The issue of data protection in the Internet of Things with particular regard to self-driving cars' (2017) DIMT 1 ff.; IA Caggiano, 'Il consenso al trattamento dei dati personali' (2017) *DIMT online* 12 ff; L Aulino 'Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come rimedio ex ante' (2020) II *Diritto dell'informazione e dell'informatica* 303,312.

[31] Art. 9 of GDPR - Processing of special categories of personal data: "*1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be*

it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 9 let. j of GDPR.

As recently outlined by the EDPB in its opinion 5/2019[32] on the interplay between the "ePrivacy" directive and the GDPR,13 art. 5,3 ePrivacy directive provides a rule that shall take precedence over art. 6 GDPR, with regards to the activity of storing or gaining access to those information already stored in the terminal equipment of a subscriber or user. In fact, this article states that prior consent is required for the storing of information, or the gaining of access to this class of information.

However, we can say that the personal data obtained by accessing information in the terminal equipment, must additionally have a legal basis under art. 6 GDPR in order to be lawful.

Since the controller has a duty to inform the data subject about all the purposes of the processing when seeking consent for the storing or gaining of access to information pursuant to art. 5,3 ePrivacy directive, the consent will normally also cover such processing operations.

Because of that, consent gained will likely constitute the legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the aforementioned processing operations.

So, as we can see, the data processing as a whole involves specific activities for which the Eu legislature has sought to provide additional protection. That's why controllers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis between the GDPR and the ePrivacy directive, in order to respect the principle of fairness. And there is a bottom line: art. 6 GDPR cannot be relied upon by controllers in order to lower the additional (and better) protection provided by art. 5,3 ePrivacy directive.

The EDPB recalls that the ePrivacy directive shares the same notion of consent as described in the GDPR and must meet all the requirements of the consent as provided by art. 4,11 and 7 GDPR.

However, art. 5,3 ePrivacy directive allows the processing of information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, but only if it satisfy one of the following criteria:

- Exemption 1: for the sole purpose of carrying out the transmission of a communication over an electronic communication network;

---

proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. (j) ***processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*** *in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. 3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health".*

[32] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, in *https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.*

- Exemption 2: when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

In such cases, the processing of personal data, those data already stored in the terminal equipment, falls under art. 6 GDPR's provisions.

Therefore, it may be considered unnecessary to collect the consent of data subjects only in certain specific cases, although it is more appropriate to collect consent.

4. Data processing in AutoMate.

In the AutoMate project, as described in chapter 2, a so-called AutoMate was developed to support the driver in special situations. For the present scientific work, a use case was used to investigate the extent to which case law is applicable to the Automate Assistant.

Since data protection and the use of data are at the center of this, this chapter must first clarify which data is used and how it is processed.

In the given example, the Protagonist Peter is driving the Car and could be supported by the AutoMate. To show Peter the HMI in Figure 1, the automation system acquires certain sensor values. These values can be subdivided in three categories: *Environmental data*, *explicit user data* and *implicit user data*.

Environmental data includes all data collected by the sensor system in the environment - independently of the driver in the environment. This includes e.g. the car coming from the front, the truck or the driven speeds.

In addition, *implicit user data* are also recorded for the application under consideration. These are for example information about the use of the system itself but also conclusions about the driving behaviour.

Explicit user data such as eye positions, tracking of emotions etc. are not yet recorded. However, these are under strong discussion for future applications.

Sensor data necessary for the AutoMate is stored in a temporary buffer after use for the HMI. For the model of the AutoMate, data in the model is processed anonymously so that the model changes. In this case, however, it is not possible to speak of a classic persistence of data, since the data is not written to a database[33].

Conclusions.

Given that the data used in the AutoMate experiment were completely anonymous and not attributable in any way, neither directly nor indirectly to a natural person, then the GDPR does not apply.

Consequently, there is no need to release the privacy information or collect consent to data processing.

If in the future data will be collected in any form that can be considered personal, according to the definitions of the GDPR, then it has to consider all the assessments that have been reported in the previous paragraphs to ensure compliance with processing in accordance with the GDPR.

Secondly, this study showed the importance of a multidisciplinary approach in the autonomous driving design that combines law, design and technology. Infact, incorporating legal regulations into the design phase can improve their ex ante application.

Furthermore, in this matter, it emerges the importance of introducing a code of conduct that can improve the application in every process of the principle of privacy by design and by default, ensuring adequate protection for the rights and freedoms of the data subjects

[33] M Eilers - E Fathiazar – Suck – T Stefan - D Twumasi, 'Dynamic Bayesian networks for driver-intention recognition based on the traffic situation' in *Cooperative Intelligent Transport Systems: Towards high-level automated driving* (Transport, IET Digital Library 2019), 465,495.

right from the design phase of the vehicle processing and construction.