RedFame

International Journal of Law and Public Administration
Vol. 2, No. 2; December 2019
ISSN 2576-2192 E-ISSN 2576-2184
Published by Redfame Publishing
URL: http://ijlpa.redfame.com

# Regulatory Architecture of Data Processing for Connected and Automated Driving in Europe

Olga Shevchenko

Correspondence: Olga Shevchenko, L.L.M., PhD candidate at Vilnius University, Vilnius, Lithuania.

Received: October 29, 2019 Accepted: November 26, 2019 Online Published: December 1, 2019

doi:10.11114/ijlpa.v2i2.4594 URL: https://doi.org/10.11114/ijlpa.v2i2.4594

**Abstract**

The beginning of the 2020s ought to reflect a steady conclusion of the vast majority of the European Union's projects with regards to the new era of connectivity and mobility within the European Union dimension. We expect Intelligent Connected Vehicles (ICVs) to step into free circulation within the internal market. Since the operation of the ICVs depends on the number of data processing operations, data processing operations should be precisely determined and framed beforehand. ICVs data operations consist of extraordinarily large volumes and velocity of a data flow which previously existed in traditional relational database systems and could not have been processed within the desired timeframe. Even though the currently adopted database systems are ready to face the new level of data processing, a huge data stream is also faced with complex obstacles and new risks which have never been experienced beforehand.

While seeking to ensure safe and secure introduction of a new level of data processing for connectivity and automation at the European Union market, the author precisely examines all potential risks and possibilities of integration into a uniform legal regulation to ensure secured ICVs data processing at all levels. The regulatory framework should document adequate security requirements and defences against ICVs attacks e.g. interference and remote-control interception.

**Keywords:** Intelligent Connected Vehicles (ICVs), interference protection, Vehicle-To-Vehicle (V2V), Vehicle-To-Technologies (V2X), ICV certification

## 1. Introduction

The modern world is faced with a need to collect, store and transmit an endless flow of data properly. Currently, a new stage of development has been reached; the new era of digital technologies, such as Big data, Internet of Things (IoT) and Artificial Intelligence (AI). In different historical periods of the world's evolution, divergent things were considered as valuable as opposed to convergent things. Currently, we consider data as a valuable resource of the modern world. For smooth integration into the new era of Big data, uniform legal regulations should be established. Data regulation is not related to the classic approach of legal regulation. Instead, Big data requires a complex approach including the implementation of an additional range of AI and Informational Technologies (IT) solutions. Big data integration within the current market is not unreachable, therefore considerable responsibility is placed on experts and stakeholders from different fields, (where law-making bodies in cooperation with the legal scholars have to put in additional efforts) not to slow down technological progress. Legal practitioners have always been one step behind in terms of legal supervision of technological development. Big data regulation is one of the examples where urgent legal intervention is necessary.

Even though there is a strong need to provide new legal regulation for a whole Big data block, it is necessary to distinguish data processing regulation for every field which requires an individual approach from data processing for connected and automated mobility in Europe that requires special attention alongside the individual complex approach. The huge volume of data, which will be processed for a connected and automated mobility in Europe, includes not only commercially valuable information, but also personal data of millions of individuals. An enormous data stream will require a complex approach to ensure proper ICVs data processing. Even though data privacy will be analysed within this article, this article will not address the personal data issues in detail. The main focus will be on ICVs data processing for a connected and automated mobility in Europe.

This article *aims* to provide certain legal solutions to uniform legal regulation of the ICVs data processing that will ensure safe and secure ICV applications in Europe. The *research object* of this article ought to be considered as a regulatory scheme addressing secure ICV applications and providing high-level protection against Electronic Control Units (ECUs) errors, remote-control interception and interference at all stages of data processing.

The objective of this article is to examine the proposed security measures for ICVs data processing at the European Union level. In order to achieve this aim, it is necessary to analyse major foreseeable risks that might occur because of ICV data processing. Another issue that ought to be considered is analysis of ICV certification at the EU level, which is one of the most significant issues in ICV data processing security. The data storage platform will also be scrutinized in the course of this research due to its high level of vulnerability based on the volume of data and hypothetical interferences.

Although environmental, energy, public health, risk-reduction and technological issues in ICVs have been thoroughly studied in the past decades, to the best of the author's knowledge, very few papers addressed the regulatory scheme of data processing for connected and automated mobility in Europe. This article claims its relevance to further integration of secure and credible ICV data processing regulation in connected and automated Europe.

In order to achieve the aim of this article, the *logical analysis method* was applied through the prism of evaluation to the proposed security measures for ICVs data processing at the EU level. The *synthesis method* was used to analyse interventions among the different entities, units, stations and network systems which ensure real-time protective vehicle-to-all (V2ALL) communication. The *comparative method* was also applied while collating the range of proposed ICV data processing approaches in Europe and the United States. With a need to acknowledge particular statements related to ICV applications, the *descriptive method* was used.

