Grant Agreement Number: 731993

Project acronym: AUTOPILOT

Project full title: AUTOmated driving Progressed by Internet Of Things

D4.10

Legal perspectives on the use of IoT for AD

Final delivery date: 31/12/2019

Actual delivery date: 23/12/2019

Organization name of lead participant for this deliverable: ERTICO – ITS Europe

Project co-funded by the European Commission within Horizon 2020 and managed by the European GNSS Agency (GSA)		
Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Project funded by the European Union's Horizon 2020 Research and Innovation Programme (2014 – 2020).

Document Control Sheet

Deliverable number:	D4.10
Deliverable responsible:	ERTICO - ITS Europe
Work Package:	WP4
Editor:	Thomas Desseilles

Author(s) – in alphabetical order

Name	Organisation	E-mail
Alejandro Manilla	IDI	Alejandro.Manilla@idiada.com
Francois Fischer	ERT	f.fischer@mail.ertico.com
Haibo Chen	UNL	H.Chen@its.leeds.ac.uk
Jean-François Siméon	CONTI	Jean-Francois.Simeon@continental-corporation.com
Jo-Ann Pattinson	UNL	J.M.Pattinson@leeds.ac.uk
Johan Scholliers	VTT	Johan.Scholliers@vtt.fi
Jordanne Monseau	CONTI	jordanne.monseau@continental-corporation.com
Jordi Pont	IDI	jordi.pont@idiada.com
Joseph Allard	ERT	j.allard@mail.ertico.com
Ralf Willenbrock	TSI	Ralf.Willenbrock@t-systems.com
Rita Bhandari	ERT	r.bhandari@mail.ertico.com
Romina Quaranta	TSI	Romina.Quaranta@t-systems.com
Thomas Desseilles	ERT	t.desseilles@mail.ertico.com
Yassine Banouar	CONTI	yassine.banouar@continental-corporation.com

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	**Modified by**
v01	08/01/2019	Version of the document compiled for Legal Experts review#1, based	Joseph Allard, ERTICO-ITS Europe

		on D4.9.	
v02	22/02/2019	Intermediate version consolidating the Legal experts reviews	Joseph Allard, ERTICO- ITS Europe
v03	17/10/2019	Integration of inputs (Livorno workshop, Legal experts, Webinar1, State-of-the-Art) and of partners' contributions1	Thomas Desseilles, ERTICO-ITS Europe, Jordi Pont Idiada, Alejandro Manilla Idiada, Jo-Ann Pattinson University of Leeds, Haibo Chen University of Leeds, Jordanne Monseau Continental, Ralf Willenbrock T-Systems
v04	26/11/2019	Rework with focus on recommendations on legal issues	Thomas Desseilles, ERTICO-ITS Europe, Jordi Pont Idiada, Alejandro Manilla Idiada, Jo-Ann Pattinson University of Leeds, Jordanne Monseau Continental, Ralf Willenbrock T-Systems
v05	02/12/2019	Integration of the task review. Submission to peer review.	Thomas Desseilles, ERTICO-ITS Europe
v06	20/12/2019	Peer review integration	Thomas Desseilles, ERTICO-ITS Europe
v1.0	23/12/2019	Version for submission	Rita Bhandari, ERTICO-ITS Europe

Abstract

As a likely disruptive technology, Internet-of-Things (IoT) comes with a number of potential legal challenges. These challenges are heightened when IoT technologies are used in the context of automated driving (AD).

This document presents the legal perspectives and the methodology for evaluating legal issues – such as security and privacy aspects, liability issues, concerns and expectations – relating to AUTOPILOT's use of IoT technologies for advancing AD in a connected environment. Quantitative and qualitative consultation methods were used in the form of surveys and workshops to define, analyse and report on the legal aspects of using IoT solutions for AD. Expertise from AUTOPILOT project partners representing various stakeholder clusters is gathered and is complemented by user surveys on legal issues from pilot sites. The description by the internal experts of the legal impacts of using IoT solutions for AD and the results of the user surveys are then analysed in consultation with legal and regulation experts through focus groups and workshops.

This document is the updated version of D4.9: *Preliminary legal perspectives on the use of IoT for AD*. This document D4.10 presents the outcome of the activities carried out in T4.6 and provides recommendations to the study group from the industry and the regulation committees at the European Commission and the United Nations Economic Commission for Europe that work on

regulations relating to automated vehicles.

Legal Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. © 2017 by AUTOPILOT Consortium.

Abbreviations and Acronyms

Acronym	Definition
ABAC	Attribute Based Access Control
ABE	ABE Encryption algorithm
AD	Automated Driving
ADAS	Advanced Driver-Assistance Systems
AI	Artificial Intelligence
AV	Automated Vehicle
CBR	Netherlands Exam Authority
CEMA	Crowd Estimation and Mobility Analytics
DDoS	Distributed Denial of Service – type of cybersecurity attack
DoS	Denial of Service – type of cybersecurity attack
DRM	Digital Rights Management
DSSAD	Data Storage System for Automated Driving
EDR	Event Data Recorder
EU	European Union
FAA	Federal Aviation Administration
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRVA	Working Party on Automated/Autonomous and Connected Vehicles
IDS	Intrusion Detection System
IoT	Internet-of-Things
IPE	IPE Encryption algorithm
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IWG	Informal Working Group
LLP	Limited Liability Partnership
MIT	Massachussets Institue of Technology

MITM	Man-In-The-Middle – type of cybersecurity attack
MNO	Mobile Network Operator
MPC	Multi Party Computation
OEM	Original Equipment Manufacturer
ODD	Operational Design Domain
OTA	Over-The-Air
PRE	PRE Encryption algorithm
PSA	Privacy and Security Assessment
PLD	Product Liability Directive
PoI	Point of Interest
RDW	Rijks Dienst Wegverkeer – Netherlands Road Department
RWS	Rijkswaterstaat
SAE	Society of Automobile Engineers
SIEM	Security Information & Event Management
TARA	Threat Assessment and Remediation Analysis
TKG	Telekommunikationsgesetz – German Telecommunication Act
UK	United Kingdom
UNECE	United Nations Economic Commission for Europe
V2V	Vehicle to Vehicle communication
V2X	Vehicle to Any communication
VRU	Vulnerable Road Users
WG	Working Group
WP	Work Package
X2V	Any to Vehicle communication

Table of Contents

List of Figures

List of Tables

1 Executive Summary

The goal of the AUTOPILOT project is to bring together knowledge and technology from the automotive and the Internet-of-Things (IoT) value chains in order to develop IoT-architectures and platforms that will advance automated driving (AD) in a connected environment. AUTOPILOT develops new automated driving services by connecting automated driving equipped vehicles over IoT. The services being developed will enable fully automated driving solutions such as Automated Valet Parking, platooning and real-time car sharing services.

As a likely disruptive technology, Internet-of-Things (IoT) comes with a number of potential legal challenges. These challenges are heightened when IoT technologies are used in the context of automated driving.

This document presents the **methodology for evaluating legal issues**, concerns and expectations, **evaluation study and evaluation results** related to regulation, liability, data sharing and privacy, and cybersecurity in the context of AUTOPILOT user tests related to use of IoT technologies for advancing AD in a connected environment.

Quantitative and qualitative consultation methods are used in the form of surveys, workshops and webinars to define, analyse and report the legal aspects (issues, concerns and expectations) of using IoT solutions for AD. The methodology revolves around a three-step process aligned with activities to be carried out as part of Task 4.6. The first step includes collecting information – expertise, concerns and expectations regarding legal matters – by conducting surveys of AUTOPILOT project partners and potential users as well as AD stakeholders. The feedback from internal experts on the legal impacts of using IoT solutions for AD will be then analysed in consultation with external legal and regulation experts through focus groups, workshops and webinars. Finally, the findings will be used to make recommendations on regulation in collaboration with dedicated European commission authorities.

The **Legal impacts of using IoT for Automated Driving** touch upon a number of issues ranging from regulation, data privacy and security, liability, insurance, intellectual property rights (IPR), etc. The fact that the use of cloud-based IoT for AD brings together a number of actors, who collaborate to provide an enhanced driving experience where the traditional role of the human driver is diminished, is a big contributor to legal complexities. There is also the need for regulation to match the progress in the IoT and AD domains and address issues of liability, data privacy and data security.

The large number of partners involved in bringing the connected and automated driving experience to the user could cause difficulties in attributing liability when things go wrong. The contrary pulls of cloud-based services offering privacy on one hand, and IoT, which is about wide reach and sharing, on the other hand can have legal repercussions to do with issues of customer awareness and EU regulation regarding data processing.

Last but not least, cybersecurity concerns of hacking and the potential for intrusive behaviour is also a legal concern affecting IoT based automated driving.

The potential legal intricacies of this new paradigm need to be understood and analysed so that solutions, be they standards or legislation and regulations, can be put in place as the IoT-AD services and products reach users.

As IoT does enhance the automated driving experience, we provide recommendations coming out of the provided analysis of the legal issues and summarize them in our conclusions.

2 Introduction

2.1 Purpose and scope of the Document

The AUTOPILOT project brings together knowledge and technology from the automotive and the Internet-of-Things (IoT) value chains in order to develop IoT-architectures and platforms that will advance automated driving (AD) in a connected environment. As a potential disruptive technology, IoT brings with it the possibility of a number of legal challenges. These challenges are heightened when IoT technologies are used in the context of automated driving.

Work Package 4 presents 3 hypotheses to be validated (according to AUTOPILOT D4.1[1]):

- IoT is *accelerating* the development and deployment of automated driving functions,
- IoT is *enhancing* the functionality or performance of automated driving functions,
- IoT is *enabling* new automated driving functions.

The scope of T4.6, and hence D4.9 and D4.10, is the legal impact of using IoT and the data collected for progressing automated driving. The legal issues considered within this task relate to the potential impact on privacy, data protection, physical safety and liability. The scope of this task does not involve analysing day-to-day legal obligations or due diligence of AUTOPILOT's activities individually. Legal issues relating to pilot site activities, for instance the conditions for use of an automated vehicle during the test phases or the conditions for involving users in the evaluation task, are out of scope of the task T4.6.

Deliverable D4.10 "*Legal perspectives on the use of IoT for AD*" is the final deliverable presenting the outcome of the activities carried out in T4.6, including improvements based on Deliverable D4.9 "*Preliminary legal perspectives for the use of IoT for AD"* on external legal consultations, and provide recommendations to the study group from the industry and the regulation committees at the European Commission and the United Nations Economic Commission for Europe (UNECE) that work on regulations relating to automated vehicles.

2.2 Intended audience

Since the legal issues presented in D4.9 and D4.10 bear on AUTOPILOT's core elements – IoT and AD – it is relevant to all project beneficiaries in all WPs.

D4.10 is a public deliverable and also of potential interest to an external audience concerned with the legal implications of IoT applied to AD. It will also be relevant to users to demystify the industry of automated driving.

By external audience, we understand all companies, product and service suppliers, insurance companies and public authorities who are, or will be, involved in the future of automated transportation.

2.3 Structure of the document

Chapter 2 introduces the purpose, intended audience and structure of the document.

Chapter 3 details the methodology used for legal analysis in AUTOPILOT. The activities described are: 1) information gathering by involving knowledge holders (AUTOPILOT experts and test users); 2) consulting with legal and regulation experts; and 3) providing recommendations to regulatory agencies.

Chapter 4 presents the report on the legal impacts of using IoT solutions for automated driving based on our study of current research and trends.

Chapter 5 provide a thorough analysis of the legal issues when enhancing Automated Driving by IoT in four categories: Regulation, Liability, Privacy and Cybersecurity.

Annex 1 is the internal survey used to collect feedback from AUTOPILOT partner beneficiaries on legal impacts as relevant to various stakeholder groups.

Annex 2 lists the questions provided to task T4.5 – User Acceptance Assessment - to assess the legal perspective as it relates to user acceptance.

3 Methodology for analysing legal impacts in AUTOPILOT

AUTOPILOT deliverable D4.1[2] – *Methodology for evaluation* – described the evaluation methodology and requirements developed in Task 4.1, which are to be "implemented, refined and executed" in other tasks within WP4: T4.2 – Technical Evaluation, Task 4.3 – Business Impact Assessment, Task 4.4 – Quality of Life Impact Assessment and Task 4.5 – User Acceptance Assessment. With reference to T4.6, D4.1[3] states that, "Task 4.6 will not implement an evaluation methodology, but instead investigate any legal issues that arise from piloting and the other evaluation tasks".

Task 4.6 intends to assess the legal impacts arising from the use of IoT technologies for enabling or improving automated driving in a connected environment. Issues of specific interest are security, privacy and liability. The three-step methodology presented here and illustrated in Figure 1 Methodology for evaluating legal issues in AUTOPILOT
A two rounds approach has been done in Task 4.6 with a preliminary report D4.9 submitted on 28/06/2018 and the current D4.10 which is the final set of analysis of the legal issues and the resulting recommendations.

We continued the same methodology, further nurturing the already gathered information, expert's review and recommendations throughout the Autopilot project results, their evaluations with the already submitted deliverables about Initial Technical Evaluation (D4.2), Preliminary Business Impact Assessment (D4.4), the developed IoT Policy Framework (D5.4) and Autopilot Preliminary Business Exploitation Plan (D5.5).
Within WP4 Autopilot evaluation work package, through direct contact, meetings and workshops, we did also take into account the other evaluation aspects as:

- D4.3 Final Technical Evaluation – especially for their process to gather and analyse the data from the Pilot Sites;
- D4.5 Business Impact Assessment
- D4.8 User Acceptance Assessment

Step 1: Information gathering by involving knowledge holders (AUTOPILOT experts and test users)
Description of Action: Gather the expertise of the project partners to provide a preliminary report (D4.9 draft) explaining the impact of using IoT solutions from a legal perspective. A questionnaire will be provided to task T4.5 for collecting user feedback on the legal issue during the Pilot Site tests.
Step 2: Consultation with external legal and regulation experts
Description of Action: Consultation with legal and regulation experts, analysing the preliminary report elaborated in the previous activity and the questionnaire collected from the users at the Pilot Site.
Step 3: Recommendations to regulatory agencies
Description of Action: Provide recommendations (D4.10) to the study group from the industry and the regulation committees at the European Commission and the UNECE, working on regulations relating to automated vehicles.

The processes and methods of legal impact analysis used in T4.6 are detailed in the sections that follow in this chapter. In accordance with D4.1, input from other evaluation tasks will be taken into consideration at every step.

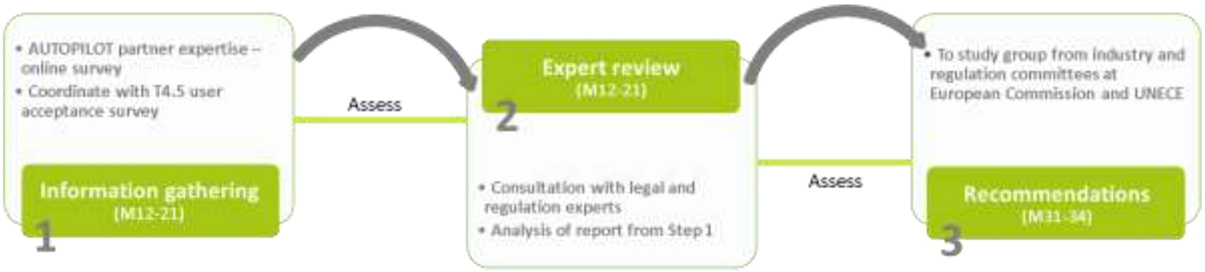

• AUTOPILOT partner expertise – online survey
• Coordinate with T4.5 user acceptance survey
Information gathering
(M12-21)
1
Assess
Expert review
(M12-21)
2
• Consultation with legal and regulation experts
• Analysis of report from Step 1
Assess
• To study group from industry and regulation committees at European Commission and UNECE
Recommendations
(M31-34)
3

Figure 1 Methodology for evaluating legal issues in AUTOPILOT

A two rounds approach has been done in Task 4.6 with a preliminary report D4.9[4] submitted on 28/06/2018 and the current D4.10 which is the final set of analysis of the legal issues and the resulting recommendations.

We continued the same methodology, further nurturing the already gathered information, expert's review and recommendations throughout the Autopilot project results, their evaluations with the already submitted deliverables about Initial Technical Evaluation (D4.2[5]), Preliminary Business Impact Assessment (D4.4), the developed IoT Policy Framework (D5.4[6]) and Autopilot Preliminary Business Exploitation Plan (D5.5).

Within WP4 Autopilot evaluation work package, through direct contact, meetings and workshops, we did also take into account the other evaluation aspects as:

- D4.3[7] Final Technical Evaluation – especially for their process to gather and analyse the data from the Pilot Sites;
- D4.5[8] Business Impact Assessment
- D4.8[9] User Acceptance Assessment

3.1 Information gathering

The purpose of this step is to assemble information pertaining to the legal aspects of using IoT for AD. This information is put together in a report and used as the basis for consultation with external legal experts. Along the execution of this "Legal Issues" task, we have conducted a review of the current research and regulation relevant to connected and automated driving.

What emerges from our study is presented in Chapter 4 where we provide a more in-depth analysis using two different information sources with specific objectives. The first stream of information will be generated from experts in the AUTOPILOT project, while the second source will result from feedback collected on user acceptance as part of T4.5. The information gathered in this way will lead to legal insights covering the scientific and technical aspects as well as having a strong and practical user focus.

The following subsections layout the objectives and plans of both processes of collecting information.

3.1.1 AUTOPILOT experts' consultation

Objective: The goal of the internal consultation is to collect the expertise of AUTOPILOT partners about legal issues related to IoT and AD. The large AUTOPILOT consortium has a diverse makeup with OEMs, research institutions, public authorities as well as ITS organisations. The perspectives they bring cover a wide spectrum of legal impacts that concern AUTOPILOT's work and mission. The experience and knowledge of the various partners will provide valuable input for framing our analysis of legal issues, preliminary and concluding recommendations to relevant regulatory bodies.

Method: Two methods were used to elicit internal expertise. First, an online survey (in Annex 1) collected information from the entire consortium about legal concerns that must be addressed in the context of using IoT with AD. Second, an internal consortium consultation based on a large number of legal experts from the AUTOPILOT consortium was conducted, as a midterm review of this deliverable.

3.1.2 State of the Art gathering

Objective: The goal of the State of the Art gathering is update the knowledge and reflection in the research arena as well as in the market about the legal issues of IoT and Automated Driving.

Method: Each contributor to this deliverable kept track of the relevant readings and do reference them throughout this deliverable as reported in section 6.3 References.

3.1.3 Key learnings from research around the world

Objective: The goal of the key learnings from research around the world is to update the knowledge and reflection in the research arena as well as in the market about the legal issues of IoT and Automated Driving through participation in the ITS World Congress 2019 in Singapore SIS 10 Complex self-driving field operational tests using evolved IT infrastructures and SIS 19 Criminal Liability scheme for AV accident.

Method: Each contributor to this deliverable kept track of the relevant readings and make reference to them throughout this deliverable as reported in section 6.3 References.

3.2 Expert review

3.2.1 External legal experts' consultation

Objective: The aim of the external experts' consultations is to expand upon the legal issues found within this task, beyond the AUTOPILOT consortium. The external legal experts were selected based on their previous experience and accomplishment relevant to the legal perspectives covered in this task.

Method: Two methods of examinations were used to maximise the benefit of our consultations with the legal experts.

A first expert review panel consisted of the following:

- Insurance Industry: Giovanni Barassi – Head of Digital and open innovation – Unipolsai
- Privacy law: Valentina Frediani – CEO & Founder – COLIN & Partners
- Transport: Eetu Pilli-Sihvola – Chief Adviser – Finnish Transport and Communciations Agency
- Insurance: Jacques Amselen - Head of IoT - Allianz
- Telecom Operator – Ralf Willenbrock – Produktmanager – T-Systems International

Secondly, a consultation workshop was conducted at the LIVORNO pilot site during the stakeholder event meeting that took place in October 2018, with relevant AUTOPILOT consortium members contributing to the analysis of the issues. The LIVORNO stakeholder meeting panel consisted of:

- Mobile Network Operator: Giovanna Larini – Connected vehicle Innovation responsible – TIM

- Insurance industry: Giovanni Barassi – Head of Digital and open Innovation - Unipolsai
- Privacy law: Valentina Frediani – CEO & Founder – COLIN & Partners
- Academia: Giovanni Comandé – Full Professor - Scuola Superiore Sant'Anna, Pisa

Third, in February 2019, after examining the legal issues in light of the expert analysis of the deliverable, a review took place in June 2019.

The survey data collection methods are closely connected. Both surveys and workshops include questions that have emerged from an initial examination of contemporary research and analysis of the legal issues of connected and automated driving. In providing input to T4.5, advice and direction was sought from experts within AUTOPILOT, and feedback generated from the user surveys will be submitted for analysis by the internal experts.

3.2.2 Webinars

Objective: Webinars are means of dissemination of the T4.6 findings outside of the AUTOPILOT consortium as well as feedback gathering on the preliminary results and recommendations.

Method: Two webinars were conducted; the first event was limited to external legal experts and members from AUTOPILOT consortium, which took place in February 2019 after the first external legal experts review. The second was a public webinar occurring in July 2019, presenting the legal issues examined by AUTOPILOT, and encouraging public discussion and contribution via a question and answer session.

3.2.3 Feedback from T4.5 user survey

Objective: Feedback was collected from user acceptance surveys conducted as part of T4.5, which is the task evaluating user acceptance. This aligns with the objective specified in D4.1 for task T4.6 to "investigate any legal issues that arise from piloting and the other evaluation tasks". The feedback identified users' legal concerns related to privacy (data anonymization), security (data protection), liability and safety.

Method: Based on our research review (see Chapter 4), T4.6 identified legal issues that could impact user acceptance. A questionnaire (see Annex 2) was provided to T4.5 to include in the user acceptance surveys conducted on pilot sites. The results from T4.5 are analysed and integrated in order to contribute to the external consultation workshops on legal impacts of IoT based AD.

3.2.4 External experts' consultation on the final recommendations

Objective: While finalizing the recommendations resulting from the T4.6 Legal Issues, discussions have taken place in order to verify the potential alignment, market readiness and the content for further research on some of the recommendations. The ideas, observations and comments have been integrated in the recommendations formulated in chapter 4.

Method: Bilateral discussions with stakeholders' representatives:

- Insurance Industry: Charles Low and Thomas Gelin, Policy Advisors - Insurance Europe;
- Road Users: Oliver Lenz, Programmes Director – FIA;
- OEM representative: Joost Vantomme, Smart Mobility Director – ACEA;
- OEM suppliers' representative: Frank Schlehuber, Director Aftermarket – CLEPA;
- Public Authorities' representatives: Eric Kenis, Advisor – Ministerie Openbare Werken; Hans Kramer and Sebe Vogel - Rijkswaterstaat.

3.3 Recommendations – industry and regulation

3.3.1 Current regulatory environment

Connected and automated vehicles pose new challenges regarding privacy and data protection. Since 1995 until recently, the EU approach to privacy was mainly regulated by the Data Protection Directive (Directive 95/46/EC of the European Parliament)[10]. It has now been replaced by the General Data Protection Regulation 2016/679 (GDPR)[11], approved by the EU Parliament on 14th April 2016 and enforced since 25th May 2018. This is the main European regulation regarding data protection. EU privacy laws apply to all sectors and industries, including connected and automated vehicles.

The GDPR applies to information related to identified or identifiable (directly or indirectly) natural persons (the "data subject"); not to anonymous information, i.e., the information not related to an identified or identifiable natural person, or that has been made anonymous in such a manner that the individual is no longer identifiable. In particular, the GDPR requires a legal basis to process private data such as performance of a contract, user consent for the purposes of data processing. In any case, the data subject user shall be informed thereof. Concerning consent specifically, it must be clearly distinguishable, freely given, as easy to withdraw as it is to give, and auditable or verifiable. Consent must be an explicit (not a passive) activity. Consent shall not be included in a long privacy policy and consent shall be given for a single use, i.e., it cannot be bundled with other types of consents. Under certain circumstances, the GDPR recognizes a right to data portability, therefore, allowing the data subject to request the transfer of his/her information from one provider to a different one. This right has consequences regarding harmonization of standards. Organizations dealing with personal data need to ensure that their process for collecting, using, transferring and storing this information is compatible along the data processing chain with other companies. This topic is further covered in section 4.3.

Some of the other regulations in place at European level are:

- Directive ECE/TRANS/WP.29/2017/46. Guidelines on cybersecurity and data protection, prepared by the expert from Informal Working Group (IWG) on Intelligent Transport Systems / Automated Driving (ITS/AD)
- Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe)
- Directive 2009/136/EC of the European Parliament and of the Council of 25th November 2009 amending Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Directive 95/46/EC of the European parliament and the Council of 24th October 1995, concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data

- Directive 2016/680 if data sharing involves Public enforcement authorities or receive data from them

Regarding safety and liability, the following regulations are to be found:

- ISO 26262, Road vehicles - Functional safety, concerning functional safety of electrical and/or electronic systems in production automobiles is an international standard defined in 2011 by the International Organization for Standardization (ISO)
- Decision 2001/95/EC of the European Parliament and of the Council of 3rd December 2001, concerning general product safety (the General Product Safety Directive)
- Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9th July 2008, concerning the application of certain national technical rules to products lawfully marketed in another Member State
- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products Regulation (EU) – Product Liability Directive (PLD)
- No 1025/2012 on European standardisation
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

It is also worth mentioning that there is currently a legislative initiative concerning the review of the type-approval of motor vehicles.