Regarding the structure of the article, it consists of the legal analysis of the ICV applications and proposed security measures concerning the ICV data processing at the EU level. Section 1 provides an analysis of new level ICV data processing, certain data-related obstacles alongside major risks towards secure automation and connectivity in Europe. Section 2 examines proposed security measures of ICV data processing to protect ICV applications and safer connected mobility in Europe. Section 3 aims to provide a legal analysis of the Data Storage Platform as one of the most vulnerable units of ICV data processing.

## 2. Connected and Automated Mobility in Europe: new Level Data Processing

At the moment, we have approached the beginning of the new era of 5G and smooth progress in robotics, IoT, AI, high-performance computers and powerful networks. The idea of a completely driverless vehicle has been in mind for decades. Whilst Automated Guided Vehicles (AGVs) have successfully proven their efficiency in industries, in terms of the conveyors, cranes, lifts and elevators, there is a real possibility of gaining maximum efficiency out of ICVs in traffic.

Alongside the new possibilities of faster data processing, we expect connected and automated driving in Europe to step into a free circulation at the common market soon. Without a new level data processing, the so-called Big data occurrence at the market, it would not be possible to integrate automated and connected vehicles within the market. It is necessary to precisely assess all potential risks related to data processing for connected and automated driving in Europe once the data processing plays its leading role in the whole integration of automation and connectivity in Europe.

The era of "fifth generation" of telecommunication systems (5G network) certainly brings a range of benefits for automated and connected mobility in Europe. 5G network aims to enable V2ALL communication through high-bandwidth, low-latency and high-reliability links (Community Research and Development Information Service [CORDIS], 2019). Although the European Union law-making institutions have made several significant steps towards the introduction of "fifth generation" of telecommunication systems in Europe, there are still several challenges and obstacles which should be analysed, tested and eliminated prior to the introduction of ICV into free circulation in the common market. At this stage, Europe has launched 3 main projects, namely 5GCroco[1], 5G-Carmen[2] and 5G-Mobix[3], which aim to test and deploy 5G availabilities. These projects will set up 5G trials over more than 1000km of a highway. These areas will cover cross-border corridors and demonstrate connected and automated mobility in Europe.

In case of a poor network connection, the Global Positioning System (GPS) allocated within a connected and automated vehicle might fail to navigate autopilot properly, hence put its' user under the gross jeopardy. Under conditions where GPS must prove flawless in its operation, imperfections such as the possibility of being affected by strong biases due to the atmospheric dissemination delays and multipath should be taken into account (Tao & Bonnifait, 2015). Harsh environmental wireless channel conditions might lead to a lost connection in tunnels, skyscrapers and bridges (Xu et al., 2018). Therefore, connectivity must be secured to create a safe environment for safe ICV application.

Currently, the distribution of a large data flow among heterogeneous entities is available at the new level. It is possible to

[1] 5GCroco will demonstrate public trial of 5G technologies over highways between Metz, Merzig and Luxembourg.

[2] 5G-Carmen aims to reflect public tests across the north-south corridor from Bologna to Munich.

[3] 5G-Mobix aims to demonstrate public trial along two cross-border corridors between Spain and Portugal and the corridor between Greece and Turkey.

ensure in-put and out-put data transmission of vehicle-to-vehicle (V2V), vehicle to the telecommunication infrastructure (V2I), vehicle to other technologies (V2X) and vehicle to others (V2OTHERS). V2V data distribution enables automated and connected vehicles to share safety and control messages between each other, while V2I enables vehicles to collect and transmit relevant data to the infrastructure facilities. V2X enables data distribution between ICV and other technologies that analyse traffic, navigate and calculate further ICV's actions. These applications aim to improve ICV perception of the environment. Even though the EU market claims to be ready for the new era of data processing, discrepancies and uncertainties still exist. As regards the legal regulation of new level data processing, Europe should be ready to face a huge data stream it has never experienced before.

The data processing should be understood as a block of operations, such as data collection, data transmission, data storage, data exchange, data computation and access to data. Even though European Union institutions have already introduced a range of projects[4] towards legal regulation of data processing for connected and automated driving in Europe, there is still a wide berth of legal and technical barriers to a secure and credible new level of data processing. These legal and technical obstacles keep slowing down the process of integration of connected and automated driving in Europe. To step into the new era of mobility and connectivity, first-hand qualitative analysis of all legal aspects of new level data processing for automation and connectivity should be provided.

In the modern world, progress and technical development are always a step ahead of law-making organizations. While the society may await legal integrations in some cases, for an automated Europe, we cannot be one step behind progress. It should be clear that automated and connected vehicles should not enter the internal market without complete and uniform legal control of the new level data processing. Connected and automated driving in Europe should be considered as a new challenge for law-making institutions at both domestic and the European Union levels. It is the time legal practitioners stopped working alone and closely collaborated with the AI and IT experts, telecommunication road infrastructure operators, Software providers and Industry. The era of Big data may only survive under the conditions of close cooperation among experts of different fields. Historically, different manufacturers and stakeholders collaborated for smooth integration of new market solutions. At the end of the day, Industry has always been one step ahead of law-making institutions. In order to match technological progress, law-making bodies should come up with particular resolutions to address ICV data processing a priori.