- COM(2018) 286 final 2018/0145 (COD) Proposal for a regulation of the European Parliament and of the Council 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/… and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009[12].
    - The first round of inter-institutional negotiations between Parliament and the Council were conducted begin of 2019 with a provisional agreement reached on 25 March 2019;
    - The current status of this is that the European Parliament approved a corrigendum on 10 October 2019. It still needs to be adopted by the Council and signed into law[13].

3.3.2 Approach

We have evaluated current EC and UNECE regulations relevant to automated driving and IoT mentioned in the preceding section. The findings have been presented and discussed with external experts and now, AUTOPILOT present recommendations to industry and regulatory bodies to ensure the best possible outcome for cloud-based IoT automated driving in terms of wide impact and exploitation.

In the following section, we look at some of the greatest legal issues facing connected and automated driving in the current climate.

4 Legal impacts of using IoT solutions for AD

In their paper entitled 'Use of IoT Technology to Drive the Automotive Industry from Connected to Full Automated Vehicles', Krasniqi & Hajrizi (2016)[14] point out that IoT is transforming the automobile industry in a revolutionary manner, even compared to other forms of connectivity. They point out that the transformation involves transitioning "from an age of products to an age of services and experiences, from hardware to software, from functionality to information as the key object of value creation, and from industry silos to complex connected ecosystems". It is to be expected that such a disruption in business models will bring with it a host of legal consequences.
A 2017 paper by the international legal firm Allen & Overy LLP[15] states that "six of the biggest legal issues facing the connected and self-driving car market" are: *regulation*, *liability*, *big data and data analytics*, *cybersecurity*, *collaborations and partnerships*, and *cars as socially networked devices*. The paper describes the risks that coincide with these issues and suggests ways to mitigate them. For instance, EU regulation must keep pace with the rapid development of ITS technology, with particular attention to cross-border use of connected cars, interoperability of platforms, net neutrality, etc. The connected and automated mobility paradigm is creating new partnerships between the automotive sector, technology companies and mobile service providers, among others. Such cross-industry collaborations will need to address matters such as third-party liability allocation, responsibility of complying with laws and standards and ownership of jointly created intellectual property. Automobiles as connected vehicles also have legal implications relating to driver distraction, liability, data usage (and its implications for open access to third parties, cost apportionment) and cyberattacks.

In 2017, the legal firm Foley & Lardner LLP[16] conducted a survey of automakers, suppliers, start-ups, investors and technology companies in the US about the business and legal issues significant for the development of connected and automated vehicles. The survey found that the technologies behind connected cars and automated vehicles were at different stages of development and implementation, and thus had different obstacles to growth. While safety and user acceptance were the big challenge for automated vehicles, the concerns regarding connected vehicles related foremost to cybersecurity and privacy issues. Four of the legal issues mentioned in the Allen & Overy report – regulation, liability, big data and data analytics, and cybersecurity – cut across all stakeholder clusters, be they regulatory authorities, original equipment manufacturers (OEMs), mobile network operators (MNOs), public and private fleet operators, or end users (drivers). This is how we structured our research on the legal issues and report it in the chapter 4.

By using cloud-based IoT to advance AD, AUTOPILOT has a distinct perspective on EU regulation, cybersecurity, big data analytics and privacy, and liability – matters which are the focus of task T4.6. This document, deliverable D4.10, provides a final synthesis of how these issues are impacted by the use of IoT for automated driving.

4.1 Regulation

4.1.1 Introduction

As new IoT technologies and automated vehicles emerge, the challenge is to create regulation within legacy frameworks, while encouraging innovation. The effective introduction and governance of automated vehicles would potentially reduce the numbers of traffic accidents and road deaths across Europe. Careful regulation may facilitate public confidence and positively affect the uptake of the new technology. Prototype testing in projects such as AUTOPILOT allows space for issues such as safety to be addressed in the confines of a managed testing environment. However, the lessons learned from such pilots may be inhibited by the complex European testing framework for automated prototypes. This section will comment upon the ad-hoc prototype testing regulation framework for large-scale European pilots, contrasted to the harmonised UNECE adaptive model of regulation applicable to automated vehicles intended for public use.

The specification and implementation of a harmonious cross-border testing framework in Europe is essential for continued advancement and reproducibility in areas such as safety and standardisation of IoT and highly automated vehicles. Analysis arising as a result of large-scale testing in Europe contributes to the developing regulatory framework governing IoT and automated vehicles, addressing issues of trust, security, privacy and engagement.

4.1.2 The regulation of technology

As we develop the potential of automated vehicle technology, regulation ensures that public safety is not compromised in the pursuit of exploring the prospective contribution new technology may make to our society. However, there are difficulties associated with finding the correct balance of reasonable precautions. A regime allowing too much flexibility may not provide adequate safeguards, whilst a regime of over-protection through overregulation is also not desirable. In addition, it is debatable whether regulation should specify technology principles or, on the contrary, be technology neutral and specify principles, in order to be able to cope with technical evolution over time. An example of regulation where technology has been specified is the eCall implementation which faces now the phase-out of the 2G and 3G technology. Transitory arrangements for the regulation of automated vehicles provides an essential step towards end goal operations and future deployment, as the reliability of the technology is validated.

The overregulation of new technology potentially poses a hindrance to the improvement of technology. In examples from history, in the UK the Locomotive Act[17] of 1861 required locomotives be manned by two persons and not exceed 10mph when passing though towns. In 1865 the so-called Red Flag Acts[18] required a person to walk ahead of self-propelled vehicles waving a red flag to warn pedestrians[19]. In the United States, Pennsylvania contemplated infamous legislation, which required all motorists passing livestock to 'rapidly disassemble the automobile' and conceal its components to avoid distressing the animals. The legislation was vetoed by the Governor. [20] Regulation tends to reflect an understanding of yesterday's technology instead of the emergent technology. [21]

Conversely, the death of a 49-year-old pedestrian in Arizona in 2018 caused by an Uber in automated mode, [22] provides a tragic cautionary tale. People tend to accept that humans make mistakes and as such are likely to have empathy for others when human error causes an accident. However, the same type of empathy is not reserved for machines. We expect machines to simultaneously perform better and to make less mistakes. Humans show nearly zero tolerance for injury or death caused by a flaw in a machine. [23] This is why regulation regarding standards and testing is an essential component of automated vehicle development.

4.1.2.1 The link between automated vehicles and enhanced safety

There are pertinent incentives for embarking upon the deployment of automated vehicles sooner rather than later. Motor vehicle accidents involving traditional vehicles are associated with 1.25 million deaths, with a further 20-50 million injured in collisions. [24] Europe has some of the safest roads in the world. Compared to the global average of 174 deaths per millions of population, Europe's toll is relatively low at 49. However for every person killed in a crash, there are 5 people who suffer life-changing injuries. [25] Road safety is a visible concern for the public, and automated vehicles are proposed as a solution for reducing collisions resulting in casualties as most of them are attributed to the "human factor".

The types of functions contained within automated vehicles can support safe driving and improve driver performance. Recognition errors may be reduced by minimizing inattention and obstructed vision. Decision errors may be addressed by remedying tailgating and excessive speed. Erratic and wilful actions of drivers, such as failing to control the vehicle by the misuse of mind-altering substances such as alcohol, or performing wilfully unsafe driving acts, [26] are expected to no longer endanger other road users.

A study by RAND corporation about the introduction of automated vehicles and considered the scenarios of introducing new technology which improved safety by 10%, compared to waiting longer for the technology to significantly advance so that safety was improved by 75% and then waiting longer for the technology to improve safety by 90%. Comparing the potential number of lives saved from automobile accidents under 'Improve10', 'Improve75' and 'Improve90' strategies, the study proffers that if we are able to deploy safer vehicles cars sooner, which are only 10% safer, they will save more lives overall than waiting to deploy technology until the cars are 90% safer. [27] However in order to achieve this ambition of making the roads safer overall by the introduction of automated vehicles, the public must be assured that the new technology is safer than vehicles which drive on the roads today.

4.1.2.2 Public trust

Survey data from 2016[28] highlights expressed public opinion on automated driving, indicating that safety of the new technology was a main concern:

"*I welcome the advancements in technology, provided it has been independently and rigorously (scientifically!) tested and researched"*

"I do not know enough about their capabilities and safety features"

"I am opposed to these vehicles being on the road without emergency manual braking available to a human at all times"

"If you know an automated vehicle is going to stop, why not just pull out in front of them?"

Such concerns have been corroborated by AUTOPILOT research. Participants of the online survey designed to ascertain barriers to trust, acceptance and engagement with automated vehicles, identified safety as principal concern, with participants pinpointing fears about technical failures, malfunction, loss of data, and the ability to stop a fully automated vehicle. [29]

Scepticism about new technology is understandable. Whilst IoT and automated vehicles may offer convenience and new services to consumers, technology also causes fear and apprehension. [30] The discomfort refers to a lack of control over technology and a feeling of being overwhelmed by it. [31] Regulation may address the problem of how automated vehicles may be introduced usefully to public roads and spaces with the support of the public and business, by ensuring standards relating to safety, privacy, liability and security. [32] Appropriate standards may temper some of the cynicisms expressed by the public, and provide sufficient confidence to try the new technology. An adaptive regulatory strategy may address how such standards should be devised, validated, implemented and assessed, in a manner which addresses the public's concerns and while allowing innovation to occur.

A specific study is being conducted within the AUTOPILOT project about User Acceptance and will be reported in the deliverable D4.8.

4.1.2.3 Adaptive regulation

The law must be stable, yet it cannot stand still. The perception of policy instability may erode confidence in the regulation of technology, however society may also lose confidence in obsolete technology and frameworks. The regulation of technology must be flexible and promote social well-being in order to be accepted. [33] Regulation may be designed, exercised and evolve as a dynamic process to manage interdependencies in a non-finalising way. The governance of new technology may be best placed to avoid unrealistic assumptions about the direction of innovation and instead, it should provide opportunities to open up insights about circumstances, conditions and contexts about the limits, and even failures of overly deterministic goals. [34]

Adaptive regulation is particularly appropriate when it is likely lessons will be learned after the initial adoption of a policy. Automated vehicles and IoT present promise to improve quality of life while simultaneously presenting risks which are uncertain and changing over time. The fast pace of change creates significant uncertainties for regulators. These new technologies warrant an approach to regulation that adjusts and adapts as information about the technology changes, to provide maximum benefit. Automated vehicles must be at least as safe as human driven vehicles, and this should be expressed in concrete terms. The two key questions for regulators are: How should safety be measured for automated vehicles, and what threshold of standards should be required before they are made publicly available?

4.1.2.4 International standards

Technology standardisation can integrate newly created innovations into an ordered system, [35] by providing the infrastructure to enable the safe delivery of technology and its interoperability. Research and development, engineering and design, component production and assembly occur without regard to borders. Increasingly, vehicle manufactures are relying on international suppliers, producing a wide range of standardised and interchangeable components and platforms. Having individual countries manage minimum technical requirements for automated technology is potentially disastrous, while regulatory divergence is costly. [36] Fragmented national vehicle standards can impose substantial costs on industry, in some cases the variations in standards merely set out different ways of achieving the same outcomes. The use of different technical standards for like products can impose barriers to international trade. In 2017 in the United States, 50 legislative bills were introduced in 20 states which referred to automated driving and IoT. [37] Such breadth of uncoordinated regulation could delay innovation by creating conflict. As the automobile industry is global, or at least continental (Europe, Asia, US), in nature, the full potential advantages of automated vehicles are more likely to occur within a cooperative international legal framework, dedicated to ensuring that automated enter our public roads and spaces in a manner which ensures the safety and confidence of all drivers, passengers, road users and pedestrians. This problem is addressed at many levels in Europe by harmonious international regulation.

The UNECE is the peak international regulation body for vehicle safety. Regulation of instruments relating to automated vehicles by the UNECE and the UNECE World Forum for the Harmonisation of Vehicle Regulations (WP.29) is commensurate with the adaptive regulation strategy, whilst maintaining a clear and comprehensible legal framework across Europe. UNECE regulations have had a demonstrable impact on international road safety. Regulations introduced by the UNECE including; mandatory automatic retractor safety belts, child restraint systems and headrests, have arguably reduced the number of serious injury and fatalities, while the amount of traffic has steadily increased.

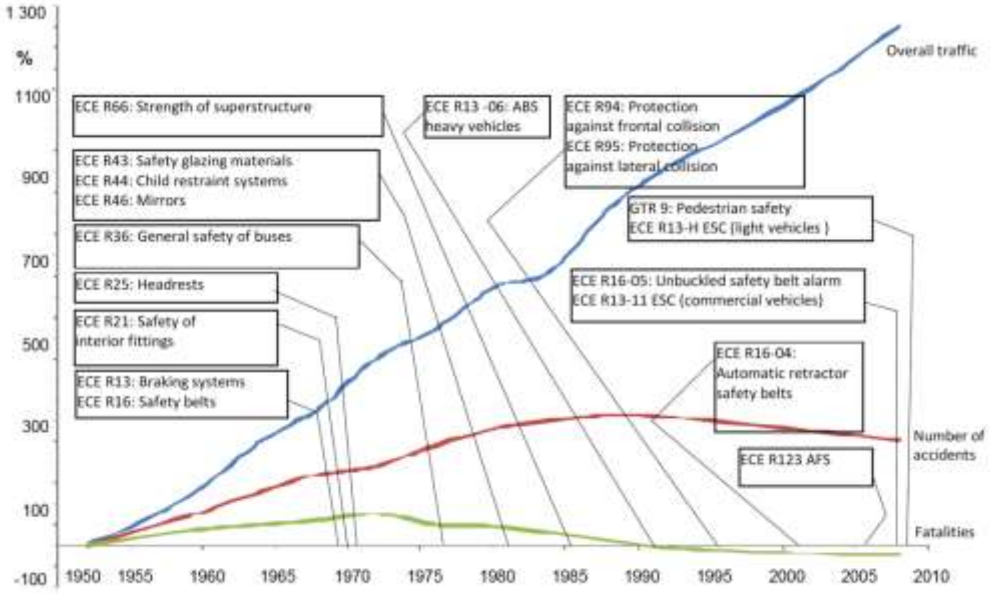


Figure 2 Regulation impact statement for the harmonisation of the Australian Design Rules[38]

WP.29 operates an adaptive regulatory framework concerning vehicle regulation. Regulatory proposals are constructed by working groups, informed by experts. The contribution of experts addresses the lack of practical experience of testing/assessing the functionality of automated driving systems and includes in its membership a wide constituency of specialist contracting bodies, [39] aiming to create a regulatory regime that is flexible to allow regular updates as required. [40]

Matters identified by the UNECE as a priority for harmonisation in respect of automated vehicles include:

- A legal framework for automated vehicles

- Functional requirements (such as acceleration, lane control and braking)
- New assessment and testing methods; and
- Cyber-security and software updates.

Projects such as AUTOPILOT can provide valuable data relevant to these regulatory priorities. Data obtained from AUTOPILOT research may be useful in determining how automated vehicles may be regulated in the future, and further, how far we have come in meeting the standard of safety and user acceptance necessary for the successful deployment of such technology onto public roads. For example, the results of AUTOPILOT testing and analysis may be relevant to the certification process for highly automated vehicles being developed at UNECE level, and this is discussed below.

4.1.2.5 Reproducibility and the certification of highly automated vehicles

In the current type approval for motor vehicles[41], there is no section covering the type approval of self-driving cars specifically.[42] The type approval process provides standardisation to ensure aspects such as safety in vehicles across Europe. Individual countries do not set the minimum requirements, the type approval of vehicles is harmonised internationally by the UNECE and WP.29. Regulations developed by WP.29 consist of internationally coordinated and uniform technical prescriptions for wheeled vehicles, equipment and parts. Complying with these requirements contributes to higher product safety and a minimisation of product liability risks.

In the 'classical approach' for the certification of vehicles, matters which are tested include; adhesion on wet surfaces, braking and minimum deceleration requirements. In the Proposal for the Future Certification of Automated/Autonomous Driving Systems[43,] these matters are still relevant, however in addition to the classical aspects of safety, vehicles fitted with automated driving systems must incorporate the anticipation of other road users, including other drivers, pedestrians, micromobility with powered two-wheelers and cyclists. Regulating automated vehicles 'function by function' may be problematic due to the likelihood of frequent software updates being provided by the manufacturer. If software updates are not permitted, this would not allow designs to improve. Flexible structures are needed to define reasonable requirements whilst allowing evolution of new technology. An extension of the certification process towards an audit of the process and functional safety is being prepared. There is herewith a further research topic with the AI-dilemma where the software could evolve in a non-controlled manner and therefore safeguards need to be put in place to prevent problems and answer the causality effect in liability.

The process for the certification of automated vehicles is being developed by the Working Party on Automated/Autonomous and Connected Vehicles (GRVA). [44] A '3 Pillar' approach is being considered, which incorporates requirements for automated vehicles to successfully negotiate 'critical' and 'edge' case scenarios to attain certification. Such scenarios consider complex and hazardous situations which may be encountered on the roads, and requires the manufacturer to have addressed such cases in the design of the vehicle and its systems.

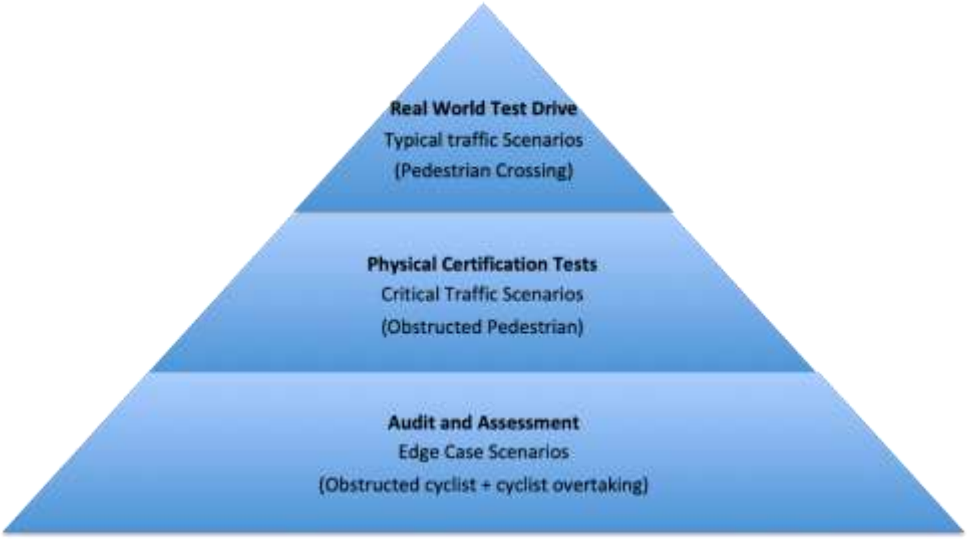

Real World Test Drive
Typical traffic Scenarios
(Pedestrian Crossing)
Physical Certification Tests
Critical Traffic Scenarios
(Obstructed Pedestrian)
Audit and Assessment
Edge Case Scenarios
(Obstructed cyclist + cyclist overtaking)

Figure 3 Concept for future certification – 3 pillars

The proposed three pillar approach may provide a streamlined and predicable approval process contingent on manufacturers providing access to key information, and providing evidence of the vehicle and its IoT complying with a functional, safety-orientated framework. [45]

The significance of a software update radically altering safety parameters was recently demonstrated with incidents involving Boeing 737 Max aircraft in October 2018 and March 2019. In these cases, a Lion Air and an Ethiopian Airlines aircraft crashed, causing the deaths of 189 and 157 people respectively. Investigators discovered an automated safety system on the 737 Max caused the nose of the plane to tip downwards, which could not be cancelled by the pilots. [46] A software update was formulated to address the fatal error, and was submitted by Boeing to the FAA for approval in May 2019. [47] The Boeing disaster is demonstrative of the high-stakes attached to developing automated technology for transport systems, potentially placing human lives at risk, where testing does not necessarily discover all potential faults.

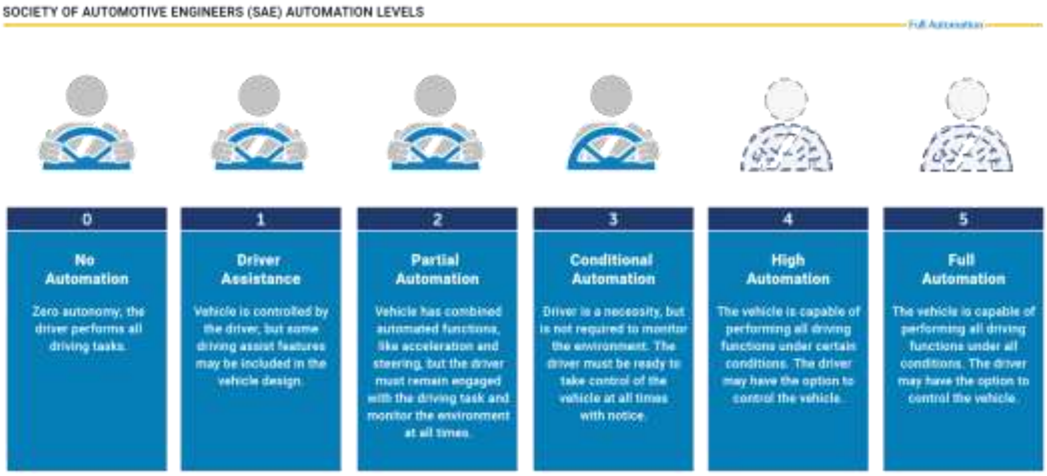
There are parallels between the aviation industry and the development of automated vehicles which may provide important lessons about how critical technology may be validated, assessed and improved. There are regulatory pathways being developed for manufacturers to include a black-box style event-data-recorder (EDR) in the event of an accident,[48] as well as a continuous data storage system for automated driving (DSSAD) proposed to store vehicle data up to 3 months as part of the future certification requirements for automated vehicles. Storage within a closed loop system of critical data such as; speed, driver attention, driver inputs and automated system inputs before, during and after a triggering event (such as airbag deployment) is pertinent for reliable safety observations, enabling the continual improvement of automated systems. [49] Further research is necessary in order to assess whether the intended DSSAD collects the necessary and sufficient data to perform a reliable analysis of an incident or if additional information concerning the context of the incident (rain, location, deceleration/acceleration in the 3D-axis, etc.) at what frequency is needed. At first sight, most data seem to be present in the vehicle and there is no need to have costly aviation-like blackboxes as reliable and technically and cost-performant systems are already developed and in use e.g. by some insurance companies to grant lower insurance premiums. The confidentiality and integrity of data stored in such systems is an essential component of the design required of manufacturers under the proposed regulation, with data older than the stipulated timeframe being erased irretrievably. The proposed regulation contemplates that access to the data will only be possible by authorised persons or agencies such as law enforcement for the purposes of accident investigation, by use of a specialised data recovery tool. [50] These Data recorders are of importance for the follow-up of the reproducibility and certification as well as who and in which circumstances has access to the stored data in them.

For automated vehicles, exhaustive testing for possible faults is problematic, due to the gap between the model and the real world. The continuous dynamics of automated vehicles are complex. It is difficult for regulators to ascertain which traffic scenarios should be tested. Additional challenges not relevant to traditional vehicles include; imperfect control algorithms, loss of connection to infrastructure, conflict between driver's instruction and faults within the system. [51] The combination of external conditions, vehicle conditions, actions of the driver, and other traffic participants create an infinite number of possible scenarios. [52]

Traffic sequence charts or catalogues may be useful in the process of developing automated vehicles, to focus the regulator's attention on the most relevant and critical scenarios. [53] Such catalogues may help to structure the development process and provide a reference test environment, providing the necessary reproducibility to achieve safer vehicles.

4.1.3 AUTOPILOT The application of project data to safety issues

AUTOPILOT testing took place across Europe and Korea using vehicles modified or created to perform part or all of the driving task without input from a driver. The vehicles used in AUTOPILOT fell within the highly automated range operating between SAE levels 3-5 as depicted below:



No Automation
Zero autonomy; the driver performs all driving tasks.

Driver Assistance
Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.

Partial Automation
Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.

Conditional Automation
Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.

High Automation
The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.

Full Automation
The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Figure 4 Level of Automated Driving[54]

4.1.3.1 Methodology

For the purposes of considering the role of AUTOPILOT data in regulation, in particular the certification of automated vehicles, we considered the Urban Driving use case and the data arising from pilots conducted at Brainport, Netherlands and Versailles, France.

The 3 pillars certification approach presented in the previous section has been applied to development and piloting of the Use Cases in AUTOPILOT.

Urban Driving involved vehicles driving autonomously between dedicated points, and the use case required the vehicle to encounter vulnerable road users (VRU) whilst in automated mode, whereupon on-board sensors and/or IoT were designed to detect and adapt the vehicles' speed and direction to safely avoid VRU. In Brainport the test involved iterations of an automated vehicle passing a crowd of people at a university campus. In Versailles, the vehicle was directed to drive between specified locations forming part of a tourist route in the city, where the vehicle encountered both a pedestrian and a cyclist. The Versailles case was particularly relevant for considering the effect of IoT in the use of automated vehicles, as it involved iterations where IoT was used, and similar iterations where IoT was disabled, and VRU were detected only via on-board sensors such as cameras. For the IoT enabled iterations in Versailles a pedestrian was equipped with a smart-watch and mobile phone loaded with an application designed to alert the pedestrian. The cyclist rode a bike fitted with an on-board unit designed to alert the cyclist of an oncoming vehicle.

The Urban Driving use case considered aspects relevant to the certification of highly automated vehicles, including how efficiently the vehicle was able to identify and avoid VRU.

Research questions included;

1. Can VRU be detected and localised using smartphone detection?
2. Can the vehicle brake and take-over control using in-vehicle sensors?
3. Can the vehicle adapt its route based on crowd information?

Hypotheses tested included;

1. IoT will extend the detection of VRUs over longer distances (such as a blocked view of in-vehicle camera) and;
2. IoT will warn VRUs of an approaching vehicle.

These questions are relevant to the proposed 3 pillar approach, in particular, for considering what type of critical and edge case scenarios may be necessary to include in the future certification of automated vehicles.

4.1.3.2 Results

At Brainport, the vehicle changed route to avoid the crowd of people, based on data provided by a Wi-Fi sniffing device searching for Wi-Fi probes or GNSS sensors within VRU devices, which was forwarded to the IoT platform Crowd Estimation and Mobility Analytics (CEMA) via 3G and 4G communication technologies. The IoT informed the automated systems about the size of the crowd, ultimately caused the vehicle to change route. [55]

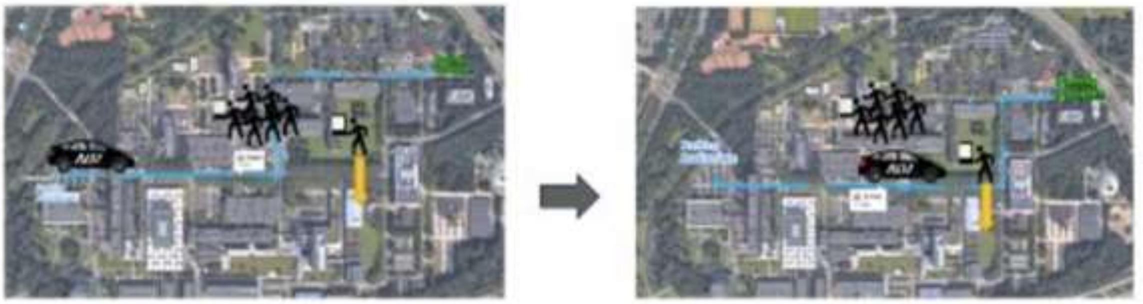


Figure 5 Iteration on the TU/e campus, Brainport[56]

In Versailles, during the first round of iterations where the IoT was switched off, the vehicle was able to detect the VRU with on-board sensors, however the detection was late and the braking occurred abruptly when identifying a cyclist or pedestrian. The 90% angle at which the cyclist crossed in front of the vehicle, proved challenging and braking was particularly hard in order to avoid the cyclist. When the IoT was switched on, the vehicle obtained information earlier.

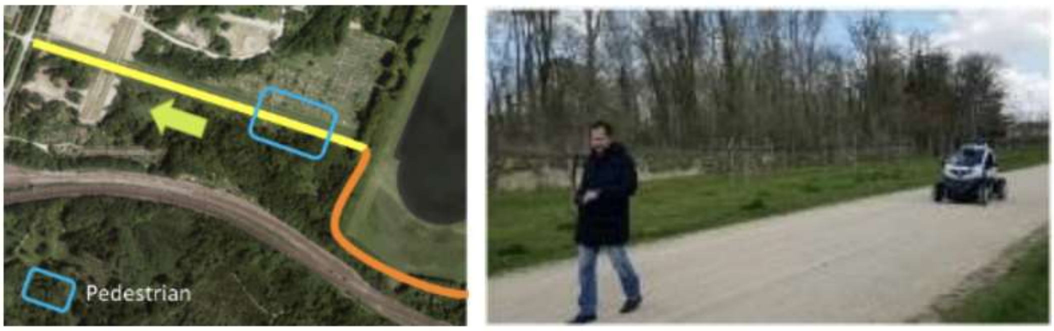


Figure 6 Test route in the castle's garden with a pedestrian who walks in front of the vehicle[57]

There was a marked difference to the reaction of the vehicle when data regarding the location and proximity of the VRU was supplied via the IoT application and platform. When the cyclist's device was connected, the vehicle adapted its speed much earlier to allow for a smooth stop.[58]

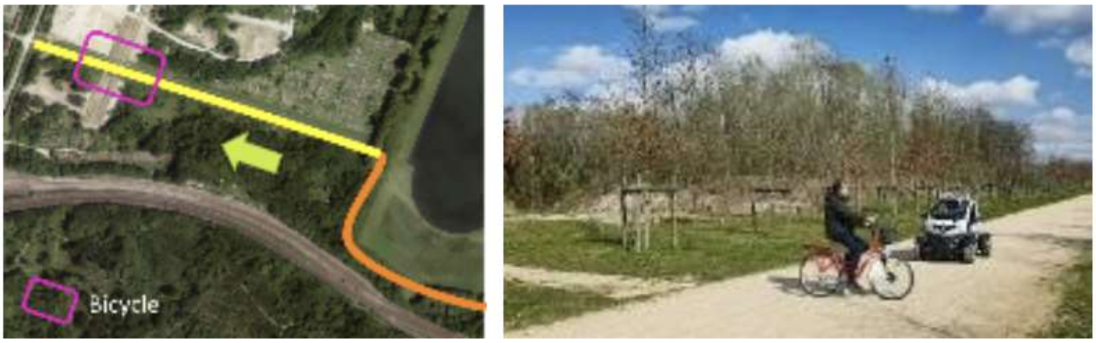


Figure 7 Test route of the AD in the castle's garden with a bicycle that crosses the road in front of the vehicle[59]

4.1.3.2 Lessons Learned relevant to future certification

Reliance upon on-board sensors such as cameras, are not likely to be sufficient to ensure the safety of the vehicle occupants and of the VRU, bringing also ethical questions like the Trolley Problem studied by the MIT[60]. In order to provide automated vehicles with enough timely information to adapt course or safely stop to avoid contact with VRU, multiple data sets may be required in the form of IoT such as mobile phones, watches, roadside cameras and on-board cameras in a V2V and V2X communication of data. It emphasises the importance of IoT for the safety of VRU, and suggests a crucial role for IoT in the development of automated vehicles, and their certification.

4.1.4 The regulatory framework for prototype testing in Europe

The legal framework for type-approval exemptions and prototype tests differ in every European Country, which impacts large scale tests such as AUTOPILOT. During the project, testing occurred in 5 European Countries (France, Finland, Italy, the Netherlands and Spain, testing also occurred in South Korea), and each country applied a different legal framework. Throughout Europe, processes for prototype testing vary, from self-certifying frameworks, to jurisdictions which administer a permission-based process. In permission-based regimes such as that operated in the Netherlands and Germany, the testing of automated vehicles on public roads may only occur within prescribed parameters, once the vehicle itself, the location and specifications relating to the test are approved. As there is no type-approval[61] for automated vehicles in Europe, prescriptive authorities require applicants to fulfil safety requirements for exemptions in respect of vehicle features which do not meet type-approval. [62]

In the example of the Brainport pilot site, all testing was overseen and approved by the Netherlands national vehicle authority, the Rijks Dienst Wegverkeer (RDW).[63] Testing approval was dependent upon research partners providing the RDW with adequate information regarding each vehicle, including how the vehicle departed from type-approval, the automated systems to be tested, while addressing safety parameters set by the RDW. After a successful completion of a paper-based application process, each vehicle operated in the Brainport use cases was physically inspected by the RDW on a test track, with approval required prior to the research taking place.

4.1.4.1 Vehicle driving licences

The Netherlands is in the process of developing a driving licence for self-driving vehicles. The concept of a licence focuses on the reproducibility and predictability of automated driving behaviour, with a vehicle and security framework being produced to assess the reliability of the technology.[64] The RDW in conjunction with the Netherlands Exam Authority (CBR) and the Netherlands Road Authority (RWS) are pioneering the software driving licence, so that the automated driving system is tested in a manner similar to that of a human driver.[65]

A parallel can be drawn between this vehicle driving licence and the certification process of the vehicle with the difference of the consideration, from a legal point of view, that the vehicle is also a “driver”.

4.1.4.1 Cross border considerations

As there is no harmonised legal framework for the testing of prototype vehicles in Europe, testing certificates issued by the RDW in respect of AUTOPILOT vehicles could not be mutually recognised in other European countries. This did not present a problem for

AUTOPILOT, as the testing of each pilot site took place within distinct legal jurisdictions, and no vehicles were used in cross-border research. However, had the methodology involved cross-border research, it would have been necessary for any vehicle approved by the RDW in the Netherlands to be re-assessed and re-approved under the national, and regional regimes of every country where it was intended to operate the vehicle. This can present challenges for large-scale, cross-border testing across Europe. Although countries such as the Netherlands have a national authority relevant to automated vehicle prototype testing, regional and municipal authorities play a substantial role in the organisation and authorisation of prototype tests, and this is often achieved separately to any national regime in place. For example, once an application to test a prototype vehicle in the Netherlands is received, the RDW negotiates the necessary permissions and infrastructure arrangements with the appropriate local and municipal authorities in the Netherlands, of which there are approximately 225. Each authority may refuse to participate in a proposed automated vehicle test, and it is only once the relevant authority agrees that the testing process operated by the RDW applies. Exemptions provided by the RDW are not mutually recognised in any other country. However the RDW has stated it may recognise an automated vehicle testing certificate from another jurisdiction, with such mutual recognition being highly contingent on the individual case and the quality of the supporting evidence.[66] The lack of a cohesive legal framework for a prototype testing regime across Europe potentially inhibits the development of automated vehicles.

There may be scope for establishing a minimum standard of prototype testing requirements across Europe, to encourage large-scale cross-border testing. Such testing would necessarily involve the cooperation of European authorities in the coordination of test routes and infrastructure. There have been developments in respect of infrastructure corridors throughout Europe, such as C-Roads, a joint initiative of European member states for testing intelligent transport systems.[67] However the necessity for duplicated legal permissions for prototype testing persists, and should be addressed.

4.1.5 Conclusion on the regulatory aspects

In the event that automated vehicles are able to increase overall road safety by even a small margin, this will reduce the number of road traffic accidents and fatalities, and provide a substantial benefit to society. Drivers and members of the public are concerned about the dangers of motor-vehicle accidents, and the introduction of technology with the potential to improve this situation may be enhanced if the standards developed are reproducible, and implemented with adequate regulation.

The adaptive strategy adopted by the UNECE and WP.29 is an appropriate method for the regulation of automated vehicle, and IoT technologies. Success will depend upon a flexible regime to permit improvements once developments have been made, while maintaining enough stability to provide public confidence in the safety and utility of the technology. The aviation industry provides important instruction as to how automated vehicle regulators may approach some issues of safety, and the development of an automated vehicle driving licence as contemplated by the Netherlands, may be a critical development in maintaining reliable standards. Improvements to technology will depend upon the quality of prototype testing in Europe, which may be encouraged by a more cohesive framework for cross-border pilots. AUTOPILOT highlights the indispensability of IoT in the development of safe automated vehicles, and lessons learned can be reflected upon in the future development of the certification framework.

4.2 Liability

A new product or a new service is always questioning new liability issues. Within this context, automated driving implies several new liability problems:

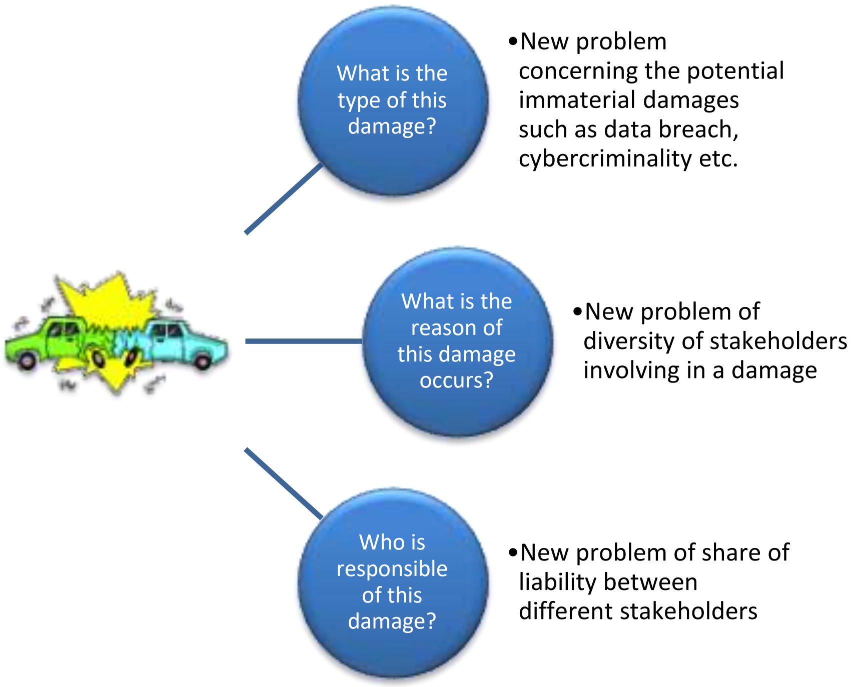

What is the type of this damage?
•New problem concerning the potential immaterial damages such as data breach, cybercriminality etc.
What is the reason of this damage occurs?
•New problem of diversity of stakeholders involving in a damage
Who is responsible of this damage?
•New problem of share of liability between different stakeholders

Figure 8 Liability - issues questioning

4.2.1 Introduction & Methodology: New paradigm of liability?

Legally speaking, the liability is defined by three cumulative elements, which represent the process of damage creation. They will allow identification of the responsible stakeholder, who will be at the origin of the event giving rise of the damage either by fault or by negligence.

These three elements are the following:

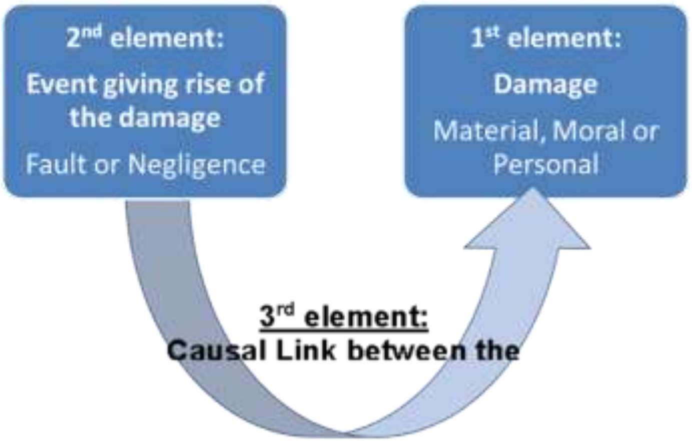


Figure 9 Liability new paradigm - 3 elements

These three elements are the basic criteria to determine liability in case of any damage. Once these three elements are clearly defined, liability can be attributed accordingly. As such, driving accidents, whether or not they involve an automated vehicle, answer to the same logical process in order to define liability of stakeholders.

Within this legal framework, the liability will be studied in this chapter following these three liability criteria.

4.2.1.1. Damage in case of driving accidents

In traditional driving, accidents can have different consequences:

- Material breach (destruction or alteration of the vehicle, public infrastructures or products within the vehicle or on the road);
- Moral harm (psychological impact, loss of time, profit, money or future);
- Personal injury (on drivers, passengers, pedestrians or any other).

In connected and automated driving, accidents will have similar consequences, except for moral harms which could be more various as for example loss of data, privacy breach, security breach, data breach, etc.

4.2.1.2. Event giving rise to damage in case of driving accidents

In traditional driving, accidents are normally caused by the following events:

- Human negligence or fault (including drivers, passengers and pedestrians), but it becomes more complex as explained in 4.2.2. with the automated system;
- Defective vehicles (including embedded products and parts of the vehicle - Council Directive 85/374/EEC of 25 July 1985[68] clearly outlines liability for defective products), for which the delineation of responsibility is not easily identifiable as described in section 4.2.3 (different stakeholders can be at the origin of an event giving rise to a defective vehicles);
- Problems with road infrastructure (including malfunctioning traffic lights and incorrect road

signs), especially today with the integration of IoT connectivity and software as mentioned in section 4.2.4 (different stakeholders can be at the origin of a fault and a negligence giving rise to a problem with road infrastructure).

In connected and automated driving, accidents will also be caused by these aforementioned events, but some new causes could also lead to an accident as for example connectivity problems, lack of update or maintenance, etc.

4.2.1.3. Causal link between the damage and the event giving rise to the damage in case of driving accidents

In traditional driving, causal link between accidents and the fault or negligence of stakeholders is quite straightforward and direct. A fault or negligence will have an impact, which will lead to an accident.

In automated driving, causal link will be more difficult to identify because the event itself giving rise to the damage will be more complex and could imply virtual stakeholders as for example artificial intelligence, software, etc. integrated into the automated system.

As such, connected and automated driving is undoubtedly complicating the attribution of liability in case of an accident because it involves a number of additional stakeholders and factors in the equation and at times blurs the distinction between the human and the vehicle. Here, we recommend to use a liability principle as a “liability tree” where the vehicle provider is the trunk, taking the liability from the driver in first line. This liability cannot be escaped. Afterwards, the first line of liability can go a second line as branches of the tree, liability this second line cannot escape. And so it can go on towards other branches. The analogy with a tree is preferred than the one of a cascade where there is the sensation of a flow and possibility to escape.

This causal link is already to be assessed during the certification process, as reproducibility principle, with the 3 pillars approach described in section 4.1.2.5.

4.2.1.4. Methodology to analyse survey results on the basis of liability concept

After this legal explanation concerning liability, the three aforementioned elements will be used as grounds for the following reasoning about automated driving and liability.

Each part of this reasoning will follow the same logical:

- Explanation of the issue identified in this part;
- Analyse of survey results relating to this issue;
- Recommendations on this issue.

The survey results highlighted three different dichotomous relating to three specific issues:
1/ Dichotomy between human and automated system relating to the new issue of automation.
2/ Dichotomy between manufacturing sand design defects relating to the product liability applied to the automated driving.
3/ Dichotomy between software and connectivity relating to the emergence of IoT.

4.2.1.5. Liability concept and Vienna Convention

As reported in D5.4[69] part "*Automated vehicles legislation overview*", according to the Vienna Convention[70] *"the driver must always be in control of their vehicle"* during the driving, settling the liability of the driving solely on the driver. Further according to D5.4, in the 2014 UNECE Amendment, it evolved towards *"the driver must be ready to take over the driving functions"*. So, the driver remains responsible even if he is helped in his driving by some Advanced Driver-Assistance Systems (ADAS).

Though, thanks to automation, a part of this liability is considered to be transferred to the automated vehicle. To be more precise, it can be transferred to the vehicle provider that did deliver the vehicle as *"product"*, according to the Product Liability Directive[71].

In the current circumstances, it is important to note that there are preliminary discussions in order to review the Product Liability Directive with position papers[72],[73] available in order to extend the product liability to services as software. In all cases, through this extension or by considering that software is embedded in the vehicle, which is a product, there is the structuration of the liability in cascade where, in first instance, the vehicle provider, mainly the vehicle manufacturer, is the liable entity in the first line, in an automated vehicle. We will now go into more details about the potential issues.

4.2.2 Automation: Driver/owner vs. Automated system

Artificial intelligence will be an important part of automated vehicles because of the involvement of the automated system in the decision-making process. As such, the liability issue for artificial intelligence would be to define the distinction between implication of the driver and of the automated system in the accident. This distinction will be the legal ground to delineate responsibilities of each stakeholder, and especially of the driver and of the automated system (IT developers).

4.2.2.1. Explanation of the issue

Within this framework, we can summarize three situations for which the driver/owner has several identities inside the vehicle:

- Driver when he has the full control of the vehicle (corresponding to the level 0 in figure 4):
  - The automated system is not used or not available into the vehicle;
  - All driving decisions made in this situation are the result of the driver;
  - The event giving rise of the damage is the sole result of the driver fault or negligence[74].
  - The causal link will be identified between the accident and the driver;
  - **Liability will be delineated as before**.

- Driver supported by the automated system (corresponding to the levels ranging 1 to 3 in figure 4):

  There are 2 cases:
  - Case 1: The automated system is used at the discretion of the driver with the

possibility for the driver to recover the control of the vehicle *("automation on demand*"**).**

- Case 2: The automated system automatically supports the driver with the possibility for the driver to deactivate it by acting differently (*"automation by default"*).
- In both cases:
    - The decisions made in these situations are done by the automated system;
    - The event giving rise of the damage is the result of the automated system at the driver's demand or automatically by the automated system itself;
    - The causal link will be more complex to identify, but it seems to be between the accident and the automated system except in some exceptions where the driver is at the origin of the event giving rise of the accident:
        - Exception 1: The driver has requested the support of the automated system in a situation not in compliance with the recommendations of use of the automated system.
        - Exception 2: The driver has requested the support of the automated system after a fault or negligence of the driver giving rise of the accident.
        - Exception 3: The automated system has supported automatically the driver after a fault or a negligence of the driver. This action of the automated system giving rise of an accident but less serious than the one caused by the fault or the negligence of the driver.
    - It seems that the liability issue will be intrinsically linked to the content of the terms of use and the liability limitations of the automated system.
    - In case the automated system has caused the first event giving rise of the accident, the possibility for the driver to deactivate the automated system does not seem to impact the liability delineation. The difficulty here is to consider the relationship between the driver and the automated vehicle. How should responsibility to override the automated system be delineated?
    - **Liability will be attributed to the manufacturer of the automated system, except if a fault of the driver is proved.**

- Driver becoming passenger because of the full control of the vehicle by the automated system (corresponding to the levels ranging 4 to 5 in figure 4):
    - The automated system automatically takes the control of the vehicle with the possibility for the driver to deactivate if needed (*"automation by default"*);
    - The decisions made in this situation are only the result of the automated system itself.
    - The event giving rise of the damage is the sole result of the automated system.
    - The causal link will be identified between the accident and the automated system except in some exceptions as for example:
        - Example of exception: The automated system has automatically taken the control of the vehicle after a fault or a negligence of the driver. This action of the automated system giving rise of an accident but less serious than the one caused by the fault or the negligence of the driver.
    - Even if the causal link between the accident and the automated system will be

identified, the problem is to clearly define where occurs the defect of the automated system which is giving rise to the accident:

- Defect in development phase: the software is not well developed and will conduct to an accident.
- Defect in performance phase: the machine-learning is bad trained by the driver and will conduct to an accident. But what happens in case of multiplicity of drivers?

How far will the system be completely representative of the driver or the IT developer? Can the driver be liable if an accident results from a decision made by the automated system that the driver would not have made? And how can the driver prove that he would not have made such decision?

- It seems that the liability issue will be again intrinsically linked to the content of the terms of use and the liability limitations of the automated system.
- **Liability will be attributed to the manufacturer of the automated system, except if fault or negligence of the driver is proved.**

4.2.2.2. Analyse of the survey results

In the survey results, it seems than the driver liability is considered less important than other stakeholders such as automakers, connectivity and mobility service providers. For example, in case of misuse or wrong data transfer, the survey shows no major liability of the driver in all cases (breakdown of data integrity/misinformation, out-dated software applications, breach in data privacy and general equipment failure).

Such result can be analysed on the business perspective, because it will not be viable for business to put the responsibility on the driver. In fact, in case of such responsibility, the driver will need more insurance covers, he will pay more for these services and driving a vehicle will become a luxury.

At the contrary if the responsibility is attributed to the automakers, connectivity and mobility service providers, these stakeholders will try to delineate responsibilities into their agreements together.

Within this framework, the automaker, as client of other professional stakeholders, seems to be in best economic position compared to the others and will be able to negotiate the agreements in his favour. That is why, the responsibilities seem to be contractually attributed to the suppliers and providers, which will also need more insurance for covering the potential damages being under their responsibility under the agreements.

To be further researched and at least considered is the fact that users do not read usage manuals with as potential recommendation the need for a specific training for the users of such a vehicle in replacement or in complement of a driving license.

4.2.2.3. Recommendations

- Concerning the automated system:
  - Giving to the driver an easy and friendly-use option to deactivate the automated system;
  - Giving to the driver the possibility to deactivate the automated system by acting

differently.