Currently, the European Commission works closely with both public and private sectors to come up with the most accurate decisions for secure new level data processing in connected and automated Europe. On the 2nd – 3rd April 2019, in the 2nd European Commission Conference on automated driving 'Europe takes the lead' the members of the European Commission discussed new challenges and opportunities in secure data processing and connection V2ALL. It ought to be mentioned that Europe is not yet on track with respect to secure new level data processing, particularly in relation to connected and automated vehicles which are directly related to public security. The European Commission keeps challenging already existing options concerning methods and instruments that might coordinate secure data processing for connected and automated driving in Europe. Although the number of the regulatory options addressing new level data processing was presented in the Conference, neither law-making bodies nor stakeholders were in agreement that the above-stated instruments might be treated as secured and credible enough, thus further research is necessary.

## 3. Major Risks and Gaps in the new Level Data Processing for ICVs

ICVs possess several benefits they ensure a safety level on public roads compared to human-driven conventional vehicles. Whereas a driverless vehicle might eliminate road traffic collisions which occur due to the human error, in urban areas especially, it is necessary to eliminate errors committed by the ICV itself. As far as the legal oversight is concerned, it is important to provide uniform legal regulation over the data processing in Europe prior to the introduction of automated vehicles in the common market. It is inevitable to clearly determine the data processing operations and cover all potential risks which may jeopardise public security. Although not everyone might recognise the whole seriousness of the automation and connectivity at this stage, the attention should be drawn to the public security and the right for privacy at first hand. We should consider entirely all potential risks before letting Europe step ahead with the new era of mobility project.

[4] ADAS&ME project aims to establish the control between the vehicle and the user. ARCADE project aims to help stakeholders to reach a harmonized deployment of CAD in Europe. AutoMate project aims to consider human-ICV interactions. CoEXist project aims to smooth transition towards a shared road network. HEADSTART project aims to determine validation procedures for the purposes of connected and automated driving in Europe, e.g. communication and cyber-security issues. ICT4CART project aims to build a sustainable connection between the ICVs and infrastructure. interACT project aims to ensure a sustainable interaction of ICVs with mixed traffic. LEVITATE project aims to develop an evaluation framework on CAD in Europe.

Both scholars and practitioners keep stating that Variable Speed Limit (VSL) control strategy might have a positive effect on, safety improvement in approximately 50% (Olia, Abdelgawad, Abdulhai & Razavi, 2015), mobility in 30% (Olia et al., 2015), minimizing unnecessary traffic up to 15% (Alessandrini, Campagna, Delle Site, Filippi & Persia, 2015) and on reducing fatal collisions by at least 40% (Alessandrini et al., 2015). However, these advantages and improvements may also bring disadvantages and new risks. Attacks against ECUs have already been experienced in the market. Back in 2015, more than a million vehicles were recalled by Chrysler due to the possibility of interception of a digital system, vehicles were affected by hackable software vulnerability in dashboard computers. Thus extraordinary attention should be paid to high-level data exchange security alongside with integration of protective measures for vehicular ECUs.

Precise attention should be paid to system protection from the *potential terrorist and other massive violent acts*. Bearing in mind the experience of recent years, we should not forget violent acts where vehicles were used as an instrument to cause death of several inhabitants. On the 14th of July 2016 after a Bastille Day fireworks performance in Nice, France, a man having a stroke drove a truck into a crowd and killed 86 people. Later in the same year on the 19th of December, a man drove a truck into a crowd in Berlin, Germany, and killed 12 people who were at a Christmas market. More terrorist attacks were undertaken during 2017 in Spain, Sweden and UK using a conventional vehicle. Although this happened with the conventional vehicle, in case of automation and connective mobility, it would have taken less zeal to commit such a violent act. Therefore, in the era of new technologies, we should not trust classic legal solutions which were helpful in the past.

Besides the risk of the violent attacks, it is necessary to mention the possible risk of *information privacy and data privacy interactions*. Whenever connected mobility is a unitary block of remotely controlled technological operations and data processing, there is always a possibility of a remote-control interception. Therefore, mandatory extra security measures should be integrated at the European Union level. When Europe will be ready to accept the risk for public security in order to ensure smooth integration of research and development into the market, competent law-making institutions should also ensure high level of security at the Union level. This should be done in the same manner as it used to happen in the past, with several regulations and directives that ensured public security, public health and the European Union’s stability alongside smooth integration.