- Concerning the content of terms of use for the automated system:
    - Clearly and faithfully informing the driver concerning the use of the automated system;
    - Defining in a transparent manner the obligations of the driver relating to the use of the automated system;

4.2.3 Product liability: Manufacturing defect vs. Design defect

There are three major types of defects according to general legal theories:

- Marketing defect concerning the way a product was commercialised (for example the product was sold with inappropriate warnings or instructions);
- Design defect concerning the way a product was thought out (for example the product did not answer to its original function and each product designed will have the same defect);
- Manufacturing defect concerning the way a product was made (for example the product was manufactured with a defect and only some products manufactured will have this defect).

4.2.3.1. Explanation of the issue

Within this framework, it seems obvious than the type of defect will imply the liability. In fact, liability will be attributed as follows:

- A marketing defect will be attributed to the person in charge of marketing, mainly the original equipment manufacturer who commits a fault or negligence.
- A design defect will be attributed to the person in charge of design, mainly the original equipment manufacturer or its subcontractors in case of specific pieces, except if they have exactly followed the original equipment manufacturer's specifications and requirements. This defect will also be based on a fault or negligence because the product will be not used for its original function.
- A manufacturing defect will be attributed to the person in charge of manufacturing, mainly the subcontractors of the original equipment manufacturer, but not only as assembling brings also its own manufacturing risk, whatever it is a fault or negligence (according to product liability legislation).

The fact that manufacturing defect will occur even without any fault or negligence according to the product liability legislation, will increase the cost for the stakeholders. As such, the direct consequences are:

- The increase of potential costs for stakeholders;
- The increase of written recommendations, instructions and specifications between the stakeholders;
- The increase of watchfulness of stakeholders on liability limitations and cap;
- The increase of insurance covers for stakeholders;
- The increase of vehicles price for the user.

Liability will depend on whether the flaw lies in manufacturing or in the design.

4.2.3.2. Analyse of the survey results

In the survey results, it seems that the delineation of liability inclines always in the same direction:

- Case of out-dated software applications: major responsibility of automakers and minor responsibility for connectivity and mobility providers;
- Case of general equipment: major responsibility of automakers and equal responsibilities for connectivity and mobility providers.

The automaker, as main contact of the vehicle user[75], is clearly the person in charge to answer to the buyer in case of defect. But even if the automaker seems more responsible according to the survey results, he, as client of other professional stakeholders, seems to be in best economic position compared to the others and will be able to negotiate the agreements in his favour. That is why, the responsibilities seem to be contractually attributed to the suppliers and providers, which will also need more insurance for covering the potential damages being under their responsibility under the agreements.

4.2.3.3. Recommendations

- ➢ Concerning the design defect:
  - o Using clear and transparent specifications;
  - o Clearly delineating responsibilities of each stakeholder relating to each part of the specifications.

- ➢ Concerning the manufacturing defect:
  - o Clearly define the stakeholder in charge of manufacturing;
  - o Using a written process of manufacturing for easily and quickly finding a potential defect.

4.2.4 IoT: Software vs. Connectivity

In another way than the automated vehicle, the connected vehicles will also impact liability. In fact, the software embedded into the vehicle and their connection to the vehicle environment will extend the possibility of defects and the potential liability relating to it.

4.2.4.1. Explanation of the issue

Indeed, the difficulty would be to define where the defect occurs:

- Collection of data: software defect of the vehicle;
- Transmission in-out of data: connectivity defect or software defect of the road infrastructure or the other vehicles in case of problem in collecting data by road infrastructures or the other vehicles;
- Translation of data: software defect of the road infrastructure or of the other vehicles;
- Transmission out-in of data: connectivity defect or software defect of the vehicle in case of problem in collecting data.

Such defect can occur because of a manufacturing defect or a design defect as explained before, or also because of a lack of update. The problem of maintenance in case of software is very important because of two different issues.

First one is the provision of the update. How transfer quickly the update to the user?

Second is the time to perform the update. When is the best time to perform an update? Automatically when the vehicle is off whatever the potential urgent situations of the user? Automatically when the vehicle is on whatever the risk for the user? Or at the request of the user with the risk that the user does not perform the update even if this is a major update?

4.2.4.2. Analyse of the survey results

In the survey results, it seems that the delineation of liability is mixed between automakers and connectivity and mobility providers:

- Case of breakdown of data integrity / misinformation: equal responsibility for all actors;
- Case of breach in data privacy: major responsibility of mobility providers and equal responsibility for automakers and connectivity providers;

This mix seems logical in light of previous reasoning and the increase of potential accidents caused by software and connectivity problems will enforce the automakers to precisely in detail the authorized use of the software and infrastructure as well as the software development process. This documentation will be a strong basis for the judge in case of legal suits after an accident.

4.2.4.3. Recommendations

- Concerning the software:
  - Clearly defining the software development process in order to find out the defect;
  - Providing secure and easy-performed updates to the users.

- Concerning the connectivity:
  - Limiting the use of connected vehicle within well connected areas;
  - Delineating responsibilities of each stakeholder relating to potential connectivity issues.

In some projects like EUEIP[76], "Operational Design Domains" (ODD's) have been introduced to define the level of readiness of an area depending a.o. on their connectivity levels.

4.2.5 General recommendation: Management of causality chain and at the same time of liability chain

In order to get some distance from this liability issue and having the ability to formalize recommendations, it seems necessary to integrate this analysis into an international legal framework, and especially into the application of Vienna Convention on road traffic.

First paragraph of Article 8 of Vienna Convention on road traffic of 8th November 1968 providing that: *"1. Every moving vehicle or combination of vehicles shall have a driver. […] 5. Every driver shall at all times be able to control his vehicle or to guide his animals."* has been amended on 23rd March 2016 in order to add new 5bis paragraph such as:

"Vehicle systems which influence the way vehicles are driven shall be deemed to be in conformity with paragraph 5 of this Article and with paragraph of Article 13, when they are in conformity with the conditions of construction, fitting and utilization according to international legal instruments concerning wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled

vehicles. Vehicle systems which influence the way vehicles are driving and are not in conformity with the aforementioned conditions of construction, fitting and utilization, shall be deemed to be in conformity with paragraph 5 of this Article and with paragraph 1 of Article 13, when such systems can be overridden or switched off by the driver."

This amendment of Vienna Convention of 8th November 1968 shows the necessity to adapt the regulation in order to integrate the new problems caused by the question of automated systems on road traffic:

- First paragraph of this amendment: In this case, the liability seems to be transferred from the driver to the automated system and at the same time to the stakeholders in charge of the construction, fitting and utilization of the automated vehicle.
- Second paragraph of this amendment: In this case, the liability seems to be shared between the automated system which causes the event giving rise to the eventual damage and the driver who is able to override or switch off the automated system.

As aforementioned in this chapter, the automated driving will shake up the causality chain and at the same time the liability chain between the different stakeholders. These chains will become more and more complex in the future and the identification of each liability and the link between each of them will be the result of a true precision work.

This work of identification shall be based on strong technical tools, which will allow to distinguish each liability. One potential opportunity is the Blackbox or data recorder (which is a sophisticated record device) just like what it is done in aircraft industry. This parallel with aircraft industry is interesting for applying some principles to the automated and connected vehicles[77], because aircraft becomes more and more automated like cars. The article also refers to the *"possibility for manufacturers to escape liability when the defect is due to compliance with mandatory regulations"*. This brings forward the importance of crafting regulation which defines clear liability associated with roles at each level of automation in order to foster trust and clarity of the user in the system.

This question of data storage system for automated driving is seriously studied by a working group in UNECE[78] in order to be able to trace the causality link in case of damage. These Blackboxes will allow the definition of a hierarchy of liabilities between stakeholders for delineating and sharing responsibilities. As mentioned earlier in section 4.1.2.5, it should be further investigated whether the data foreseen in the EDR and DSSAD will be sufficient for the determination of the causality in an incident case.

In a regional level (European Union), a group of consultants[79] has expressed their opinions on Blackboxes / in-vehicle data recorders to the Commission. According to this group, the Blackboxes *"can be used in cars and commercial transport as a valuable research tool to monitor or validate new safety technology, to establish human tolerance and to record impact speeds"* or *"to influence driving behaviour and facilitate forms of automatic policing (100% surveillance of all traffic offences)"*. But even more important, the investigation of the circumstances of an accident will be a very valuable source of information to help perfecting the technology, the road infrastructure, the connectivity, the drivers or operators themselves. This is thus recommended for continued improvement.

Two different type of in-vehicle recorders are distinguished (both interesting for liability issues):

- crash data recorders collecting data over a period before and after a crash (which allows to identify liability in case of damage) → such recorders are already used in different countries, especially for commercial transport;
- journey data recorders collecting data concerning driving behaviour and law infringements (which allows to identify liability of driver in case of machine-learning automated system involved in a damage) → such recorders are already used, especially in European Union with tachographs.

The major recommendation is to adapt the concept of Blackbox for automated vehicles with collecting data which will trace the damage to identify the causality chain and like so the liability chain. Several countries, as for example Germany or United Kingdom, have already indicated their will to made data recorders mandatory in automated vehicles**.**

4.2.6 Conclusion: What new for insurance to cover liabilities?

Even if driving habits will change and introduce a hybrid environment (including more shared liabilities), most of driving accidents will still occur in *"traditional"* mode in the near future, but certain new kind of crashes could also occur. For example, pedestrians might quickly become accustomed to the increased safety provided by the automatic braking system such as the reduction of noise of electric vehicle. Thus, in case one automated vehicle did not act in the way that could be expected, they could be seriously injured. Therefore, along with the development of automated driving systems, it is essential that education and awareness not only of drivers, but of all street users are increased.

Nevertheless, the driving habits change (and especially automated driving) might quantitatively reduce the number of crashes. By limiting or even eliminating the element of human errors, recourse to driverless cars is forecast to reduce motor accidents considerably, thus diminishing the number of small insurance claims due to human distraction: however, the remaining claims due to e.g. manufacturers' bugs will probably be the biggest and fatal ones. That might imply a substantial impact on the insurance industry and its business model.

Within this context, new forms of insurance might arise. First, manufacturers will probably need to insure against the potential for failure through software bugs, memory overflow, and algorithm defects (and the resulting massive liability). Secondly, as cars become more automated and incorporate more hardware, software and depend also on external data, insurance against cyber theft, ransomware, hacking, and the misuse of information related to automobiles can become vital. Finally, as driverless cars will probably shrink the motor insurance risk pool, additional reinsurance activity may be seen in the motor market.

Where liability has to be shared between various parties it follows that insurance matters will become more complex. The intricacies of whether the fault is assigned to the vehicle manufacturer, the owner, the software provider, or the maker of a specific piece of equipment will impact insurance recovery. Also, it is likely that in the future most fully automated vehicles will not be owned by individuals, but by other service providers (such as ride-sharing services) which will act as new risk takers. It seems quite obvious than fleet and leasing will increase in the future in parallel with the price explosion of vehicles and insurances.

4.3 Data Sharing

4.3.1 Methodology

The following section reviews the current research and already established regulations concerning data sharing topics e.g. from the standpoint of an IT-service provider.

4.3.2 Data privacy

The leading trend and future development gurus predict that the digital future cannot develop successfully without taking account of people's concerns. The futurist Matthias Horx talks about the megatrend of "mindfulness" for the next five to ten years and predicts a "rehumanization" of the Internet. Adapting early on to current and upcoming developments with data protection solutions is crucial. For instance, companies and organizing need to set out principles for big data solutions and the Internet of Things to make their future products successful.

Data privacy is no obstacle to the successful marketing of data-based business models; on the contrary, the competent use of data privacy-compliant solutions gives customers confidence, as a key prerequisite for the successful marketing of data-driven business models. Considering the aspects of data privacy law in conjunction with business models that use analysis techniques, existing data and/or freely available data and/or purchased data to add value and create new knowledge is crucial for building future business. Marketing this newly created knowledge is the basis for business models.

Topics such as the Internet of Things (IoT) and automation play a pivotal role here, because they create mass data. Big data technologies, modern data analysis techniques and artificial intelligence for evaluating, interpreting and refining data are the principal tools used in data-driven business models.

Big data analyses draw data from a wide range of sources. Much of this data touches on the personal sphere and allows a wide range of conclusions to be drawn, both directly and indirectly, about the circumstances and behaviour of data subjects. The key is to strike the right balance between the interests of individuals in protecting their personal data, and the interests of companies or authorities in using new analysis techniques. This presupposes that companies and authorities operate transparently and in compliance with data privacy regulations.

4.3.3 Big data and privacy

The ever-increasing numbers of networks connecting people, devices and sensors is allowing a seemingly infinite amount of data to be collected, stored, processed and analysed. With cars becoming connected as part of the internet of things, the potential of data collection and big data analytics grows even more. This of course has major repercussions for privacy issues especially with respect to the abuse of personal data. It also has an impact on the actual possibility of sharing data and reusing them. If not correctly designed a tremendous waste of data could be envisaged.

Under the existing regulatory drafts, the competitive disadvantage for telecommunications providers in Europe remains in sub segments. Including the over-the-top service providers (such as WhatsApp and Skype) in future is only part of the solution. Compared with the General Data Protection Regulation, telecommunications providers face much tighter constraints on processing data. As a result, the telecommunications sector will have fewer opportunities to exploit big data applications than other sectors of the economy. After all, metadata can only be processed with the customer's consent under the current draft of the planned e-Privacy Regulation. Unlike in the General Data Protection Regulation, data cannot be further processed using pseudonyms for compatible purposes. As such, various service models, which the user could find useful, but which are not feasible with anonymous data, cannot be offered: These may include products for looking for a parking space, accident prevention services, on-demand TV programming or tele-monitoring services in the health care segment or usage based insurance and assistance as well as other safety/security services such as Stolen Vehicle Recovery.

MNO's, for example Deutsche Telekom, increasingly uses big data technologies to determine the likelihood of its network components failing, and to support troubleshooting. These initiatives aim to provide greater availability of network and other services, as well as reducing faults in the entire communications infrastructure. To ensure data-privacy conformity of these kinds of analyses, the individual measures were coordinated closely with Group Privacy.

Basically, the analyses tend to involve assessing technical parameters of products and of the individual components in the local loop. This kind of data is not associated with any given individual and is assessed in accordance with certain fault patterns to enable conclusions to be drawn on the infrastructure vitality; this data can, however, not provide any statement on the failure probability or fault in the customer-related portion of the local loop.

Customer traffic and usage data is accessed solely on the basis of § 100 German Telecommunications Act (Telekommunikationsgesetz – TKG) to eliminate errors and faults, taking into account the current version of the draft Regulation on Privacy and Electronic Communications (Art. 6 (1b)). The first step involves verifying whether the purpose behind processing this data complies with the legal provisions and the data is used to eliminate errors and faults. The second step involves providing an analysis based on pseudonymized data, or where specific faults reported by customers exist, based on plain data. Big data analyses are therefore completed in this context with

- Technical parameters without any association with a given individual,
- Anonymized data, or
- Pseudonymized data, or
- Plain data (where specific customer-related faults exist)

4.3.4 Personalised services versus privacy infringement

Collecting, storing and other processing operations of personal data are essential in order to provide a personalised mobility. A connected car can access data from a range of sources but when the grounds for processing data is consent and the data is not used strictly for the purpose for which the owner gave consent, it could give rise to serious legal issues. Similarly, if the data is not used solely for the stated purposes, legal problems could arise.

1. Privacy and Security Assessment process (PSA process) –a core element in safeguarding security and data privacy at telecommunication companies.
2. The standardized process implements security and data privacy requirements as part of product and system development, ensuring greater transparency, improved project support, and a suitable level of protection for the products, services, platforms, and IT applications through compliance with requirements for data privacy and security.
3. The PSA process has enabled us to put in place the foundation for uniform support in relation to security and data privacy issues. All development projects and system releases that create or change IT or NT systems are categorized, taking into account the data being processed, attack vulnerability from the public Internet (hereinafter referred to as criticality), and complexity.
4. Security and data privacy experts provide ongoing consulting and review functions for highly critical and complex projects and system releases. Before such projects go live, they need to be expressly approved.

4.3.5 Legal questions and risks

Allen & Overy (2017) point out some of the legal questions and risks linked to data collection and usage:

- **Customer awareness:** Transparency and purpose limitation specifications in data protection laws require customers to be informed about exactly how their data will be used and to get their permission to use their data for that purpose.
- **Data minimisation:** The concept of data minimisation states that there should be minimal data processing and that data should only be stored until necessary. The “Privacy by Design” principle of the GDPR, which states that data protection safeguards must be put in place from the very beginning, also seeks to find a balance between the contrary forces of data minimisation and big data. Nevertheless, data minimization has to be balanced with data quality in order to deliver service quality needed for the deployment of big data.
- **Storing and processing data under EU law:** Since the transfer of personal data outside of the EEA is restricted, the partners involved must have a compliance framework to be able to share data across national borders within the bounds of the law. The framework must eventually extend beyond data exchange between EU Member States for global compliance. Therefore, customers have to be informed and give permission about any of their data being stored in Non-EU countries.
- **Good data governance:** An individual’s vehicle speed, performance and location could be used for public benefit in the complete overall scheme of a connected vehicle system. It would be useful to define standards that make it impossible to identify individuals to enable the use of such anonymized data In any case of private data used by service provider written permission is required, e.g. for customers that wish Usage Based Insurance solutions.

The GDPR imposes severe penalties on firms that fail to comply and put consumer data privacy at risk. In order to conform with privacy legislation, especially the GDPR for instance, all participants[80] in the IoT and automotive sectors will have to take adequate measures to avoid risks of privacy infringement. Using cloud-based IoT connectivity for AD can magnify the benefits of connected and automated driving and provide a truly personalised and secure automated driving experience. Due diligence will be especially needed for access control for the IoT cloud, data anonymization and encryption, and matters of data ownership, etc. must be clearly defined[81]. Code of conducts are highly advisable for both enabling data transfer, demonstrate compliance and accountability.

All 4 topics listed, must be considered in the AD use case context, i.e. use cases which are safety critical and those which are addressing comfort aspects of mobile service delivery. Data segmentation includes privacy concerns but also public security. The following data segments can be considered as relevant for such an AD use case analysis linked to GDPR:

a) Passive speed data from GNSS satellite receivers collecting data inside the vehicle: This data is linked to a device and not to a driver, as long as the device is not installed into the vehicle. If agreed on, personal data can be included into the sent out data streams, e.g. insurance related personal data. (Only uplink or for coaching purposes, or positive incentive purposes; it enables the raise of other business models).

b) Active speed data from sensors inside the vehicle, e.g. wheel sensor:
Usually, this data is linked to the vehicle identification number (VIN) via CAN Bus and communication modules. Compared to the unspecified and passive GNSS receiver, active data is more critical as GNSS speed tracks are not seamless and are only linked to the mobile device. In case of GNSS equipped smartphone, drivers can switch them off any time and have non-seamless speed tracks in an external server. (Uplink & Downlink)

c) Other passive sensor data from mobile devices with or without SIM cards:
such data is not directly linked via connectivity module to the vehicle. These so called nomadic devices have the same characteristics with regards to data privacy as the above mentioned speed data. There are no seamless sensor data tracks possible and smart big data filter technology have to be applied in order to generate valid data for business purposes, e.g. for customer centric data analysis of travel or driving behaviour via big data AI algorithms. (Only Downlink)

d) Active sensor data from the vehicle sent out via communication module to a third-party server with no safety relevance:
This category includes acceleration behaviour indicating the quality of traffic management or road infrastructure or data exchange between the vehicle’s navigation system (POIs) and driver behaviour relative to these POIs, e.g. the frequency of stops in POI listed shopping malls. As CAN-Bus data is linked to the VIN, the data can be abused for advertisement purposes, nevertheless no direct harm or damage is causes. From GDPR point of view, data has to be anonymized before it is sent out. (Uplink / Downlink)

e) Active sensor data from the vehicle sent out via communication module to a third-party server with safety relevance:
This includes all available sensor data, which is sent to a server in case of an emergency call (uplink e-Call default). VIN and personal data are required, e.g. blood type. Except of e-Call, all type of sensor data detecting instable driving behaviour forcing the vehicle to drive anonymously. In this case, personal data has to be shared in order to initiate accident prevention. Here GDPR is fulfilled as long as the driver agrees aforehand to share his data in

such cases.

f) Video data (uplink) and teleoperated driving (up- and downlink):
All data which allows pattern recognition and personal identification has to be analysed carefully in order to avoid any potential abuse. In Hamburg for example, the installed infrared cameras cannot be used for face recognition algorithms, whereas video cameras were rejected by the public authorities due to privacy concerns. In other countries, these privacy concerns may not apply, e.g. P.R. China, nevertheless other regulatory frameworks for AD services and data distribution apply.

The given examples show that data segmentation can be developed from many different angles, where security concerns are an important aspect of segmentation. But other aspects, such as sensor type (active, passive, vehicle-centric or nomadic) or others might have the same relevance for setting up appropriate data segments and categories of GDPR relevance. As GDPR is in place no longer than recently, new data standards and categories have to be formulated and agreed on taking concerns of all parties into account: private and public sector, industry and consumer markets.

During the AUTOPILOT Large Scale Pilots, everything was prepared to collect technical data for further analysis and evaluation, according to the WP4 guideline[82]. Even though no personal name was collected for the testing nor for evaluation purposes[83], we cannot prevent that by combining several sources of information, like geolocalisation and external video cameras, personal data could be spotted although such a risk is minimized and would mean that the threat would be an internal threat due to the need to have access to such sources of information. This is the reason why we recommend that Privacy-enhancing and privacy-preserving techniques to be used in case of IoT usage.

4.3.6 Privacy-enhancing and privacy-preserving techniques

Several EU projects funded under ICT-18-2016[84], ICT-14-2016-2017[85] and ICT-15-2016-2017[86] have addressed the privacy-enhancing and privacy-preserving issues in the context of the acquisition, analysis, curation, storage and usage of big data. As many datasets generated from AUTOPILOT are IoT-enabled and can be easily integrated with other big data sources, these privacy enhancing and preserving techniques should be considered (and preferably used) in the AUTOPILOT project [87].
The e-SIDES project[88] carried out a comprehensive literature review of eleven privacy-enhancing and privacy-preserving technologies which are briefly summarised as follows.

1. **Anonymisation**: Encrypting or removing personally identifiable information from datasets by using full de-identification models such as k-anonymity, l-diversity, t-closeness and differential privacy.
2. **Sanitisation**: Encrypting or removing sensitive information from datasets by using sanitisation techniques such as masking data, substitution, shuffling and number variance.
3. **Encryption**: Big data applications require fine grade sharing policies using cryptographic primitives include ABE, IBE, PRE and functional encryption.
4. **Multi-party computation (MPC)**: Distributing data and processing tasks over multiple parties to allow securely computing the result of any function without revealing the input data.
5. **Attribute Based Access Control (ABAC)**: Supporting fine grained access control policies in big data based on attributes that are evaluated at run-time.
6. **Automated policy enforcement mechanisms**: Focusing on the enforcement of rules for the

use and handling of resources to ensure that data policies do not get lost or neglected in the course of data being transferred between different systems.

7. **Accountability**: Providing the provision of automated and scalable control and auditing processes that can evaluate the level of compliance with policies.
8. **Data provenance**: Attest the origin and authenticity of information.
9. **Transparency**: Explicating information collection and processing to allow data subjects informed choices.
10. **Access and portability**: facilitating the use and handling of data in different contexts, and enabling data subjects to change service providers without losing their data.
11. **Users control**: Specifying and enforcing rules for data use and handling by using consent mechanisms, privacy preferences, sticky policies and personal data stores.

More recently, two EU big data-focused projects (i.e. NOESIS and LeMO) are identifying and addressing the potential privacy and security concerns. NOESIS focuses on the assessment of possible areas of misuse and potential danger that arise with the implementation of big data generation and technologies in the field of transport. LeMO aims to bring crucial issues linked to privacy, data security and legal aspects to the forefront, paving the way for future legal framework for the collection and exploitation of big data in transport. So far, no deliverables have been published, although at company level, all GDPR relevant documents are publicly available so that suppliers can implement them in advance and become compliant to the regulations. However, the AUTOPILOT Task 4.6 team will work closely with these projects to ensure that their relevant outputs are taken into account when handling the IoT-enabled personal data.

4.3.7 Data-driven Insurance

As interconnection of intelligent transport systems necessarily implies the collection, processing and transfer of huge amounts of data, it will be vital for insurance companies to have access to such data in order to provide better services and be able to provide a full coverage for all the actors involved and the risks they are subject to.

In this context, regulation the field of in-vehicle access to data should make a careful and clear distinction between customer provided data (i.e. personal data of the driver and passengers of the automated vehicle, such as data concerning localization, mobile synchronization) and vehicle-generated data (mostly technical data). Thus, while customer provided data, as personal data, shall be subject to the GDPR (with all the relevant consequences e.g. in terms of legal basis of the processing), all (non-personal) vehicle-generated data shall be freely processed outside the scope of the GDPR; all the more so, considering that some subjects (such as insurers) need free access to these data in order to better fulfil their contractual obligations towards their client with a clear and explicit consent request, enabling trust through transparency. Another point that regulators should take into account in the field of access to data in the context of intelligent transport systems is the need to ensure interoperability between data generated by connected/automated vehicles and infrastructure in the so-called “smart-roads”. In order for interconnection of intelligent transport to be fully effective, as well as for insurance to truly become data-driven, it is essential that universal and binding standards are set.

4.3.8 Results

For MNOs and IT service providers the acceptance of IOT products is closely linked to personal data protection, which is why these organizations introduced strict PSA procedure and decided to publish them in open web-sites. When the grounds for processing data is consent and the data is not used strictly for the purpose for which the owner gave consent, it could give rise to serious legal issues. We recommend that the consent shall therefore be very explicit and include the ability to process data with regards to provision of personalized services. It should be the data subject's decision to allow it or not.

Here at stake is data protection by default. Note that while directive 46/95 referred to the right to privacy. Regulation 679/2016 refers to data protection changing altogether the fundamental right of primary reference in the Treaty (charter of fundamental rights). All the language in the regulation now refers to data protection rather than to privacy.

For now, it is important to summarize the findings of the before mentioned data sharing topics once the gathering of information is complete and to detailing more the regulations concerning ePrivacy activities.

4.4 Cybersecurity

The legal stakes around data security are extremely high for connected and automated driving. Cybersecurity breaches would have major legal and business consequences for car manufacturers, other equipment makers, service providers, mobile network operators and all other stakeholders.

4.4.1 Key Principles

The following list provides some key principles related to cybersecurity in vehicular systems.

- Defence in depth for the highest risk threats. Threat mitigation should not rely on only a single cybersecurity control while leaving other vulnerabilities could let opened a door to hack and exploit the system if the primary cybersecurity control is penetrated.

- Protect sensitive data and personally identifiable information. PII stored on the vehicle should be protected, and access to the data stored should be controlled and limited. To reach the previous mentioned the next points should be followed.

    - Ask to the responsible of the data before collecting or transferring it.

    - Prevent unauthorized access from third parties by protecting data stored in access control lists.

    - Limit the default access settings.

- No permission to make changes to calibrations or software that have not been analysed and tested.

- Least privilege principle, all the components should run with the fewest possible permissions.
- Vehicle owners should not be capable, intentionally or unintentionally, to make unauthorized changes to the system that could introduce potential vulnerabilities. Some ways that can introduce vulnerabilities in the system are for example.
    - Change calibration settings or software to get different powertrain performance features.
    - Software provided by devices such as USBs, Bluetooth-paired phones, etc. These devices may attempt to install not controlled features via the vehicle's entertainment systems. All the software installations must be informed to the users and agreed.

4.4.2 Analysis of evaluation methodologies

The process of evaluation of the cybersecurity of the system has not only one way of being performed. It depends on the characteristics of the system itself or the accuracy to be achieved using the evaluation.

In this chapter, a set of evaluation methodologies recommended by the SAE J3061 or other guidelines is analysed. The most used methods in research projects are EVITA, HEAVENS, OCTAVE, OWASP and FERMA. Each of these methods has its advantages and its disadvantages according on the purpose in which they are used. In the next lines, the overview of the most recommended methods to perform a TARA is depicted:

- **EVITA:** One of the most common TARA methods used in the research projects and recommended in the SAE J3061. It is consisted by a set of top companies in the automotive industry. This methodology provides a detailed procedure for the computation of the risk score for each discovered threat according to a set of predefined rules. The main idea of this project was to design a vehicle architecture protected against tampering and maintain the sensitive data protected against compromise[89]. The EVITA project considers threat identification and threat classification. In the threat identification the idea is to consider a generic scenario in which is possible to identify the cybersecurity threats. Once the threats are correctly identified, each threat could be classified according to its class, motivation, attacker capabilities, etc. All these threat features will influence a final degree of criticality.

- **HEAVENS:** This methodology is focused in the methods, processes and tools for the identification of the threats and risk assessment. The main idea of the project is to provide a systematic methodology which would get accurate results after threat identification and risk assessment processes. The main features of this method are: Applicable to a extend variety of vehicles, provide references between security attributes and threats during analysis, and finally, the model refers the security objectives with the impact each threat has. The phases of the HEAVENS security model are: Threat Analysis, Risk Assessment and security requirements.

- **OCTAVE** is best suited for enterprise information security risk assessments. OCTAVE is especially good at bringing together stakeholders with system experience and subject matter experts with security experience through a progressive series of workshops to develop a thorough organizational and technological view of the problem domain. A series of detailed worksheets are completed in the workshops to identify assets, current practices, Cybersecurity requirements, threats, and vulnerabilities and then to develop a strategy and plan for mitigating risks and protecting assets.

- **FERMA** is used to manage the threats and opportunities to organizations within acceptable limits. The principles of risk management are identifying, measuring and preparing for any events that could interfere with the organization's plans. Enterprise risk management (ERM) is a strategy that applies these concepts across the whole organization. FERMA can be adapted to identify risks on cybersecurity and plan according to the level of the risk identified.

Each method has its advantages. The FERMA method is simpler than EVITA method but has the advantage of assign a severity level from LOW to HIGH. In the other hand, EVITA method is detailed and provides eight levels of severity from S0 to S4, where S0 means there are not risks of being affected under the evaluated threat, and S4 represents a risky threat for multiple vehicles. EVITA method also classifies the risk according to fur different classes: safety, operational, financial and privacy. FERMA method is preferable to use for this project as it is not specific for vehicles. For this reason, there is a clear advantage of the FERMA method over EVITA, OCTAVE or HEAVENS method if the threat affects IoT devices and not only the vehicle itself.

4.4.3 Evaluation Methodology

The cybersecurity objectives for IoT are focused on providing Confidentiality, Integrity and Availability to the system. The first step in a cybersecurity evaluation is the identification of potential cybersecurity issues. This phase starts with the feature definition in which the technology is studied. The study consists on the elaboration of a report about the used technologies in the system. This report considers communication channels, communication protocols, hardware, etc.

In the second step, initiation of cybersecurity plan, the report exposes the state of the art of the cybersecurity threats related to the features of the system. Threats regarding to back-end services, communication channels, updates, unintended human actions, external connectivity and connections.

In the third step, the threat analysis risk assessment is the method to compute the risk according to the possible threats. The recommended method for computing the risk is the FERMA[90] standard approach. The TARA can use different method as is evaluated in 4.4.1 as example is defined the FERMA method. This method permits to compute in a standard way the risk score according to different grades of severity. Each threat detected in previous steps must be evaluated using this method.

Table 1 FERMA Standard

IMPACT	LIKELIHOOD		
	Low (L)	Medium (M)	High (H)
Negligible (N)	Low	Low	Medium
Marginal (MA)	Low	Medium	Medium
Critical (C)	Medium	Medium	High
Uncontrollable (U)	Medium	High	high

In the fourth step, the cybersecurity concept consists in the development of the security plan for the threat study, threat prevention and threat mitigation. This phase could include a definition of a penetration test plan as a security check, draw the route map to be followed according to the known threats and the score risk they have. The threats should be analysed, and the risk should be considered in order to determine the actions and countermeasures to be applied. The idea is to isolate the elements that are the source of the problem. When the source of the problem is known, the process continues classifying the problem into: hardware, protocols, interfaces, channels of communication, encryption key failure, etc. Taking into account the source of the problem, the cybersecurity concept will provide some options to solve or mitigate the problem to reduce the risk to the minimum possible.

Finally, the cybersecurity assessment consists of the process to execute the security tests and apply the security concept. Extracting conclusions from the analysis of the threats and apply preventions and mitigation against them. See possible legal responsibilities in threats in relation to data privacy, in case of leakage.

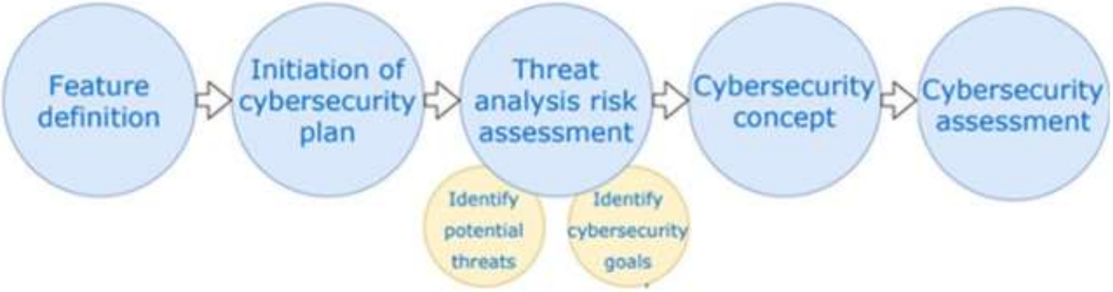

Feature definition
Initiation of cybersecurity plan
Threat analysis risk assessment
Cybersecurity concept
Cybersecurity assessment
Identify potential threats
Identify cybersecurity goals

Figure 10 Methodology adapted and based from SAEJ3061

4.4.3.1 Assessment process

Each threat should be considered with the possible tests to evaluate the possibility of exploitation. The use of threats and vulnerabilities databases helps the test users to elaborate the penetration tests for the evaluation of the risks. The results of the tests will determine, joined to the risk score of the threat, the possible actions to be executed in order to mitigate the risk if it is necessary. If the risk score is high and the result of the pentesting shows the possibility of exploitation, the threat must be solved. In case of a low risk score and the result of the pentesting shows it is not possible of exploiting (under the conditions of the tests), the mitigation actions of the problem should be considered.

Once the cybersecurity goals are defined, it is necessary to determine whether the vulnerabilities associated with the risks encountered exist in the vehicle at the beginning of the test. This step follows a similar methodology to "pentesting" in the IT world:

- **Recognition** - The vector to be tested is investigated to learn the technology used and the possible ways to attack it.
- **Enumeration** – Data found from the vector in the vehicle are listed and will be used for further analysis and exploitations.
- **Analysis -** Potential vulnerabilities existing in the system and threats that can pose risks to the vehicle are analysed. The previously calculated risk eases the analysis.
- **Exploitation** - The potential vulnerabilities are demonstrated by attacking the vehicle and checking whether the tested vectors are protected against these attacks. If the attack is unsuccessful, it means that the vehicle meets the prerequisites and thus can be considered protected.
- **Documentation** - Test results are analysed and the level of the vehicle's cybersecurity is documented, providing a rating.

4.4.4 Cyberattacks and liability

Cyberattacks on a vehicle, particularly an automated driving one, in an IoT system could have direct consequences for the safety and privacy of the user. Any of the electronic devices in a connected car or the car itself could be vulnerable to cyberattacks through various entry points. In this case, the private data collected by the system to enhance the safety and comfort of the automated driving experience could be used for exactly the opposite effect. The responsibility of each participant in the IoT connected automated car ecosystem must be clearly considered. Ultimately, they shall have adequate tools in place to prevent security threats that are proportionate to their legal liability.

Connected and automated vehicles are nowadays the objective of malicious hackers. Stored and exchanged data by the vehicle and IoT services might show the behaviour of the user. The data contains a lot of personal information that, in case of not being protected enough, could affect the user in case of disclosure. An attack could also create safety issues for the members of the vehicle and around it too. In case the attacker gets access to the data, it is usually sold and used for threating. According to the GDPR, if a device or a service needs data from the user for working, data must be handled in a secure way. The IoT devices and the vehicles usually have resources limitations, but they have to be assured as other devices which do not have these limitations. IoT systems must include intrusion detection systems, firewalls, encryptions, secure storage, etc. In case these security requirements were not covered, the legal responsible of data leakage has to be clearly defined.

The main vulnerabilities are related to connectivity vectors. Connectivity vectors are the vehicles entry points that give access to functions inside the vehicle as: WiFi, RKE, GPS, TPMS, USB, OBD, Bluetooth and new ones that can come. The security issues related to these technologies have to be followed up closely because the vulnerabilities are found constantly.

4.4.4.1 Threats

According to UNECE, there are some known threats to vehicles[91] and the vulnerabilities can be classified in relation to the threats.

- Threats regarding back-end servers:
  - Back-end servers used as a means to attack a vehicle or extract data.
  - Services from back-end server being disrupted, affecting the operation of a vehicle.
  - Data held on back-end servers being lost or compromised ("data breach").
- Threats to vehicles regarding their communication channels:
  - Spoofing of messages or data received by the vehicle.
  - Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data.
  - Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks.
  - Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders.
  - Denial of service attacks via communication channels to disrupt vehicle functions.
  - An unprivileged user is able to gain privileged access to vehicle systems.
  - Viruses embedded in communication media are able to infect vehicle systems.
  - Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content.
- Threats to vehicles regarding their update procedures:
  - Misuse or compromise of update procedures.
  - It is possible to deny legitimate updates.
  - Misconfiguration of equipment or systems by legitimate actor, e.g. owner or maintenance community.
  - Legitimate actors are able to take actions that would unwittingly facilitate a cyberattack
- Threats to vehicles regarding their external connectivity and connections:
  - Manipulation of the connectivity of vehicle functions enables a cyberattack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications.
  - Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems.
  - Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems.
- Potential targets of, or motivations for, an attack:
  - Extraction of vehicle data/code.
  - Manipulation of vehicle data/code.
  - Erasure of data/code.
  - Introduction of malware.

  - Introduction of new software or overwrite existing software.
  - Disruption of systems or operations.
  - Manipulation of vehicle parameters.
- Potential vulnerabilities that could be exploited if not sufficiently protected or hardened:
  - Cryptographic technologies can be compromised or are insufficiently applied.
  - Parts or supplies could be compromised to permit vehicles to be attacked.
  - Software or hardware development permits vulnerabilities.
  - Network design introduces vulnerabilities.
  - Physical loss of data can occur.
  - Unintended transfer of data can occur.
  - Physical manipulation of systems can enable an attack.

Also, for more information about detailed information on cybersecurity threats is possible to check D1.9[92].

For an IoT environment we can expose a few examples of threats with already calculated level of risk using the mentioned FERMA standard.

<table>
<tr><td colspan="3"><b>Risk/Threat #1:</b> Loss of information in the cloud</td></tr>
<tr><td>Likelihood: Medium</td><td>Impact: Critical</td><td>Exposure level: Medium</td></tr>
<tr><td colspan="3"><u>Impact</u>:
Sensitive data may be lost due to accidents or attacks when stored by third-party cloud service providers, introducing IoT applications into the automotive domain allows for large-scale data gathering and “Big Data” analysis. Losing part of the collected data is an issue that can result in financial consequences, and consequently, loss of trust with customers. Losing all of the data will result in the inoperability of the service.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Risk/Threat #2:</b> Loss from DRM (Digital Rights Management) conflicts</td></tr>
<tr><td>Likelihood: Low</td><td>Impact: Marginal</td><td>Exposure level: Low</td></tr>
<tr><td colspan="3"><u>Impact:</u>
DRM technologies try to control the use, modification, and distribution of copyrighted works, as well as systems within devices that enforce these policies. User data, traffic or travel related services, audio and video entertainment (etc.) may be deleted due to DRM issues, if not correctly implemented. A third party attacker can modify DRM to make the data collected unavailable.</td></tr>
</table>

Risk/Threat #3: Replay of commands

Likelihood: Low	Impact: Uncontrollable	Exposure level: Medium

<u>Impact:</u>

If internal networks are not adequately protected against replay attacks, attackers could have potential access to a range of functionality that can influence vehicle control. This can have detrimental consequences if the control such as steering, braking, acceleration can be maliciously influenced remotely. This can cause a significantly poor image to the company and in a more extreme case, human casualties.

Risk/Threat #4: Man in the middle

Likelihood: Medium	Impact: Critical	Exposure level: Medium

<u>Impact:</u>

A variety of interfaces means that, with poor protection of the session, there are a lot of ways to perform MITM attacks for different purposes:

- Impersonating a service provider, or an app store, may cause financial abuse.
- Impersonating backend systems can result in attacker downloading a rogue firmware on the vehicle.
- Impersonating the vehicle on a V2X communication can result in fake messages and fake results obtained in the data computation.
- Potential risks to privacy:
    - Location tracking based on GPS position.
    - Identification of individuals and their behaviour.

Risk/Threat #5: APK reverse engineering and code vulnerabilities

Likelihood: High	Impact: Critical	Exposure level: High

Impact: The code of the applications can be obtained by reverse engineering and investigated later to find code vulnerabilities that can result in a range of possible attacks, for eavesdropping or executing application functions without permission of the user.

Risk/Threat #6: Denial of Service (DoS) and Distributed Denial of Service (DDoS)		
Likelihood: High	Impact: Critical - Uncontrollable	Exposure level: High
Impact: This attack consists of sending vast amounts of messages to the victim in order to block its connectivity and saturate the underlying hardware resources. There are several possible targets: • The IoT Cloud Platform: legitimate smart-objects will not be able to get connected. The final services built on top of the platform may become unavailable. • An infrastructure smart-object: depending on the victim the consequences will go from a loss of information (e.g. vehicle detector) to the service outage. • If the architecture of the internal vehicle networks is not correctly designed, the attack may affect the own vehicle functions. In a DDoS, the severity and complexity are even higher since multiple attackers collaborate together.		

Risk/Threat #7: Malware infection		
Likelihood: Medium	Impact: Uncontrollable	Exposure level: Medium
Impact: The IoT device installs malware software during an Over-The-Air (OTA) update. As it happens with risk #3, this attack may suppose getting access to multiple functionalities probably affecting the vehicle performance.		

4.4.4.2 . Mitigations and security mechanisms

Within the data processing systems technical standards for cybersecurity have to be considered State-of-the-art technical security measures should be implemented such as:

- Access control and authentication
- Password rules for use of secure passwords
- Logging and monitoring
- Security for databases, servers and workstations
- Use of encryption solutions for specific files and pseudonymisation techniques
- Fixed security settings for workstations
- Use of constantly updated antivirus applications
- Firewalls which are properly configured and using the latest software
- Network and communication security
- Use of cryptographic protocols
- Controlled access to wireless network only for specific users
- Monitoring of traffic inbound and outbound, controlled through Firewalls
- Mobile device security
- Implementation of rules for proper use of mobile devices and roles and responsibilities for device management
- Use of encryption software and theft protection
- Application lifecycle security process
- Early definition of specific security requirements
- Use of secure coding standards
- Implementation of testing procedures
- Rules and strategy for data deletion and disposal
- Data deletion process of outdated and irrelevant personal data should be established, additional physical destruction of media (CDs) if needed

Besides the previous security mechanisms, we can identify the next linked mitigations regarding the threats related with IoT exposed previously.

Risk/Threat #1: Loss of information in the cloud
Mitigation action: As the cloud service is maybe provided by a third-party, there are measures to take to avoid the potential loss of data in cloud. In order to mitigate the potential loss, frequent periodic backups are encouraged to prevent significant loss and only lose the data collected since the last backup point.

Risk/Threat #2: Loss from DRM (Digital Rights Management) conflicts

Mitigation action:

Implementing DRM only in data that has sensitive copyright properties, this is essential to avoid the access of DRM files and prevent data being copied or modified.

Risk/Threat #3: Replay of commands

Mitigation action:

The application only needs to know the necessary commands, for example, if the application needs to know the interaction between the driver and the brake pedal, the application should only need to collect relate to the pressure applied pedal and the influence that has on the vehicle speed. The application should not expose information relating to how the braking functionality is performed. Limiting application knowledge relating to vehicle control is necessary. By adding IDS (Intrusion Detection System) to the system, it can be considered to prevent replay attacks; it is also considered a way to mitigate the chance of being attacked.

Risk/Threat #4: Man in the middle

Mitigation action:

By implementing encryption to the communication exchanges, software/firmware validation, firewalls and digital signatures this can contribute to system protection against MITM attacks. These methods make it challenging to an attacker to obtain the data in transmit and prevent the injection of false messages by an unauthorized body.

Risk/Threat #5: APK reverse engineering and code vulnerabilities

Mitigation action:

To prevent an attacker from finding backdoors into the application, it is important obscure information relating to critical functionality before uploading to the app store. Security vulnerabilities can be prevented by following a strict code review process, testing buffer under/overflow and following design rules for safety-critical embedded software, such as MISRA C.

Risk/Threat #6: Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Mitigation action:

- The system should be able to switch the communication channel or transceiver in case of a DoS attack.
- Active monitoring of network conditions to early detect DoS attacks.
- The use of blacklists.

Risk/Threat #7: Malware infection

Mitigation action:

OTA mechanism is a double-edged sword since, on one hand, it is a powerful mechanism to solve zero-day vulnerabilities. On the other hand, it exposes an entry point that may allow an attacker to gain almost full control over the target system. Mitigation actions need to cover at least the following aspects: use of secure protocols to transmit the update, implementation of authentication and authorization mechanisms, cryptographic validation of update manifests and signed code images.

4.4.4.3 Internal responsibility

In the current climate, personal data is highly valued and could have large consequences. Allen & Overy (2017)[93] point out that 60% of the data-security breaches in 2015 came from within the company. Additionally, sloppy follow through of data-protection policies and procedures could lead to data security being compromised.

IoT sensors will allow wider and more detailed perception of the environment making it more efficient to assess responsibilities in case of incidents, but the leakage of this type of information can suppose a break on the privacy and can contain sensitive information for of the system or driver, as personal data. In any event, car manufacturers will have to have robust and secure software in their vehicles from the start. Network providers must have measures in place to detect, and if it is possible counter hacking attempts, as we provide examples in this chapter. Data security compromises in an IoT system of AD could have consequences ranging from privacy infringement to loss of life.

At the end, the provider of the data bases and the developed systems is responsible of maintain the privacy and security required and acknowledge any user of the data being transmitted, also the user should agree on the data usage. In case of an issue on security happen, the responsible of the systems should have a process to react to any unexpected security problem.

4.4.4.4 React methodologies

The system should include mitigation methodologies to ensure integrity, reliability, availability and confidentiality. The cybersecurity concept provides the process to analyse risks, discover threats and find possible mitigation against the known threats. The mitigations themselves provide the first react methodologies.

These react methodologies are linked to a known threat but there are other undiscovered risks or threats. For this reason, is important to have a security management system which permits to log information about the communication, interactions and events in the system. Security information and event management systems in IT allow the real-time monitoring and analysis of security alerts when an attack is detected. The possibilities of this type of systems are:

- **Data aggregation**: The information of the communications, interactions and events permits aggregating the data from different sources or devices. In a deep analysis of the data is possible to make a traceability of the attack, from the point of intrusion to the affected devices.

- **Data correlation**: There are multiple techniques that permits to identify possible issues in the system, event based, rules based, anomaly based, and risk based are the most used ones.

- **Data normalization**: cross-referencing data to remove redundancy, repetition and untypical elements.

- **Alerting:** Notify the issue once it is detected and start the mitigation process. The alerts have different priorities and these priorities have relation according to the severity of the detected attack. The alerting system is based in a set of alert rules which has in consideration if there are threat indicators present.

- **Control panel:** Permits to control the events and issues reported in the system.

- **Forensic analysis:** In case of being affected by an attack, this type of tools permits to re-build the action plan of the attacker and identify the traceability of the attack. The logs help in the actions of the cybersecurity experts during the forensic analysis. The types of forensic analysis are[94]:

  - **Digital forensics**: consists on obtaining the data evidences from the computer or devices. The techniques include the identification of information, preservation, data recovery…

- **Software forensics**: The software forensics determines whether software has been stolen. This is based in the comparison between the source code and check any possible change.

- **Memory forensics**: As many complex attacks also has in consideration to erase data from the hard disk, this technique searches in the computer memory for possible clue about the attack.

We can find analogous system for the security event management in IT, called SIEM.

SIEM means Security Information and Event Management[95]. The SIEM systems include a set of tools for the IT security management. The use of a SIEM provides the global security view of the whole organization. Companies often are composed by some business units. The SIEM includes them into a unique global vision helping to know the IT security state of the organization. The SIEM system often includes the centralization of the log storage and log analysis. Also, it includes a real time analysis. The real time analysis improves the reaction time in case of attack. The SIEM system helps the administrators to be compliance in the GDPR regulation.

The SIEM systems are based in the data acquisition from client devices, antivirus, firewalls, IDSs, etc. All the acquired data is sent to the central administration system where is possible to identify the unusual events. The most important is to create an accurate event profile of the system to avoid possible errors in the event categorization.

The SIEM basics are the set of rules or statistical correlation engine which is able of create a relation establishment between the event log.

Usually, the deployment of these SIEM systems is expensive and is often adopted by big organizations. Other companies also consider the benefits of the SIEM systems and they consider the use of a SIEM service provider.

It is possible to see the correlation of the mechanisms from previous chapter “React methodologies” in the SIEM systems. Basically, the SIEM system includes part or all of them in a unified tool to build a robust analysis system of the security state of the organization.

Similar approach can be applied in automotive sector, despite SIEM systems are developed to provide a security monitoring process inside a company, something also required for the cybersecurity of a product, vehicles should apply a system to monitor and report issues on their internal communications, then we will be able to react to new vulnerabilities and new types of attacks performed in vehicles and have logs for the times when attacks happens.