One more separate potential risk to be considered is *hacking and system breakdown for the competitive purposes*. The whole system of connected mobility consists of huge data flow which that be properly distributed and stored at different stages of usage. Therefore, the potential interference opportunities might be expected at any of these stages. Despite a wide range of violent acts and criminal activities, systems breakdowns might also be due to competitive reasons. In tight economic conditions, market Industries are getting more competitive. Speaking of a new product which might be introduced at the internal market shortly, we should also consider the current number of conventional vehicles existing within the EU, which is approximately 218.6 million according to the Eurostat data (Eurostat, 2019). Bearing in mind that automated and connected mobility is highly attractive at the market, the demand is expected to grow rapidly. Hence, we expect enormous competition between manufacturers and ICVs service provides. Historically, intensive competition in the market has raised several antitrust offences, such as formation of cartels in different industrial fields. The recent example of the heavy trucks Industry cartel including MAN, Volvo/Renault, Daimler, Iveco, and DAF who were colluding for 14 years on truck pricing and passing on the costs of compliance with stricter emission rule (European Commission, 2016), reflects the real danger for both private and commercial customers. Therefore, there is always a real possibility of a bad faith competition which might also have its negative effect on the ultimate ICVs user.

Despite the potential risks mentioned beforehand, it is necessary to consider the possibility of a wide range of *crimes* that might appear due to lack of security measures to control and safeguard data processing and address connectivity and mobility. Besides the crimes, *hacking for blackmail purposes* and *espionage* are distinguished as separate gross risks that might pose an absolute danger once the vast majority of conventional vehicles are replaced by automated and connected transport.

Although the mentioned risks consider different illegal aims, there is just only one instrument in force, the so-called illegal remote-control interception or system interference. Although there are various ranges of available protocols for secure and fast data processing, currently none of them suits Level 4 and Level 5 intelligent and connected vehicular digital systems. From 1986, the Controller Area Network (CAN) protocol[5] vehicular hardware communication has deliberately been seeking to ensure a high level of security and sustainability against attackers. To this day, a divergent range of

[5] Controller Area Network (CAN) protocol was developed by BOSCH (Robert Bosch GmbH) and published in 1986 as a *multi-master, message broadcast system that specifies a maximum signalling rate of 1 megabit per second (bps)*”. Steve Corrigan. Introduction to the Controller Area Network (CAN). Application Report SLOA101B – August 2002 – Revised May 2016.

communication networks has been established for the purposes of automated applications, such as LIN (Local Interconnect Network), MOST (Media Oriented Serial Transport), Ethernet, DSRC (Dedicated Short Range Communications) and ITS (Intelligent Transportation Systems), which nonetheless remain vulnerable to attacks (Dibaei et al., 2019). Bearing in mind the need to face extraordinarily large volume of data which should be distributed in a reliable and efficient manner, the Information Centric Networking (ICN), specifically its instantiation Named Data Networking (NDN) was identified as a candidate architecture for future Internet and networking solution for connected vehicles (Amadeo, Campolo & Molinaro, 2016). Even though it might be currently impossible to name the most accurate and reliable system for ICV data processing, it is clear that European law-making institutions should pay special attention to mandatory security measures. Thus, precise and accurate minimum compulsory requirements for uniform security instruments should be established at the EU level.

## 4. ICV Data Processing Regulatory Framework: Minimum Clause Requirements

While seeking to prevent existing potential risks with regards to the data processing, respectful law-making bodies should establish uniform legal requirements in security measures and testing systems for data processing at the EU level. It should be highlighted that each separate data operation ought to be considered individually for security purposes. The European Commission should consider the need to list a block of requirements for the security instruments and tests for each stage of data processing, such as data collection, data transmission, data storage and access to the data. Bearing in mind that different algorithms are integrated for each stage of data processing, law-making institutions in collaboration with the rest of parties that will take an active role in the introduction of the automated and connected mobility in Europe should provide an urgent report.

At the beginning of a new Big data era, it will no longer be possible to establish a well-functioning secured system in isolation, instead, it is time all involved parties cooperated closely. To ensure safe and secure connectivity in Europe both the European Union and domestic law-making bodies are now closely collaborating with (1) Academia, (2) Software providers, (3) Industry, (4) Telecommunication, (5) Infrastructure providers and (6) Operators. Despite collaboration within the domestic Union, external experiences have to be also assessed for the most accurate legal solution. Here, legal solutions from Japan and the United States might have a positive effect in the approach selection at the EU level, even though the Union's legal tradition is rather divergent. Although the European Union's law-making bodies might not adopt an overseas' legal approach without further adjustments, such an approach should be certainly considered. The European Commission has been collaborating with the rest of the world actors that have already made legal, IT and AI solutions for ICV secure data processing and further integration of automation and connectivity (Innamaa, Smith & Uchida, 2017).