4.4.5 GDPR and Cybersecurity

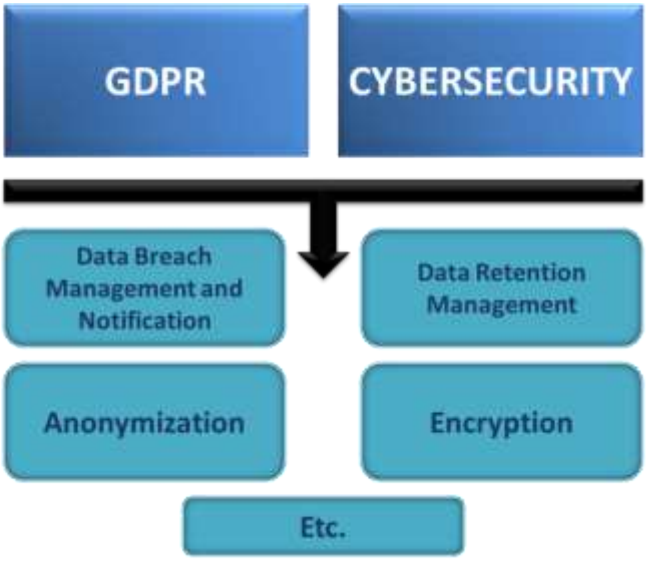

GDPR
CYBERSECURITY
Data Breach Management and Notification
Data Retention Management
Anonymization
Encryption
Etc.

Figure 11 GDPR and Cybersecurity [Colin & Partner Srl]

4.4.5.1 GDPR compliance

Besides technical specifications, compliance with the General Data Protection Regulation2 (GDPR) is something to take into account. This regulation entered into force the 25th May 2018 and it aims to harmonise data privacy laws across all European member states. GDPR repeals the previous directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4.4.5.2 Data-related risks

Service providers shall be aware that they are receiving ‘personal data’ from users and they have to comply with GDPR.

Users may not be yet prepared to share these data, since they are aware of the possible privacy implications. Transmitting and receiving capabilities of vehicle and surrounds means information that maybe will be public.

Users need to be aware of the types of data collected, the recipients, how these are processed and for what purpose. This awareness is needed to establish user consent, which is a tricky question in general. In effect, users will become continuous broadcasters. They must be fully aware of the scope of the processing.

Article 7 of the EU GDPR explicitly states that the controller has to be able to demonstrate a legal basis such as users consent in terms of processing their personal data. Also, data subjects have the choice to exercise their rights to withdraw their consent, to rectification and erasure of their personal data.

Pilot sites should explicitly be able to demonstrate users’ consent, when user data is collected as legal basis, in terms of processing their personal data. Control of personal data can be ensured through a number of tools for informed consent.

Messages can be received by an unrestricted number of entities, whose intentions and technological capacity cannot be known to the sender. Thus, control of personal data is imperative.

Last, the amount of data collected may be used for business exploitation. This opens questions on the free flow of non-personal data (either technical or anonymized) and the question of data access and data ownership. This area is not yet sufficiently legislated to make a definitive judgment of what will happen.

Next steps for data protection can be summarized as follows:

4.4.5.2.1 Legal

The regulations on e-Privacy and Free Flow of Data, once adopted, will provide more depth to the legal development.

4.4.5.2.2 Political

A fundamental decision on data ownership and consent for processing will be crucial. Given the lack of awareness by end users in this regard, this is likely to be top-down. If car data is understood to be personal data and consent as currently exercised found to be invalid, then political initiatives are needed.

4.4.5.2.3 Practical

It is crucial to determine the role and the responsibilities of each partner involved in the application of the GDPR. New regulation introduces changes in relation to duties and rights.

4.4.5.3 Cybersecurity (GDPR)

From the data point of view, the security is a top layer that protects it from external entities. However, the legitimate communicating entities may also make a bad use of it. The new GDPR regulations tries to protect this data and this section provides the technical steps.

4.4.5.3.1 Principles of processing personal data outlined in Article 5 of the GDPR

According to Article 5 of the GDPR, the following are the principles of processing personal data:

- *Purpose limitation:* The purpose of the data collected. Specify the exact purpose and assessing which data is necessary.
- *Data minimisation:* The main aim of data minimisation is guaranteeing that data only will be asked when adequate, relevant and necessary for the purpose.
- *Accuracy*: Delete the information once processed, since is possible want to keep the information for a long time, in this situation, the personal identifiers should be removed, making the identification of the Data Subject impossible.
- *Storage limitation:* Depending on the legal basis of processing data may also have to be stored for limited time periods for liability reasons
- *Integrity and confidentiality*: Personal data should be used according to technical and organisational measures, such as: protection against unauthorised processing and against disclosure, accidental loss, destruction or damage

In addition to the General Data Protection Regulation, the EU also applies sectorial data protection legislation-2002/58/EC 'concerning the processing of personal data and the protection of privacy in the electronic communication sector', also known as 'Privacy and Electronic Communication Directive or 'ePrivacy Directive'. The current directive strongly focusses on obligations for providers of electronic communication services.

5 Conclusion

We acknowledge the technical achievements and results of AUTOPILOT and thus the fact that IoT can improve the automated driving experience. The legal aspects of IoT enhanced automated driving increase the complexity of IoT along with the increasing complexity of the technical landscape of automated driving. This is the reason why we herewith make recommendations in order to facilitate the further implementation of IoT to enhance AD.

From the regulation of automated vehicle and IoT technologies point of view, the adaptive strategy adopted by UNECE and WP.29 is an appropriate method. It is recommended to use a flexible regime to permit improvements once developments have been made, while maintaining enough stability to provide public confidence in the safety and utility of the technology.

Out of this research and assessment, we recommend as further research topic the AI-dilemma where the software could evolve in a non-controlled manner and therefore safeguards need to be put in place to prevent problems and answer the causality effect in liability

The liability concept is at the heart of the potential legal issues of AD and IoT, and regulation should help increase clarity in this area. As soon as, by default, the vehicle is in an automated mode, the liability lies at the vehicle provider side, as first line. A liability tree is based on the causality link starting with the automated vehicle and including all elements ("trunk" and "branches") helping to improve the safety. The safety improvement lies at the liability principle and may therefore include the connectivity provision towards the different elements helping improve and make trustworthy the safety at the end. The Product Liability Directive contributes to this clarity and may be extended to services and even data if these become integral part of the safety-guarantee chain of automation. In other words, if these services or data providers prove to be liable by increasing the safety of the automated drive and minimising the collision risk while driving, they will increase the trust and thus acceptability of the users. If they commit less to this safety enhancing, the value will be questioned and may therefore request to go through service- or data-cleansing before arriving to the safety system.

We introduce the concept of data segmentation making a clear distinction between safety-critical data segment, recommended as liable data, with other data segments which enhance comfort of the automated drive or inform the user or even entertain him.

In liability, we showed there are three elements which are the damage, the event giving rise of the damage and the causal link between them. To help to follow-up the causality link between event and damage and at least to further improve the quality of the driving experience, we recommend the usage of data recorders. This kind of device help reproduce the situations during which events can take place. As it is already part of a regulatory process, as project recommendation we further insist towards regulators on the clarification and standardisation of their use especially in a geographical zone which is the range of an automated vehicle like Europe where currently many different local regulations co-exist. This harmonisation is of highest interest to increase the usage of automated driving. Most importantly, this shall increase the trust of the road users in general which is not a trivial aspect.

The certification process, also introduced in some countries as the “vehicle driving license”, is also very important to verify the compliance to minimum requirements. At the same time, it shall not be intended to escape liability for the automated vehicle system, provided by a vehicle manufacturer due to a regulatory compliance. The regulatory aspect of this certification process is recommended to be extended towards the 3 pillars described in the document.

As further recommendation, the privacy and (cyber-)security shall be embedded by default in the automated driving system with mention of clear purpose to comply with the current regulation and enhance the trust in the system. The current state-of-the-Art techniques have been employed and demonstrated during the piloting in AUTOPILOT.

6 Annexes

6.1 Annex 1 – Internal survey of AUTOPILOT beneficiaries

This internal survey was aiming to collect knowledge from AUTOPILOT partner beneficiaries on legal perspectives related to the use of the Internet of Things (IoT) for Automated Driving (AD). The survey was conducted by ERTICO – ITS EUROPE during June 12th to July 9th 2018.

All the questions in this survey pertain to the context of using IoT for AD and focus on regulation, liability, privacy and cybersecurity in this area. The automation level implied in this survey is towards the higher end - at least L3 and above, with the driver being non-active.

A total of 30 respondents answered this survey.

Q1. Your sector (choose from only one)

a. Automotive
b. IoT
c. Service providers
d. Research
e. Public authorities
f. Users
g. Other (please specify)

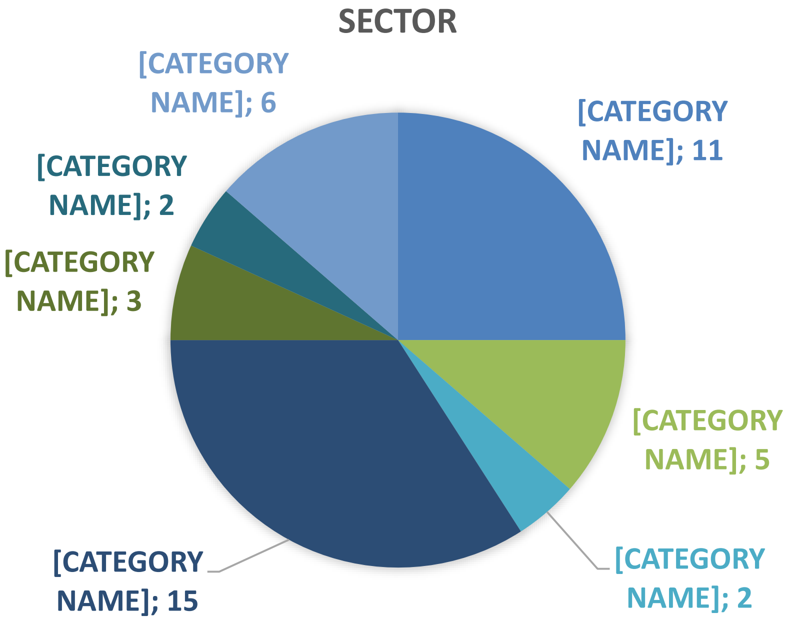


Figure 12 Respondents sector

Most of the respondents were from "**Research**" sector, followed by "**Automotive**" sector and by "**IoT**" sector.

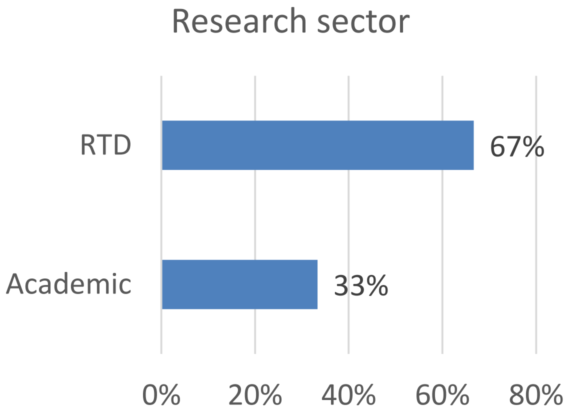


Figure 13 Respondents from research sector

"**Research**" sector is mostly represented by RTD sub-sector, then by Academic sub-sector.

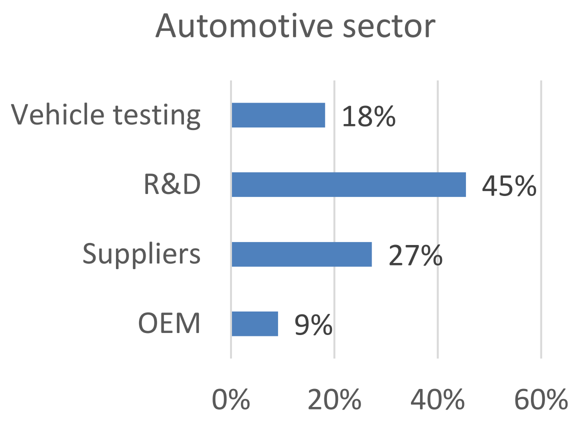


Figure 14 Respondents from automotive sector

"**Automotive**" sector is mostly represented by R&D sub-sector and by the suppliers sub-sector.

"**IoT**" sector is largely represented by Telecoms, followed equally by IT solutions and electronics. Finally, other sectors were represented, by several sub-sectors:

- Ministry
- Government body
- Private road operator
- Legal
- Transport research
- Transport Industry

Q2. How well are you acquainted with national and international regulatory matters in this area?

a. 1-Not at all familiar
b. 2-Not familiar
c. 3-Not familiar
d. 4-Average familiar
e. 5-Familiar
f. 6-Familiar
g. 7-Very familiar

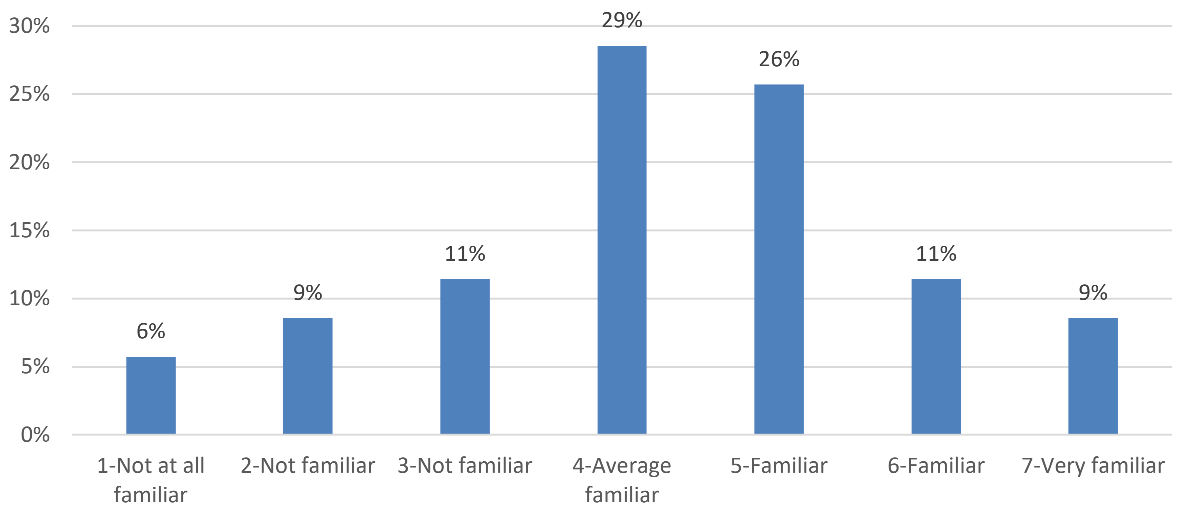
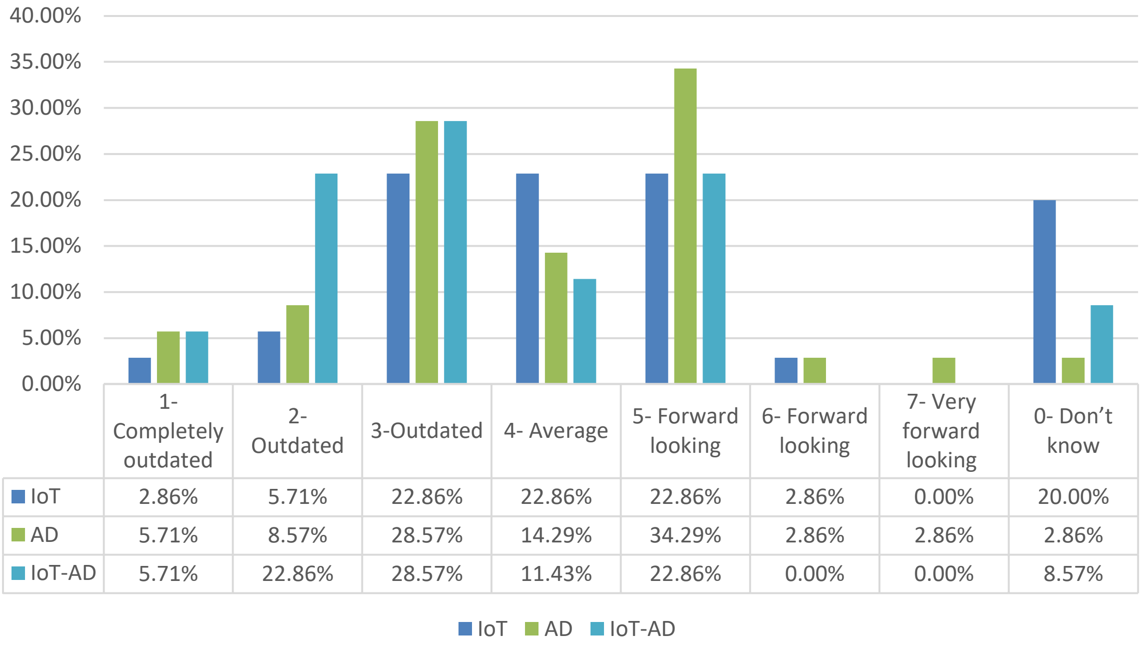


Figure 15 Acquaintance with national and international regulatory matters

Respondents were averagely familiar to familiar with acquaintance with national and international regulatory matters in the area of legal issues applied to IoT-based AD.

Q3. How well do you believe that EU regulation is keeping pace with technological developments?

- **a.** 0- Don't know
- **b.** 1- Completely outdated
- **c.** 2- Outdated
- **d.** 3- Outdated
- **e.** 4- Average
- **f.** 5- Forward looking
- **g.** 6- Forward looking
- **h.** 7- Very forward looking



	1- Completely outdated	2- Outdated	3-Outdated	4- Average	5- Forward looking	6- Forward looking	7- Very forward looking	0- Don’t know
IoT	2.86%	5.71%	22.86%	22.86%	22.86%	2.86%	0.00%	20.00%
AD	5.71%	8.57%	28.57%	14.29%	34.29%	2.86%	2.86%	2.86%
IoT-AD	5.71%	22.86%	28.57%	11.43%	22.86%	0.00%	0.00%	8.57%

Figure 16 Is EU regulation keeping pace with technological developments

Respondents answered that they believe that EU regulation is averagely keeping pace and is forward looking to IoT, AD and IoT-AD technological developments.

Q4. What area of IoT-AD do you believe needs clear(er) regulation?

a. Open question

Respondents answered that areas of IoT-AD that needs clear(er) regulation are technology, privacy, security, liability, safety and tests.

- **Technology:** Communication channels (spectrum allocation), Cross-border use, standards for interoperability, vehicle data roaming, remote software update, etc.
- **Privacy:** Private data privacy and management, Data access and use, data ownership, etc.
- **Security:** Cybersecurity and responsibility, data security and protection, etc.
- **Liability:** Liability of AD, Liability of services, etc.
- **Safety:** safety of AD, etc.
- **Tests:** Test on road in standard conditions, certification schemes, etc.

Q5. Are you aware of any differences in regulation/legislation between countries (inside or outside EU) that may cause conflict within regulation design?

a. Open question

Respondents answered that differences in regulation/legislation between countries are existing between countries of the EU and between EU and other countries (US, China, etc.). Most significant differences that were highlighted are GDPR, Communication technology (frequencies, protocols), liability in AD.

Q6. In what aspects are standards most needed for or most challenging to the following agents?

a. Automaker

b. Connectivity provider

c. Software developer

d. Other

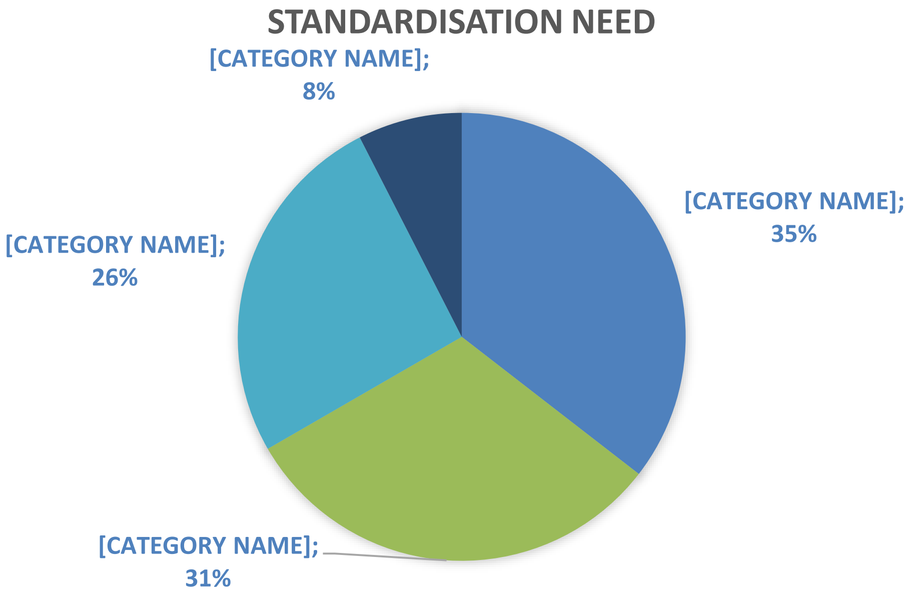


Figure 17 Standardisation need related to different agents

Mostly relevant agents that are expected to bring standardisation are "**Automakers**", followed closely by "**connectivity providers**" then by "**software developers**".

Specific standardisation activities by the three relevant agents are:

- **Automaker:** Security/Privacy, Liability, Regulation, Interoperability.
- **Connectivity provider:** Interoperability, Availability of service/QoS, Security, Liability.
- **Software developer:** Security, HMI (user interface).

Q7. Who should be responsible for conformity with national and international regulation? Choose one sole responsibility or multiple joint responsibility.

a. Automaker

b. Connectivity provider

c. Software developer

d. Other (please specify)

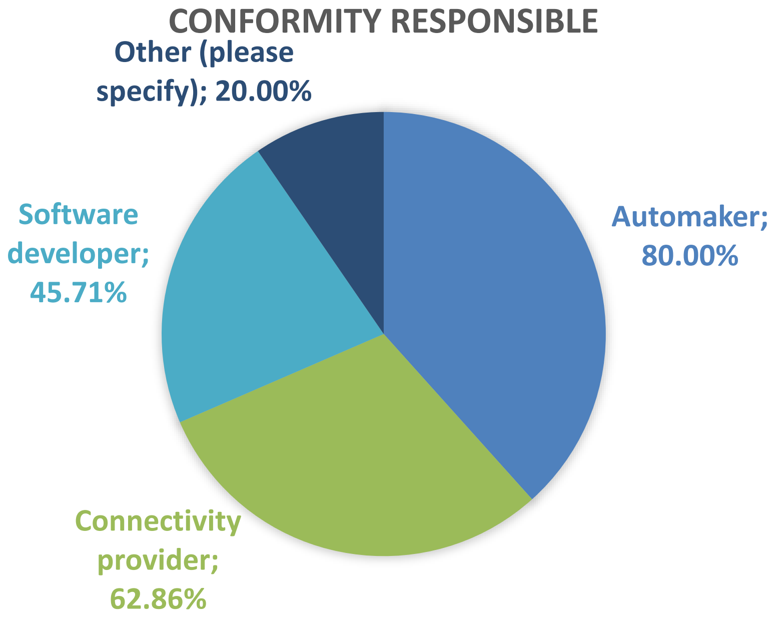


Figure 18 Responsible for conformity with national and international regulation

The designated responsible for conformity with national and international regulation, by the survey respondents, are "**Automakers**" in first position, followed by "**Connectivity providers**", then by "**Software developers**".

Q8. Is net neutrality (connectivity/internet service providers treating all content equally and impartially) important for IoT-based AD?