Bearing in mind different vehicular models and systems, all existing requirements are established solely by the developers at the local industry level. While the development of requirements for both architectural components and system descriptions is determined by different manufacturers or vehicle domain standards, there is no automatic support and traceability available yet (Rodriguez-Navas, et al., 2014). In the meantime, ICV requires integration of complex and uniform regulatory frameworks that address a specific block of requirements and mandatory standards which should identify essential security elements and components at the EU level instead of the domestic one. However, until qualitative defences against the possible attackers are agreed among the actors, there will be additional obstacles to complete a legal block of security measures at the EU level. At this stage, several IT and AI professionals keep developing defences against a different spectrum of attacks against the intelligent connected vehicular systems, such as cryptography, 3GPP and software (network) security, software vulnerability and malware detection (Dibaei et al., 2019).

The security requirements should be integrated into the minimum clause mandatory legal requirements at the European Union level, either in terms of a separate directive, or amendments to the already existed directives. Both IT and AI professionals are now developing the most accurate security requirements for the purposes of data processing at all levels, such as (a) *authentication and authorization* in terms of identity verification, (b) *integrity* in terms of a data validation, (c) *privacy* in terms of the users security, (d) *availability* in terms of a network real-time support (Dibaei et al., 2019) and (e) *calibration* in terms of secure adjusting.

A. Authentication and Authorization.

The regulatory framework should ensure that either a manufacturer or software and hardware providers have integrated the authentication clause within the security model of the ICV. This ensures every subject who interacts with the system has a valid credential. In the meantime, the authorization stage should ensure that only to the listed users that have the particular permission to access certain operations are allowed to use the system. The parties should guarantee that the access control list remains completely secured and protected from invasion.

B. Integrity.

Validation of data is the process of comparing data with a set of rules or values that seek to ensure accuracy and further data integrity and avoid possible errors. The existence of the errors on the ICV system's application might lead to a gross collapse. Thus, data validation and data integrity that seeks to ensure data accuracy, consistency and further secure ICV usage remains vital.

C. Privacy.

Whereas V2V and V2I enable data distribution among the various stations and entities, private and sensitive data belonging to ICV users might be used for illegal purposes, e.g. tracking, kidnapping and blackmail. Therefore, privacy is another crucial aspect to be secured and enforced by law.

D. Availability.

Real-time availability is a difficult trait to be achieved; however, it out to be attainable to eliminate delays in data distribution. For instance, in the United States, the Federal Communications Commission (FCC) has introduced the IEEE 802.11 (in particular, amendment *p*) MAC layer (Xu et al., 2018) for V2V and V2I data transmission that aims to satisfy a real-time support application. However, MAC is still unable to achieve data distribution within the desired time frame. To ensure real-time data transmission, several connection-free MAC protocols have been proposed, such as Time Division Multiple Access (TDMA), Space Division Multiple Access (SDMA) and Code Division Multiple Access (CDMA) (Xu et al., 2018).

E. Calibration.

Although calibration is complex itself, the process should automatically contain additional security barriers to avoid both data leakage and interception of packages. Besides the autonomous criteria of calibration, it should be impossible to interfere with and intercept. Control interception might result in calibration errors or drift and further failure of ICV.

Notably for these security requirements to reach their approval and complete security status, the European Commission should perform particular steps urgently to determine whether security requirements will go beyond the scope of the Automotive industry regulations and standards. ICV data processing security requirements should be integrated into a separate Directive to ensure smooth application of ICV systems at the EU level. Member states should be strictly prohibited from imposing lower standards of ICV data processing security as it may result in jeopardy of public security. Besides the lower standards ban, the European Union Directive should include strict determinations and instructions for a wider range of security applications. It should lay down within the Directive that member states are not allowed to integrate additional security measures in the event the latter may alter mandatory ICV securities. In case extra securities (1) do not have direct connection with mandatory applications or (2) are well-functioning solitary units operation connected to one or more mandatory securities, such extra security measure should be regarded as approved by the Directive.

Security requirements of mandatory nature should include defences against possible attacks to ensure the high-level protection of ICVs data processing. While considering recent suggestions made for the IT and AI dimension, an additional range of defences should be incorporated into the minimum clause security requirements, such as (a) *cryptography*, (b) *network security*, (c) *software vulnerability detection* and (d) *malware detection* (Dibaei et al., 2019). Speaking of cryptography, it has been an essential defence used to protect valuable data or information for a long time before the introduction of the conventional vehicles. Therefore, new level encryption should be recognized as a secure and protective instrument against attacks. The introduction of the network itself has provided a wide range of opportunities of invasion, hence it remains an attractive target for remote interception of relevant data, information or control. ICV networks consist of internal on-board transceivers and external or the so-called roadside equipment (RSEs), which use DSRC for transmission (Olia et al., 2015). However, wireless transmission should be considered under risk of attack in the context of ICV security, especially in terms of poor wireless links that complicate data delivery. Once the ICV user decides to connect to a wireless device, the vehicle becomes a target itself. Both software vulnerability detection and malware detection should be considered as the most necessary protection for complete security to ensure safe usage of connected and automated vehicles.