- **a. Yes**
- **b. No**
- **c. Unsure**

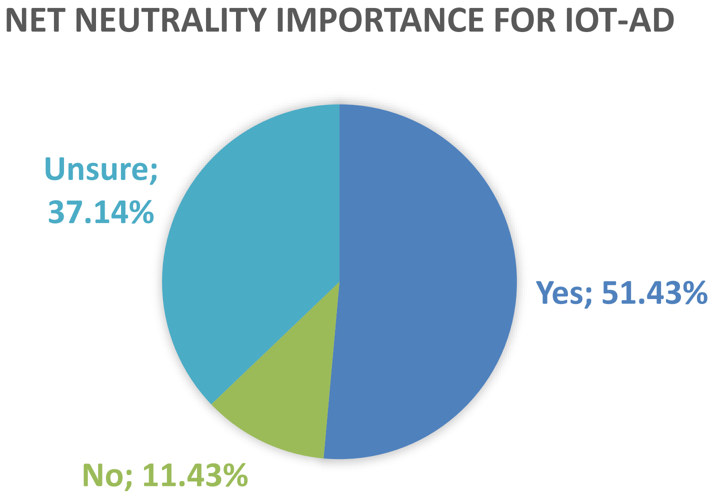


Figure 19 Neutrality importance for IoT-based AD

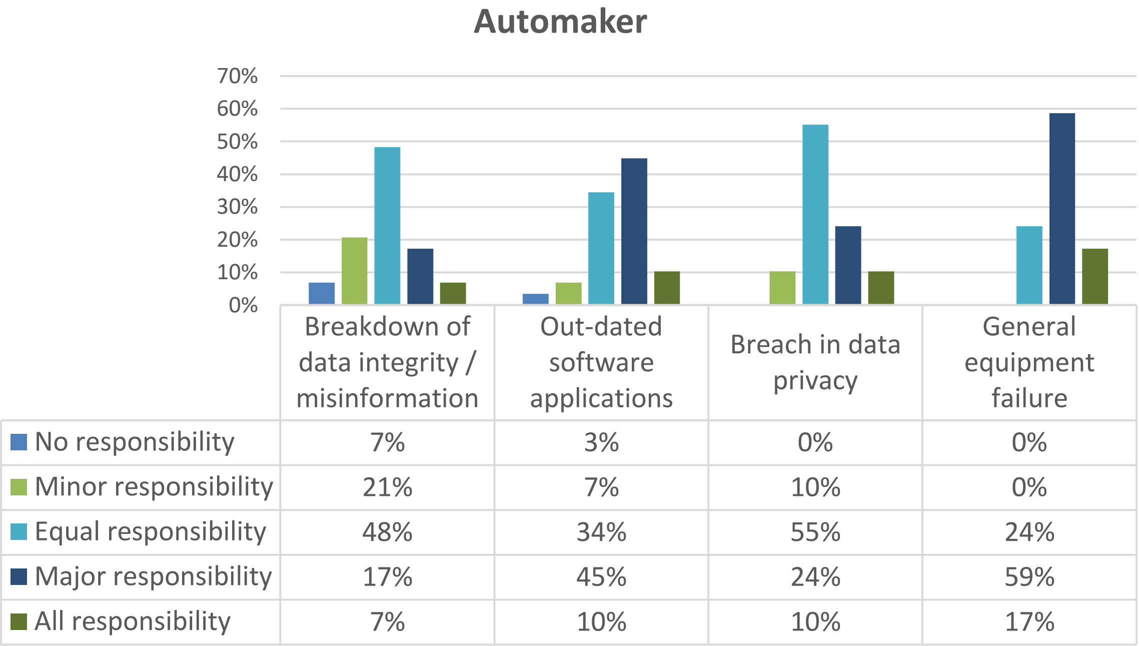
Respondents answered that net neutrality is **very important** for IoT-based AD.

Q9. Who should be liable in the event of an accident due to the following issues?

a. Failure type
   i. Breakdown of data integrity / misinformation
   ii. Out-dated software applications
   iii. Breach in data privacy
   iv. General equipment failure

b. Possibly liable actors
   i. Automaker
   ii. Connectivity provider (MNO)
   iii. Mobility service provider
   iv. Car user/driver

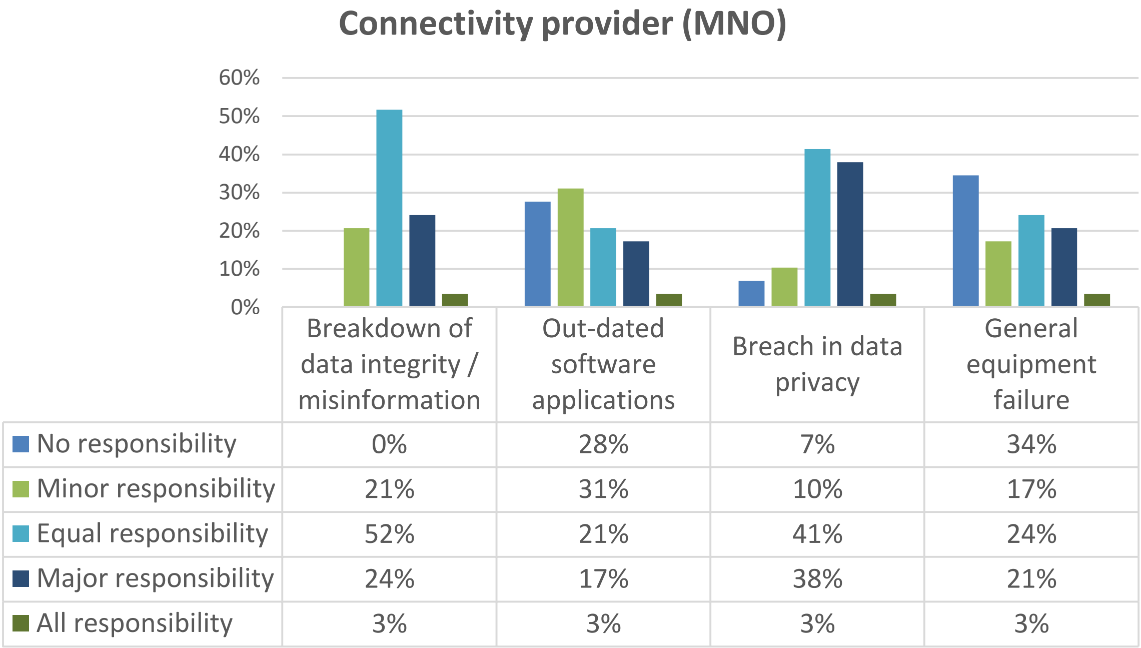
c. Level of responsibility
   i. No responsibility
   ii. Minor responsibility
   iii. Equal responsibility
   iv. Major responsibility
   v. All responsibility



	Breakdown of data integrity / misinformation	Out-dated software applications	Breach in data privacy	General equipment failure
■ No responsibility	7%	3%	0%	0%
■ Minor responsibility	21%	7%	10%	0%
■ Equal responsibility	48%	34%	55%	24%
■ Major responsibility	17%	45%	24%	59%
■ All responsibility	7%	10%	10%	17%

Figure 20 When an Automaker should be liable in the event of an accident

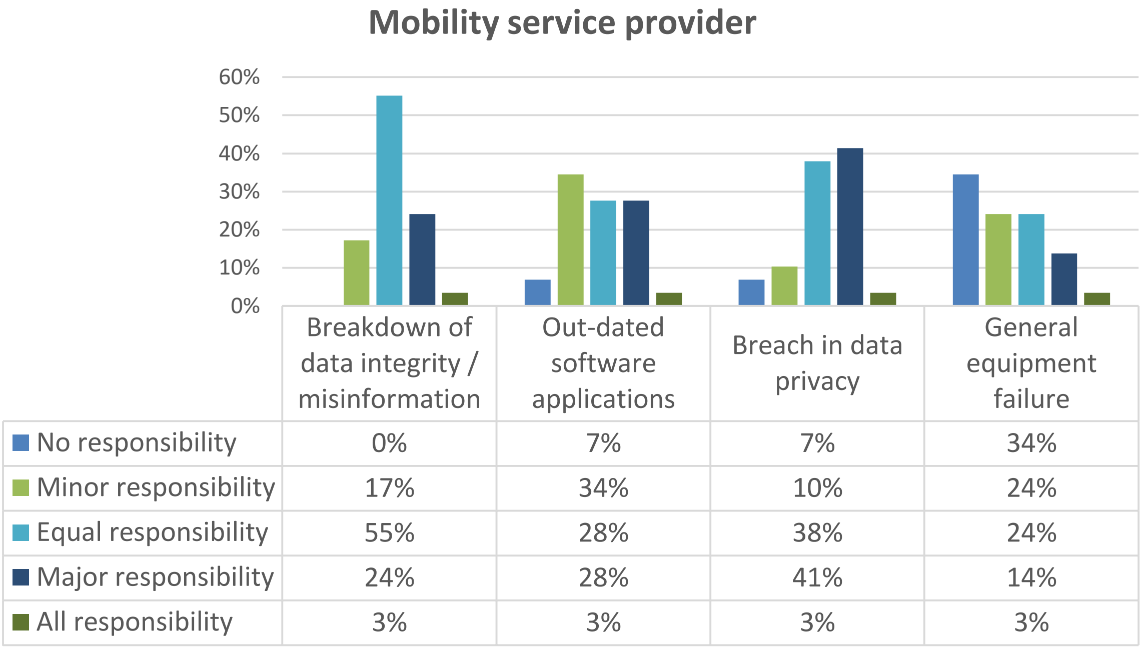
Based on the answers of the respondents, an automaker should be liable with "**a high level of responsibility**" in the event of an accident, mostly in case of "**General equipment failure**", followed equally by "**Out-dated software applications**" and "**Breach in data privacy**".



	Breakdown of data integrity / misinformation	Out-dated software applications	Breach in data privacy	General equipment failure
No responsibility	0%	28%	7%	34%
Minor responsibility	21%	31%	10%	17%
Equal responsibility	52%	21%	41%	24%
Major responsibility	24%	17%	38%	21%
All responsibility	3%	3%	3%	3%

Figure 21 When a Connectivity provider (MNO) should be liable in the event of an accident

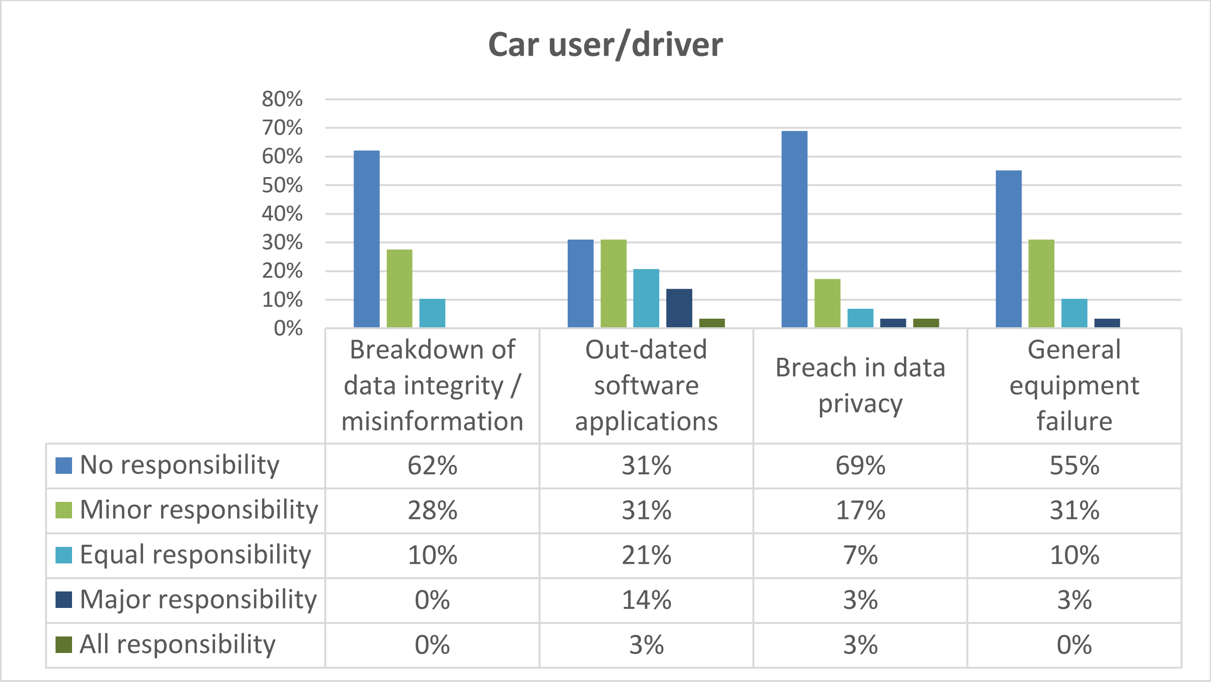
Connectivity provider (MNO) should be liable with an "**Equal responsibility**", based on respondents answers, in the event of an accident, mostly in case of "**Breakdown of data integrity / misinformation**", and followed by "**Breach in data privacy**".



	Breakdown of data integrity / misinformation	Out-dated software applications	Breach in data privacy	General equipment failure
No responsibility	0%	7%	7%	34%
Minor responsibility	17%	34%	10%	24%
Equal responsibility	55%	28%	38%	24%
Major responsibility	24%	28%	41%	14%
All responsibility	3%	3%	3%	3%

Figure 22 When a Mobility service provider should be liable in the event of an accident

Mobility service provider should be liable with an "**Equal responsibility**", based on respondents answers, in the event of an accident, mostly in case of "**Breakdown of data integrity / misinformation**", and followed by "**Breach in data privacy**".



	Breakdown of data integrity / misinformation	Out-dated software applications	Breach in data privacy	General equipment failure
■ No responsibility	62%	31%	69%	55%
■ Minor responsibility	28%	31%	17%	31%
■ Equal responsibility	10%	21%	7%	10%
■ Major responsibility	0%	14%	3%	3%
■ All responsibility	0%	3%	3%	0%

Figure 23 When a Car user/driver should be liable in the event of an accident

Based on respondents’ answers, Car user/driver **should not be liable** in the event of an accident. But, in case where responsibility is to be applied, “**Out-dated software applications**” then “**General equipment failure**”.

Q10. How can IoT help in providing information for attributing liability related to AD?

a. Open question

Data monitoring based on a secured communication from different sources *(Vehicle, road devices – traffic lights, sensors, cameras, etc.-, weather conditions, incidents on the road, traffic information, etc.) could help or improve the attribution process of liability related to AD.*

Q11. What IoT data would need to be accessed for IoT to facilitate liability attribution or apportionment?

a. Open question

The following data should be accessed in order to facilitate the process of attribution or apportionment of liability.

- **Specific vehicle data** *(speed, acceleration, distance, etc.)*
- **All vehicle data**
- **Road data** *(weather, traffic information, road conditions, road events, etc.)*
- **Other** *(DSSA data | data logs | metadata | Information about data trust levels | Who is in charge of what and by whom each product is made. | Identifiers, message checksums & signatures. Transaction-based messages like operations in banking).*

Q12. **With reference to the two previous questions, is there any additional data needed that would not be required for 'normal' operation (i.e. gathered 'just in case')?**

a. **Open question**

The following data should be accessed in order to facilitate the process of attribution or apportionment of liability.

- **Vehicle logs** *(devices logs, leisure services, automation settings, etc.)*
- **Weather information**

Q13. **For how long should the collected data be stored for later analysis?**

a. 6 months - 1 year
b. 1 - 5 years
c. 5 - 10 years
d. More than 10 years
e. Indefinitely

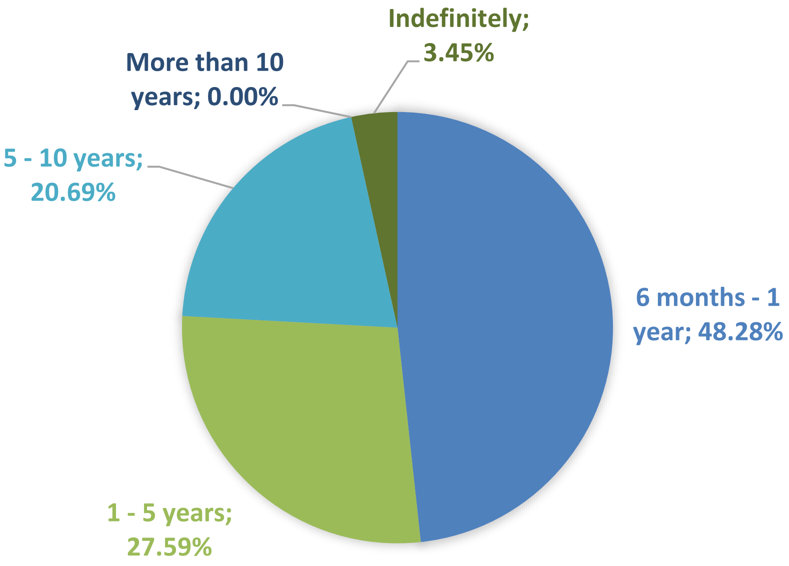


Figure 24 Storage time of collected data

Short periods of time are expected by the participants, where period of 6 months - 1 year of storing collected data is highly represented, followed by period of 1-5 years. Adding that the participants commented to choose as short periods as necessary.

Q14. **What aspects of IoT use are likely to increase or decrease insurance premiums for automated car owners?**

a. Increase premiums
b. Decrease premiums
c. No change

Respondents commented that Dangerous driving behaviour and Global ICT security issues are IoT aspects that are likely leading to insurance premiums increase. While, driving behaviour, Cybersecurity, vehicle maintenance status aspects are possibly leading to decreased insurance premiums. No comments were given for a no change option.

Q15. How could personalised IoT AD applications affect privacy?

a. 1 - Complete loss of privacy
b. 2 - Loss of privacy
c. 3 - Average loss of privacy
d. 4 - Average privacy
e. 5 - Average privacy protection
f. 6 - Privacy is protected
g. 7 - Privacy is completely protected

Respondents answered that privacy could be affected by a loss of privacy in case of collected Data collected, tracking destinations, driving behaviour, driving time, permanent geo-localisation, where/what we are doing, duration of activities, medical problem, etc.

Q16. What data would you be willing to give up to get more personalised IOT-AD service?

a. Open question

Respondents are willing to share their **Geographical data** (location, trip, speed) and **Personal Data** (name, age, driving behaviour, Calendar, Music taste) to get more personalised IoT-AD services.

Q17. What data would you be not willing to give up even to get more personalised IoT-AD service?

a. Open question

Respondents are not willing to share their **Personal data** (home address, name, gender, age, date of birthday, family status, bank data, biometric data, driving behaviour, phone number, email, health status, etc.) and **Location** even to get more personalised IoT-AD service.

Q18. To what extent is data minimisation (processing only data necessary for the specific functions) effective for IoT-AD?

a. Open question

Data minimisation is at least important and regularly very important in a way that it is a GDPR requirement and IoT-AD must respect it in order to increase trust of users.

Q19. What IoT-AD data should be accessible to other parties such as?

a. Police / National security
b. Automakers
c. Connectivity providers
d. Insurance companies

e. Mobility service providers
f. Other automated vehicles

All the choices above are highly represented and willing to share with each actor the following data sets:

a. **Police / National security**
   - **Specific data:** *speed |Emergency situation, Speed/location history. |ID+ Positioning+ Driving parameters (setting, speed...) |driving speed, risky driving behaviour |vehicle registration data |Some |itineraries and trips |traffic conditions |Location tracks, event-based information about accidents |all relevant |all data necessary)*
   - **All data**

b. **Automakers**
   - **Specific data** *(vehicle performance data |diagnostics of lifetime of components without link to the VIN |vehicle data, personal location data |Vehicle status information and information from IoT devices |failures related to driving behaviour |CAM messages and current GPS data |Energy consumption, errors |Car dysfunctions |automation malfunction protocols, accidents protocols |Driving behaviour, fuel consumption |vehicle status data |behaviour of the car |Car performance, driving behaviours |Event data of incidents)*
   - **All data**

c. **Connectivity providers**
   - **Specific data** *(open data |rough location data (cell-based) |IoT logging data |GPS data - vehicle type |Connectivity problems |Data gaps and loses protocols |location |traffic data |information about physical performance of communication link |Elements density, data traffic flow |quality of data transmission with / to the vehicle |Payload type for network QoS and prioritization)*
   - **All data**

d. **Insurance companies**
   - **Specific data** *(open data |CAM messages and current GPS data |Accidents and causes |driving behaviour (but also quite and controversial critical point) |traffic data, vehicle status data, driving styles data |Driving behaviours |liability related data, vehicle safety functionalities data (on/off) |only information about a driving risk, not about exact location and speed |incidents)*

e. **Mobility service providers**
   - **Specific data** *(data needed for performing the mobility services | only information absolutely needed for the service and upon consent of the person involved | open data | Vehicle status information and information from IoT devices | commuter trips | GPS data - vehicle type | depends on need | User needs | all necessary | upon request | as necessary for the purpose | location | routing, driving speeds, traffic signalling | traffic data, traffic conditions | Some | availability of automated car when and where | Location)*

f. **Other automated vehicles**

- **Specific data** *(safety related V2X data | anonymous data that disappears after some seconds | open data | Vehicle status information and information from IoT devices | speed | CAMs and DENEMs | depends on need | Braking manoeuvres, detections | GPS position and short-term trajectory | all traffic relevant data | only safety relevant | in actual traffic situation or anonymised | as necessary for the purpose | location, direction, speed | Incidents, and detected objects for shared world models | Emergency situation, traffic jam, forecast | traffic data, | As much as needed | position of automated vehicles)*

Q20. Is GDPR a barrier or an enabler for developing new data-based IoT-AD applications?

a. 1 – Strong Barrier
b. 2 - Barrier
c. 3 – Average Barrier
d. 4 - Average Enabler
e. 5 - Enabler
f. 6 - Enabler
g. 7 – Complete Enabler

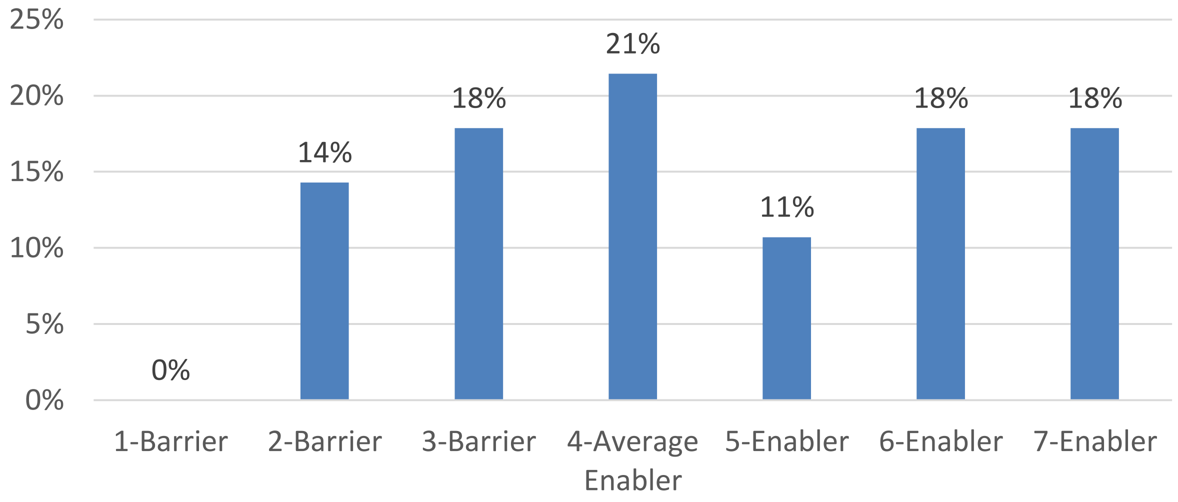


Figure 25 GDPR for data-based IoT-AD applications

The GDPR is seen as an average enabler for the developing of new data-based IoT-AD applications.

Q21. Would the IoT managed system inspire more trust if personal information is segregated – for instance, if anonymous data could be freely shared with many organizations and/or IoT devices but law enforcement authorities (Police/National security) would hold the de-anonymization key?

a. 1-Strongly disagree
b. 2-Disagree
c. 3-Disagree
d. 4-Average Agree

e. 5-Agree
f. 6-Agree
g. 7-Strongly agree

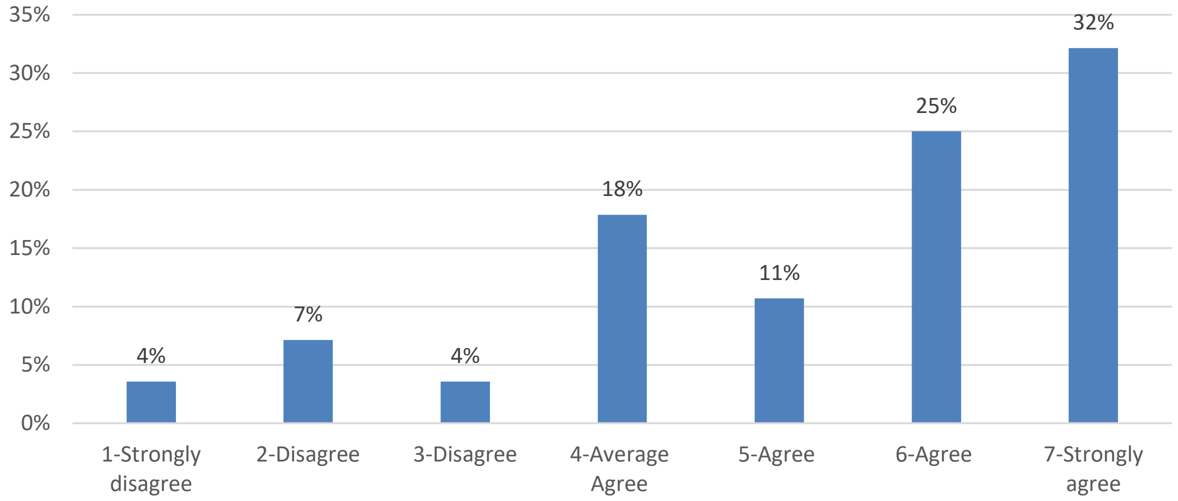


Figure 26 IoT managed system vs Trust of segregated personal information

Respondents are strongly agreeing on the fact that if personal information is segregated, IoT managed system inspire more trust.