## 5. ICV Certification as a Mandatory Requirement at the European Union Level

The higher level of ICV automation is, the lower range of user's involvement in the driving process is. Until now, each driver was obliged to confirm their capacity to drive and make the right decisions at all stages of the driving process. Whilst the driver will no longer be considered as the main actor of the vehicle operation, the burden of confirming the culpability of making right choices while operating a vehicle should be passed to the ICV itself. Therefore, besides the inevitable upcoming changes with respect of the vehicle registration and licensing of the drivers, ICVs certification should be considered as a core aspect towards the ICV introduction at the common market.

Before a conventional vehicle can be granted access to the road traffic, it should prove its conformity with security requirements designed for registration and introduction into the road network. Divergent motor vehicle standards have been available for the decades, however, none of them might be relevant for the upcoming driverless ICV. Besides its obscurity for technical requirements for ICV certification, it also unclear which institution should be responsible for performing the safety certification. For instance, in the United States, most of the certification protocols for conventional vehicles were designed through the prism of self-certification principle, where US manufacturers took control of both safety requirements and safety tests (Cunningham, Regan, Catchpole & Ballingall, 2016). In the ICV world, self-certification should be recognized as inadmissible. Whenever an issue that may certainly endanger human life relates to ICV, a self-certification approach should be abolished. The European Union has suggested a rather divergent approach to conventional vehicles certification, registration and reregistration; in particular Regulation (EC) No 661/2009 addresses type-approval requirements for the general safety of motor vehicles and separate units (European Parliament and the Council, 2009), Directive 2007/46/EC establishes a framework for the approval of motor vehicles and their trailers (European Parliament and the Council, 2007), while Regulation (EC) No 595/2009 regulates type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles and access to vehicle repair and maintenance (European Parliament and the Council, 2009). The Regulation suggests a wide range of safety control measures, such as lane departure warning system, advanced emergency braking system, load-capacity index and tyre pressure monitoring system. The Regulation passes to manufacturers the obligation to ensure those vehicles, systems, components and separate technical units, comply with relevant security requirements including (1) vehicle structure integrity alongside with the impact tests, (2) systems to aid the driver's control of the vehicle, (3) systems to provide the driver with relevant visibility data, (4) lighting systems, (5) vehicle occupant security measures, (6) electromagnetic compatibility, (7) warning devices, (8) heating systems, (9) identification systems, (10) electrical safety and (11) indicators. Despite a wide range of safety requirements laid down within Regulation (EC) No 661/2009 for the purposes of conventional vehicles, these requirements are certainly not able to cover ICVs.

Although safety requirements for conventional vehicles' access to the road network remain debatable, there are no doubts that ICV certification (1) should be done at the European Union level and (2) should be granted mandatory status. Whilst a conventional vehicle should be brought to a certified workshop for periodic safety checks in accordance with Directive 2014/45/EU on periodic roadworthiness tests for motor vehicles, it is questionable how the safety of software updates or modifications will be ensured while ICV keep operating on public roads (European Parliament and the Council, 2014). Regardless of the type of software which will also be consistent with Level 4 and Level 5 ICV, there is always a need to update such software akin to how Microsoft updates on PCs thereby benefiting both consumers and industry. Hence, an additional range of security measures that will be used during the updates should be established. Without certification of software upgrades, there will always be a risk of a negative impact on the safe operation of ICV during an update or after it. Thus, inevitable compulsory monitoring and frequent calibration tests for each ICV within the European Union dimension should be undertaken to ensure the integrity of the ICV software updates (Cunningham et al., 2016).

Whereas ICV might prove its capability of self-diagnosis, certification standards should address the need to undertake additional periodic safety tests in certified workshops. As regards certified workshops, manufacturers might be willing to ensure that these workshops are capable of ICV safety check performance. Once ICV workshops are required by Industry, it would be necessary to have mutual agreements between the manufacturers and the institutions that will be in charge of certification and licensing of ICVs workshops.

ICV certification should be interpreted as a crucial issue that would allow driverless vehicles to enter the road network and ensure a safe plethora of applications with smooth connectivity and mobility in Europe. Therefore, ICV certification should be suitably determined and brought to the European Union level, either in terms of a separate Directive, or amendments to Directives 2007/46/EC and 2014/45/EU alongside with Regulations (EC) No 661/2009 and (EC) No 595/2009 in order to ensure a credible safety approach through the lifecycle of a driverless vehicle.

## 6. Data Storage Platform Towards Protective Intelligent Connected Vehicles (ICVs)

The extreme necessity of introducing a secure data storage approach brings more challenges to the ICV project. Therefore, storage types and storage mechanisms remain core elements in the drive towards automation and connectivity in Europe. At this stage, divergent options which might solve ICV data storage challenge have been presented, such as *on-board storage*, *roadside storage* and *Internet storage* (Xu et al., 2018). However, in the light of a massive data stream, none of the storage solutions has been proven high-level security yet.