Q22. IoT must answer the contrary needs of both data protection and data sharing. Can cloud design for IoT automated driving do justice to both equally in an effective way?

a. Yes
b. No
c. Unsure

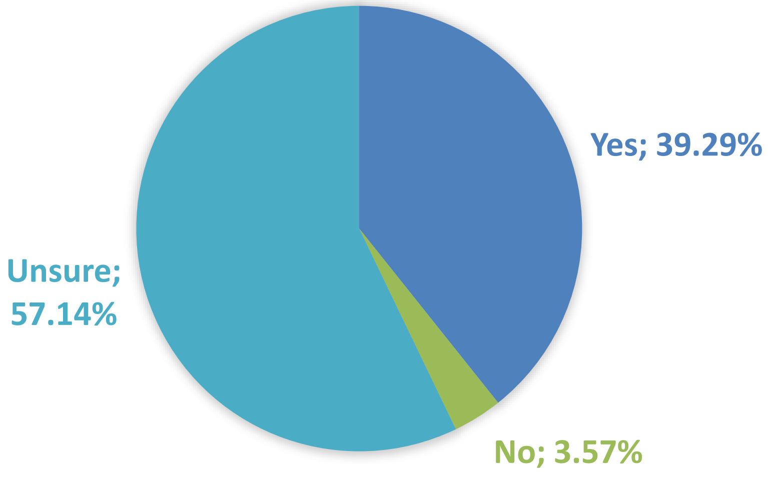


Figure 27 Data protection and data sharing

57% of the respondents were unsure if IoT must answer the contrary needs of both data protection and data sharing. From the respondents that answered "by "Yes" or "No", we clearly identify that cloud design for IoT automated driving can do justice to both equally data protection and data sharing in an effective way.

Q23. What are some of the risks that cloud computing brings to IoT-AD?

a. Open question

Respondents answered that IoT-AD could be affected by the following cloud computing risks:

- **Availability of services and Data,** Quality of Service (QoS) when accessing to services,
- **Confidentiality and integrity of data,**
- **Authentication and access to systems and accounts,**
- **Global security issues** (cyberattacks, hacking, espionage, etc.).

Q24. What is the greatest risk of those mentioned above?

a. Open question

The most significant cloud computing risks that could affect IoT-AD are:

- **Global security issues:** Confidentiality/Integrity, Authentication/Access, Quality of Service (QoS).

Q25. How could these risks be minimised?

a. Open question

Global IoT-AD security issues could be tackled by:

- **Setting and defining dedicated security policies:** Improved data security| regular updates of hard- and software| constant control, constant update of security policies| multiple step authentication. limiting accessibility based on location (i.e. only accessible within range of 5 km.) | By securing the communication between IoT infrastructure and vehicle| regular audits| By data minimisation and data deletion| continuous security update, redundancy| Increasing the security, reducing the data that will be used
- **Implementing robust security mechanisms:** Redundancy |Development of protocols and credibility framework |implementing redundancy |build in trust level mechanisms and traceability |Technology robustness and standardisation |Scalability and data minimization

Q26. Which of the various participants in the IoT for AD system is most vulnerable as an entry point for a cyberattack?

a. Open question

Entities of the system that are mostly vulnerable as entry points to a potential cyberattack of a security breach in the IoT-AD system are listed by priority order as following:

- **User devices,**

- **Vehicle,**
- **Service provider,**
- **Infrastructure,**
- **Global:** all the elements of the system

Q27. What aspects of IoT-AD require more specific cybersecurity than other IoT elements?

a. Open question

In an IoT-AD system cybersecurity implementation, special attention should be paid to the following entities listed from high to low priority:

- **Vehicle,**
- **User,**
- **Infrastructure,**
- **Service provider,**
- **Global:** all the elements of the system.

Q28. In terms of security, how do you view the use of mobile apps for user authentication and access to IoT devices and services? Do you believe they are secure enough?

a. 1- Not at all secure
b. 2- Not secured
c. 3- Averagely unsecured
d. 4- Average secured
e. 5- secure
f. 6- Highly secure
g. 7- Completely secure

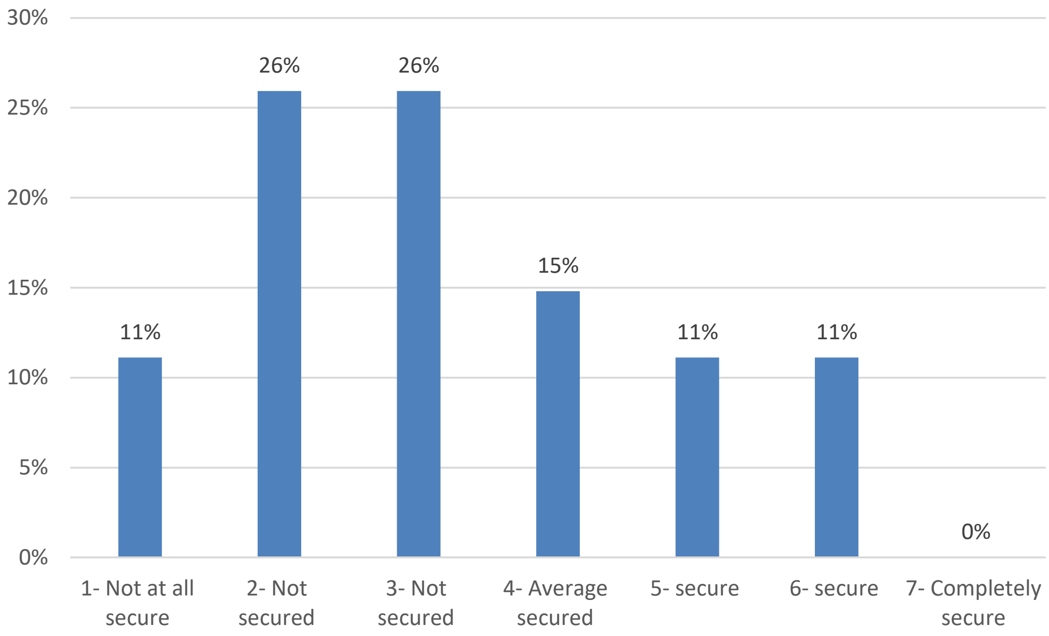


Figure 28 Security related to users' devices and applications

The use of mobile apps for user authentication and access to IoT devices and services are seen by the respondents as not secure.

Q29. With reference to the previous question, what is for you an unacceptable risk?

a. Open question

Based on respondents' answers, unacceptable cybersecurity risks are listed by high to low priority order to:

- Confidentiality/ Integrity
- Authentication
- Vehicle hazardous remote Access
- Service providers
- Users
- Availability/QoS
- Global security issues

Q30. What would you perceive as the main legal risks related to mobile app usage for user authentication and access to IoT devices and services?

a. Open question

The main legal risks related to mobile app usage for user authentication and access to IoT devices and services are seen by the respondents as listed in following by priority from high-low.

- Liability / Regulation
- Authentication
- Confidentiality / Integrity
- Availability

Q31. Any other comments on legal issues regarding using IoT to advance automated driving?

a. Open question

Respondents' advice to Legal issues regarding using IoT to advance automated driving are the improvement of Road safety, Ethics and Liability.

6.2 Annex 2 – User survey

AUTOPILOT legal issues questions from Task 4.6 for user acceptance survey (T4.5)

Q1. IoT-enabled automated driving (AD) adds many benefits (e.g. informed route choice, congestion avoidance, and quick emergency break to avoid collision) as well as complications to the assignation of liability in case of malfunction. If you decide to buy or hire such a vehicle for the first time, would you:

a. Disable the IoT device straightway

b. Like to know more about the safety standards of the IoT technologies before drive off

c. Use the IoT device with no concern as your insurance policy covers liability

Q2. Compared to your mobile phone which provides your location data, do you think that an IoT-enabled vehicle possesses more concerned about security and vulnerability of access to your location data?

a. Yes

b. No

c. I don't know

Q3. (business) When developing IoT technology for AD, which of the following legal issues would your company be most concerned about?

a. Consumer data privacy

b. Cybersecurity attacks

c. Personal injury/property liability

d. Intellectual property protection

e. Warranties

f. Compliance with state and federal regulations

Q4. Who should be legally responsible in the event of a pedestrian being injured during a valet parking manoeuvre?

a. The owner of the vehicle

b. The owner of the parking premises

c. The car maker

d. The software/application provider

Q5. Vehicle-to-vehicle communication can enable safer interaction at intersections, but there is also a complex chain of responsibility (software providers on each vehicle, sensor providers, road authorities, map-makers and communication providers. Who should have legal responsibility if things go wrong in the case of:

a. An advice system — one that gives the driver warning messages?

b. A control system — one that adjusts the approach speed of two or more potentially conflicting vehicles so that they do no collide at an intersection?

Q6. With connection to cloud data, for example to provide weather or traffic information to CAVs, who should have legal responsibility to ensure the accuracy of the information?

a. The information provider if they charge for the information to be used

b. The car maker or their service supplier

c. The cloud service provider

d. No-one

Q7. Would you be willing to provide some personal data (e.g. your address, workplace, commuting patterns) to get more personalised service?

a. No

b. Yes, what data would you be happy to give up?

Q8. If IoT can help in providing information for attributing liability, would you switch on IoT while driving?

a. Yes

b. No, why?

Q9. Would you perceive usage of mobile Apps for user authentication and access to cars as secure enough?

a. Yes

b. No

c. I don't know

Q10. Are you aware about how to react to a cyber-attack if you were in the automated car?

a. Yes

b. No

c. I don't know

Q11. Do you know how protection system from your device works?

a. Yes

b. No

c. I don't know

Q12. AUTOPILOT has a team dedicated to IT and cyber security in order to have always the last version of its App updated and installed. Do you feel safer with a double check control for login to the AUTOPILOT App?

a. Yes

b. No

c. I don't know

Q13. Do you prefer a card to be inserted to access the system instead of giving data by the AUTOPILOT app?

a. Yes

b. No

c. I don't know

Q14. Would you be more willing to share information if your data were anonymized?

a. Yes

b. No

c. I don't know

Q15. Would you trust the system more if personal information is segregated – for instance, if anonymous data could be freely shared with many organization but law enforcement authorities (Police/National security) would hold the de-anonymization key?

a. Yes

b. No

c. Unsure

6.3 References

[1] AUTOPILOT D4.1 Methodology for evaluation: https://autopilot-project.eu/wp-content/uploads/sites/16/2018/10/AUTOPILOT-D4.1-Methodology-for-Evaluation-v1.0.pdf

[2] ibid

[3] ibid

[4] AUTOPILOT D4.9 Preliminary legal perspectives on use of IoT for AD: https://autopilot-project.eu/wp-content/uploads/sites/16/2018/10/AUTOPILOT-D4.9-Preliminary-legal-perspectives-on-the-use-of-IoT-for-AD-v1.0.pdf

[5] AUTOPILOT D4.2 Initial Technical Evaluation: https://autopilot-project.eu/wp-content/uploads/sites/16/2018/10/AUTOPILOT-D4.2-Technical-Evaluation-v2.0docx.pdf

[6] AUTOPILOT D5.4 IoT Policy Framework for autonomous vehicles applications: https://autopilot-project.eu/wp-content/uploads/sites/16/2019/11/AUTOPILOT-D5.4-IoT-Policy-Framework-for-autonomous-vehicles-applications-v1.0-SYSGA.pdf

[7] AUTOPILOT D4.3 Final Technical Evaluation – drafted document

[8] AUTOPILOT D4.5 Business Impact Assessment – drafted document

[9] AUTOPILOT D4.8 User Acceptance Assessment – drafted document

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

[11] 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) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[12] Regulation of the European Parliament and of the Council on type-approval for motor vehicles, 17.05.2018, https://eur-lex.europa.eu/resource.html?uri=cellar:f7e29905-59b7-11e8-ab41-01aa75ed71a1.0003.02/DOC_1&format=PDF, accessed on 25/11/2019;

[13] Status of legislative train on the Regulation of the European Parliament and of the Council on type-approval for motor vehicles, 17.05.2018, https://www.europarl.europa.eu/legislative-train/theme-internal-market-and-consumer-protection-imco/file-general-safety-of-vehicles-and-protection-of-vulnerable-road-users/10-2019, accessed on 25/11/2019;

[14] Krasniqi, X. and J. Hajrizi 2016, *Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles* https://www.sciencedirect.com/science/article/pii/S2405896316325162

[15] Allen & Overy LLP 2017, *Autonomous and connected vehicles: navigating the legal issues* http://www.allenovery.com/SiteCollectionDocuments/Autonomous-and-connected-vehicles.pdf

[16] Foley & Lardner LLP 2017, *Connected Cars & Autonomous Vehicles Survey* https://www.foley.com/files/uploads/2017-Connected-Cars-Survey-Report.pdf

[17] Locomotive Act 1961(UK)

[18] The Locomotives on Highways Act 1861, The Locomotive Act 1865 and the Highways and Locomotives (Amendment) Act 1878 (UK)

[19] House of Commons Hansard, Amendment of the Locomotives Act: Col 1093 (9 July 1878) <https://hansard.parliament.uk/Commons/1878-07-09/debates/15a3acd2-2f6e-49ff-b207-11e7106ad4e8/AmendmentOfLocomotivesActs1861And1865>

[20] William D Eggers, Mike Turley and Pankaj Kishani, 'The future of regulation: Principles for regulating emerging technologies' (2018) Deloitte Insights, a report from the Deloitte Centre for Governmental Insights

[21] William D Eggers, Mike Turley, Pankaj, 'The future of regulation: Principles for regulating emerging technologies' Deloitte Insights (19 June 2018)

[22] 'Uber halts self-driving car tests after death' BBC News (20 March 2018) <https://www.bbc.co.uk/news/business-43459156>

[23] Gill Pratt, Toyota Research Institute, 2017 Consumer Electronics Show Remarks Dr. Gill <https://corporatenews.pressroom.toyota.com/article_display.cfm?article_id=5878>

[24] World Health Organisation <https://www.who.int/en/news-room/fact-sheets/detail/the-top-10-causes-of-death>

[25] European Commission '2017 Road Safety Statistics: What's behind the figures?' European Commission Face Sheet 10 April 2018

[26] Paul Rau, Mikio Yanagisawa, Wassim g. Najm, 'Target Crash Population of Automated Vehicles' (Volpe National Transportation Systems Centre 2015)

[27] Nidhi Kalra and David G Groves, 'The Enemy of Good: Estimating the Cost of Waiting for Nearly Perfect Automated Vehicles' (RAND Corporation 2017)

[28] Lynn M Hulse, Hui Xie, Edwin R Galea, 'Perceptions of autonomous vehicles: Relationship with road users, risk, gender and age' (2018) 102 Safety Science 1

[29] Elina Aittoniemi, Yvonne Barnard, Haibo Chen, David Ertl, Gillian Harrison, & Ors 'User Requirement Analysis' Deliverable 4.7, AUTOPILOT, Grant Agreement 731993

[30] He Michael Jia, Yonggui Wang, Lin Ge, Guichen Shi and Shanji Yao, 'Asymmetric Effects of Regulatory Focus on Expected Desirability and Feasibility of Embracing Self-Service Technologies' (2012) 29(4) Psychology and Marketing 209

[31] Jiun-Shen Chris Lin, Hsing-Chi Chang, 'the role of technology readiness in self service technology acceptance' (2011) 21(4) 424

[32] Paul Pearah, 'Opening the Door to Self-Diving Cars' (2017) 38 High Technology Law 39

[33] Bennear & Wiener 'Adaptive Regulation: Instrument Choice for Policy Learning over Time' Draft working paper (12 February 2019)

[34] Stefan Kuhlmann,Peter Stegmaier, Kornelia Konrad, 'The tentative governance of emerging science and technology- A conceptual introduction' (2019) 48 Research Policy 1091

[35] Hong Jiang, Shukan Zhao, Siwen Zhang, Xiabo Xu, 'The adaptive mechanism between technology standardization and technology development: An empirical Study' (2018) 135 Technological Forecasting and Social Change 241

[36] International Federation of Accountants and Business at OECD, "Regulatory divergence: Costs, risks, impacts," February 2018, p. 4

[37] Nathan Bomey and Thomas Zambito, 'Regulators scramble to stay ahead of self-driving cars' *USA Today* (25 June 2017)

[38] Australian Government Department of Infrastructure and Transport, Regulation Impact Statement for the Harmonisation of the Australian Design Rules

[39] 'Contracting parties' refer to the parties to the 1958, the 1997, and the 1998 Agreements which are:
the 1958 Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts; the 1997 Agreement Concerning the Adoption of Uniform Conditions for Periodical Technical Inspections of Wheeled Vehicles and the Reciprocal Recognition of Such Inspections, and the 1998 Agreement on UN Global Technical Regulations (UNGTRs), see: <http://www.unece.org/trans/main/wp29/publications/other_vehicles.html>

[40] Automated Vehicle Testing Task Force Terms of Reference <https://globalautoregs.com/groups/119-tfav>

[41] Current type-approval of vehicles in Europe, Regulation (EC) No 78/2009 of the European Parliament and of the Council of 14 January 2009 on the type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users, amending Directive 2007/46/EC and repealing Directives 2003/102/EC and 2005/66/EC, https://op.europa.eu/en/publication-detail/-/publication/94ff03fe-2a9f-48e8-9854-f4321b9b39f4/language-en , accessed on 25/11/2019.

[42] Type-approval of vehicles in Europe refers to the national process to certify a vehicle meets all EU

safety and environmental requirements: European Commission- Type Approval of vehicles <https://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/faq-auto_en> last visited 15 September 2019

[43] UNECE 'Proposal for the Future Certification of Automated/Autonomous Driving Systems' (19 November 2018) <https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-13e.pdf>

[44] Informal Document GRVA-02-09 2nd GRVA 28 January – 1 February 2019 <http://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/GRVA-02-09e.pdf>

[45] William D Eggers, Mike Turley, Pankaj, 'The future of regulation: Principles for regulating emerging technologies' *Deloitte Insights* (19 June 2018)

[46] BBC New 5 April 2019 <https://www.bbc.co.uk/news/world-africa-47553174>

[47] BBC News 17 May 2019 < https://www.bbc.co.uk/news/business-48276232>

[48] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Type Approval Requirements for Motor Vehicles' Brussels 17.5.2018 (2018/0145)

[49] European Parliament, 'Type Approval Requirements for Motor Vehicles as Regards General Safety' (Provisional Edition) P8_TAPROV(2019)0391

[50] (Draft) United Nations Draft Agreement Concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles: Uniform provisions concerning the approval of motor vehicles with regard to the DSSAD (November 2019)

[51] AM Ivanov and SS Shadrin 'Development of Autonomous Vehicle Testing System' (2018) IOP Conference Series: Master Science and Engineering 315

[52] ibid

[53] W Damm, S Kemper, E Mohlmann, T Peikenkamp, A Rakow, 'Using Traffic Sequence Charts at the Development of autonomous vehicles' Institute for Information Technology, Germany (2018)

[54] European Transport Safety Council <https://etsc.eu/pinconference2019/>

[55] Ovidiu Vermesan, Roy Bahr, Marcus Mueller, Phillipp Lutz and Ors, 'Report on development and integration of IoT devices into IoT ecosystem' Deliverable 2.4, AUTOPILOT Grant Agreement Number 731933

[56] Yassine Banouar, Marcos Cabeza, Bram van den Ende, Mariano Falcitelli and Ors, 'Pilot Tests Report' Deliverable 3.4 AUTOPILOT Grant Agreement Number 731933

[57] Daniel Altgassen, Yassine Banougar, Marcos Cabeza, Oliver Chalier, Bram van den Ende and Ors, 'Pilot sites test activity report (period 2)' Deliverable 3.5 AUTOPILOT, Grant Agreement 731993

[58] ibid

[59] ibid

[60] "How should autonomous vehicles be programmed? Massive global survey reveals ethics preferences and regional differences." Peter Dizikes, MIT News Office, October 24 2018, <http://news.mit.edu/2018/how-autonomous-vehicles-programmed-1024 > last visited 19 December 2019

[61] Type-approval of vehicles in Europe refers to the national process to certify a vehicle meets all EU safety and environmental requirements: European Commission- Type Approval of vehicles <https://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/faq-auto_en> last visited 15 September 2019

[62] The test cannot proceed unless the RDW has carried out physical tests of the vehicle including on a test track, and stress test where the vehicle is tested in less than ideal conditions, and the relevant road authority has given permission: RDW, 'Assessment Framework, Method and process: connected and/or Automated Driving on Dutch public roads' (2 July 2017)

[63] RDW, 'Assessment Framework Method and Process: Connected and/or Automated Driving on Dutch Public Roads (2 July 2017))

[64] KPMG '2019 Autonomous Vehicles Readiness Index: Assessing countries preparedness for autonomous vehicles' (2019)

<https://home.kpmg/content/dam/kpmg/nl/pdf/2019/sector/autonomous-vehicles-readiness-index-2019.pdf>

[65] Robot Tuner 'Driving License for Autonomous Vehicles (21 March 2018) <https://www.robottuner.com/newsreader/driving-license-for-autonomous-vehicles.html>

[66] RDW, 'Assessment Framework, Method and process: connected and/or Automated Driving on Dutch public roads' (2 July 2017)

[67] C-Roads <https://www.c-roads.eu/platform.html>

[68] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31985L0374

[69] AUTOPILOT D5.4 IoT Policy Framework for autonomous vehicles applications: https://autopilot-project.eu/wp-content/uploads/sites/16/2019/11/AUTOPILOT-D5.4-IoT-Policy-Framework-for-autonomous-vehicles-applications-v1.0-SYSGA.pdf

[70] Economic Commission for Europe, Inland Transport Committee. Convention on Road Traffic. E/CONF.56/16/Rev.1/Amend.1. Art. 8. November 1968, online at: http://www.unece.org/fileadmin/DAM/trans/conventn/crt1968e.pdf, accessed on 25/11/2019.

[71] Product Liability Directive, (EU) 85/374/EEC Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN, accessed on 25/11/2019.

[72] Position Paper of CLEPA on the Product Liability Directive, https://clepa.eu/mediaroom/clepa-position-paper-review-of-product-liability-directive-85-374-eec-pld/ , accessed on 25/11/2019.

[73] Position Paper of BEUC, The European Consumer Organisation, on the Product Liability Directive, https://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf , accessed on 25/11/2019.

[74] Even if it has almost never been investigated and in such way, the driver is in 99% of the cases considered responsible, the cause of an accident could theoretically be the result of a vehicle or of infrastructure failure.

[75] The situation is already complex and can become even more complex in the future. With e.g. leasing, the oxner of the vehicle is not the driver/user of it. Therefore, we use the terminology "vehicle user" for the one who bore the liability of driving, liability which is transferred to the automaker.

[76] The ODD Issue, EUEIP European ITS Platform, Risto Kulmala, Traficon Ltd, <https://connectedautomateddriving.eu/wp-content/uploads/2018/05/Risto-Kulmala_Session-1.3.pdf>, last visited on 19/12/2019.

[77] Autonomous Systems in Aviation: Between Product Liability and Innovation, Ivo Emanuilov, Seventh SESAR Innovation Days, 28th – 30th November 2017

[78] IWG on Data Storage System for Automated Driving / Event Data Recorder (DSSAD/EDR) https://wiki.unece.org/pages/viewpage.action?pageId=87621709

[79] https://ec.europa.eu/transport/road_safety/specialist/knowledge/esave/esafety_measures_known_safety_effects/black_boxes_in_vehicle_data_recorders_en, accessed 21/11/2019.

[80] For compliance with GDPR the PSA process was implemented in DTAG according to the following document: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection/more-transparency.

[81] Data ownership is a sensitive topic and data ownership is claimed by several actors. The topic could be brought to EU Court of Justice who will decide who data belongs to.

[82] Ibid i, AUTOPILOT Evaluation methodology.

[83] Ibid vii, AUTOPILOT Final Technical Evaluation.

[84] ICT-18-2016-Big data PPP: Privacy-preserving big data technologies.

[85] ICT-14-216-2017-Big data PPP: Cross-sectorial and cross-lingual data integration and experimentation.

[86] ICT-15-2016-2017-Big data PPP: Large Scale Pilot actions in sectors best benefitting from data-driven innovation.

[87] These aspects are fulfilled in the PSA implementation, further details see https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection/more-transparency.

[88] Bachlechner, D (lead author) 2018, *D3.1 Overview of Existing Technologies*, e-SIDES: Ethical and Societal Implications of Data Sciences, www.e-sides.eu.

[89] J3061_201601

[90] FERMA standard https://www.ferma.eu/

[91] GRVA-01-17 UNECE https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

[92] AUTOPILOT D1.9 https://autopilot-project.eu/wp-content/uploads/sites/16/2018/10/D1.9-Initial-Specification-of-Security-and-Privacy-for-IoT-enhanced-AD.pdf

[93] Allen & Overy (2017)

[94] Forensic tools https://enterprise.comodo.com/blog/what-is-forensic-analysis/

[95] SIEM https://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781