An automated and connected vehicle is expected to generate over 0.75 GB – 1 GB of data per second (Bergey, 2018. Therefore, separate platforms intended for data storage might ensure smooth ITS application. Certainly, this enormous volume of data requires a database of a similar capacity. The largest sets of data have been collected from IVBSS, Safety Pilot in the United States and euroFOT, the on-going UNDRIVE in Europe (European Commission, 2017). The Coordination of Automated Road Transport Deployment for Europe (CARTRE) after revising the FOT-Net Data Sharing Framework (DSF) (European Commission, 2017) suggested the tools based on the FOT-Net DSF, e.g. the agreement with data providers and the storage which must ensure protective access to data (Coordination of Automated Road Transport

Deployment for Europe [CARTRE], 2019). Although the database might provide a favourable capacity and velocity for data storage and data distribution, the former must ensure data security beforehand.

Concurrently, the European automotive industry is working on the OSEK/VDX joint project which was established as a real-time operating system. *Real-time operation* challenge has been in the academic circle for decades. Once AGVs were introduced in the common market, both improvements in system performance and minimizing the average response time have been scrutinized. Bearing in mind a large data stream, where decision-making related applications require bigger capacity data access, while critical applications require extraordinarily fast accessibility service, there might be separate data storage platforms that would satisfy the requirements for all-type applications (Rakshitha & Radhika, 2018). While a single platform might be not enough for ICV data processing, the existence of two and more platforms may require an additional range of safety measures and responsibility issues.

Once there is a possibility of separating data storage platforms that to store enormous volumes of data, the issue of who is the actor that will take a responsibly for the lack of security measures in case of a collapse comes into question. While IT and AI professionals are currently looking for a better hardware and software powerful computation platform for Level 4 and Level 5 ICVs, in the meantime law-making bodies should recognize that a large spectrum of actors and operators may be involved in the process of assigning responsibility for hypothetical collapses to a specific actor(s) at each stage of ICVs data processing.

It is imperative to determine who is responsible actors are and to accurately frame the responsibility itself. This should be the subject of further discussion and deeper legal research. However considering all existing risks, such as interference and remote-control interception, the responsibility without the need to prove a causational link, should be consolidated for the actors. Going forward, we should move towards strict liability rules which ought to play a leading protective role for the ultimate users of the automated and connected vehicles.

Industry might consider the possibility of establishing a separate data storage platform so as to distinguish operators who may bear full or partial responsibility for any type of inconvenience that may occur without proper identification and authorisation, such as data leakage or interference. However, law-making bodies should prevent manufacturers from being exempted from liability and while placing liability on the platform operators. The EU law-making bodies should precisely consider all the necessary range of requirements for platform security. Nevertheless, the responsibility for any inconvenience or incompliance should be passed to Industry. Nevertheless, manufacturers might consider the platform as a totally separate mechanism for the purposes of data storage. If data is linked to connectivity and automation of V2ALL, Industry should be the only subject bearing liability related to the platform’s breakdown or any other inconvenience.

In all cases, when responsibility is to be borne by Industry, the latter should be granted an exclusive right to strict monitoring. Bearing in mind the sensitivity of the issue, strict monitoring for optimal performance of data processing security mechanism should be mandatory. Strict monitoring should grant the right of access to the audit report of a particular frequency to Industry. Although strict monitoring will allow the main actor to track all the necessary security steps, audit will also ensure regular check-up of all compulsory requirements and standards established at the European Union level.

## 7. Conclusions and Recommendations

Common security requirements alongside with procedures for testing and validation of each stage of ICVs data processing should be ensured at the European Union level using a separate Directive. Seeking to ensure that high-level protection for both ICVs users and other implicated parties, the precise regulatory framework in the Directive, which addresses security requirements for the data processing separate from the ICVs liability issues, should be established at the European Union level. The Directive should detail common security requirements that include defences against the ECUs attacks, such as interference and remote-control interception of ICVs. Moreover, the Directive should include both in-put and out-put data security models that would ensure ICVs users’ ‘privacy and data integrity.

ICVs certification should be understood as a crucial issue to allow driverless vehicles to enter the road network and a safe plethora of applications to smooth connectivity and mobility in Europe. ICVs certification should be determined and detailed at the European Union level to ensure a credible safety approach through the lifecycle of a driverless vehicle. Furthermore, the institution in charge of the mandatory ICVs certification and licensing of the ICVs workshops should be identified. For the purposes of ICVs mandatory certification, either a separate Directive should be established at the European Union level, or Directives 2007/46/EC and 2014/45/EU alongside with the Regulations (EC) No 661/2009 and (EC) No 595/2009 should be amended by placing ICVs certification, approval and periodic tests into a separate section.

ICVs software upgrades should include compulsory monitoring and frequent calibration tests for each ICV within the European Union dimension. While ensuring a high level of data security against interferences and data leakage, the compulsory periodic monitoring of a data storage platform should also be integrated at the EU level. Even though manufacturers might consider a data storage platform as separate mechanism, as long as data possesses connectivity and automation of V2ALL, Industry should be the only subject bearing liability for the platform's breakdown or any other inconvenience.

## References

Alessandrini, A., Campagna, A., Delle Site, P., Filippi, F., & Persia, L. (2015). Automated Vehicles and the Rethinking of Mobility and Cities. *Transportation Research Procedia, 5*, 145-160. https://doi.org/10.1016/j.trpro.2015.01.002

Amadeo, M., Campolo, C., & Molinaro, A. (2016). Information-Centric Networking for Connected Vehicles: A Survey and Future Perspectives. *IEEE Communications Magazine, 54*(2), 98-104.

Bergey, C. (Interviewee). (2018, April 13). Unique Challenges of Autonomous Vehicles. [Western Digital. Interview to Autotech Council Autonomous Cars, the CUBE, SiliconANGLE‘s online show]. Retrieved from https://video.cube365.net/c/906042

Community Research and Development Information Service (CORDIS). (2019). *Results Pack on connected and automated driving: A thematic collection of innovative EU-funded research results*. Publications Office of the European Union. ISSN 2599-8285. Luxembourg: The Community Research and Development Information Service (CORDIS).

Coordination of Automated Road Transport Deployment for Europe (CARTRE). (2019, April). *Support faster deployment of connected and automated driving across Europe and Data Exchange Platform*. Paper presented at the 2nd European Commission Conference on automated driving, Brussels, Belgium.

Cunningham, M., Regan, M. A., Catchpole, J., & Ballingall, S. (2016). Investigation of Registration, Driver Licensing and Insurance Issues Associated with Automated Vehicles. Paper number ITS-AP-TP0360. *23rd ITS World Congress* (pp. 1-14). Melbourne, Australia.

Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., … Yu, S. (2019). An Overview of Attacks and Defences on Intelligent Connected vehicles. arXiv: 1907.07455v1 [cs. CR], 1-36. https://www.academia.edu/39975663

European Commission. (2016). Antitrust: Commission fined truck producers EUR 2.93 billion for participating in a cartel. *European Commission Press Release*, IP/16/2582. Retrieved from https://europa.eu/rapid/press-release_IP-16-2582_en.htm

European Commission. (2017). FOT-Net Data Sharing Framework. D3.1, WP3, F 1.0, final. Retrieved from http://fot-net.eu/Documents/data-sharing-framework/

European Parliament and the Council. (2007). Directive 2007/46/EC establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive). *Official Journal* L 263.

European Parliament and the Council. (2009). Regulation (EC) No 595/2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC. *Official Journal* L 188.

European Parliament and the Council. (2009). Regulation (EC) No 661/2009concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended thereof. *Official Journal* L 200.

European Parliament and the Council. (2014). Directive 2014/45/EU on periodic roadworthiness tests for motor vehicles and their trailers and repealing Directive 2009/40/EC. *Official Journal L.*, 127. https://doi.org/10.1109/MCOM.2016.7402268

Innamaa, S., Smith, S., & Uchida, N. (2017). Draft version 1.0 of the high-level Trilateral Impact Assessment Framework for Automation in Road Transportation. Retrieved from https://connectedautomateddriving.eu/wp-content/uploads/2017/05/Trilateral_IA_Framework_Draft_v1.0.pdf

Olia, A., Abdelgawad, H., Abdulhai, B., & Razavi, S. N. (2015). Assessing the Potential Impacts of Connected Vehicle: Mobility, Environmental and Safety Perspectives. *93rd Annual Meeting of the Transportation Research Board,* 229-243. https://doi.org/10.1080/15472450.2015.1062728

Rakshitha, K. S., & Radhika, K. R. (2018). CarStream: An Industrial System of Big Data Processing for Internet of Vehicles. *International Journal of Trend in scientific Research and Development (IJTSRD), ISSN: 2456-6470, 2*(4), 1811-1814. https://doi.org/10.31142/ijtsrd14408

Rodriguez-Navas, G., Seceleanu, C., Hansson, H., Nyberg, M., Ljungkrantz, O., & Lönn, H. (2014, June). *Automated Specification and Verification of Functional Safety in Heavy-Vehicles: the VeriSpec Approach*. Paper presented at the Forteenth Design Automation Conference, San Francisco, CA. Abstract retrieved from https://doi.org/10.1145/2593069.2602972

Tao, Z., & Bonnifait, P. (2015). Modelling L1-GPS errors for an enhanced data fusion with lane marking maps for road automated vehicle. *CNRS, Heudiasyc* UMR 7253, CS 60 319, 60 203. https://www.academia.edu/18489700

The Eurostat. (2019). *Passenger cars in the EU – update 2019*. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php/Passenger_cars_in_the_E U#Overview

Xu, W., Zhou, H., Cheng, N., Lyu, F., Shi, W., Chen, J., & (Sherman) Shen, X. (2018). Internet of Vehicles in Big Data Era. *IEEE/CAA Journal of Automatica SINICA, 5*(1), 19-35. https://doi.org/10.1109/JAS.2017.7510736

**Copyrights**