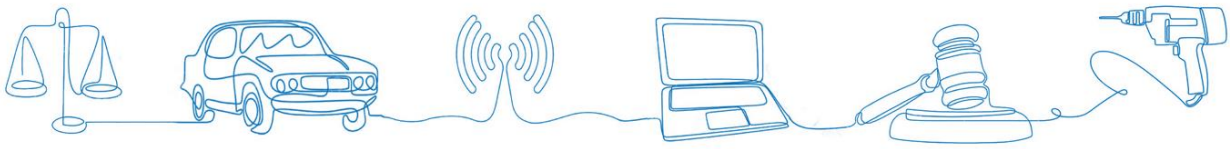
GRIMALDI STUDIO LEGALE

Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform

Legal Study



INTRODUCTION

Project title: Liabilities of Independent Service Providers when providing repair and maintenance under the Secure Onboard Telematics Platform, Legal Study

This legal study is made up of a main report and an annexed case studies report.

 MAIN REPORT

Object: The main report analyses the topic of liability of Independent Service Providers with a key focus on the automotive sector, identifying and explaining the current legal framework, and the main issues related to its application in light of new technological developments and challenges. It then takes a position on liability rules applicable to service providers when providing vehicle remote repair and maintenance and other services, in the context of specific data-sharing architectures in use. Next, it tries to assess the expected impact of a possible reform of the relevant framework which takes into account new technologies and data-related challenges and develops a set of policy recommendations addressed to legislators at national and EU level.

Author: Martina Piantoni

Contributors/researchers: Professor Gaspare Fiengo; Federica Frittitta; Marco Lauro

QA Supervisor: Giovannella D'Andrea

 CASE STUDIES REPORT

Object: The case studies report focuses on specific regulatory frameworks in place governing liability in four selected Member States: France, Germany, Italy, and Spain. Notably, it illustrates the general principles of law underpinning liability theories in the aforementioned countries, describes the legislation currently in force and draft legislation in phase of discussion, specifically focusing on the national implementation of the Product Liability Directive, as well as the legal doctrines and case law. It then reasons on the applicability of the identified rules, in each of the countries above, to Independent Service Providers in the automotive after-market.

Authors: Professor Gaspare Fiengo; Giulia Lovaste

Contributors/researchers: Federica Frittitta

QA Supervisor: Giovannella D'Andrea

CONTENT

EXECUTIVE SUMMARY

The rise of data driven mobility services in the automotive aftermarket has nursed a debate on how to ensure fair competition between Service Providers ('SPs'), by enabling both Vehicle Manufacturers ('VMs') and Independent Service Providers ('ISPs') to access in-vehicle data and resources to supply apps and services. Various data access solutions – such as the Extended Vehicle and Neutral Server, the Shared Server, and the Secure On-Board Telematic Platform ('S-OTP') - have been presented by the concerned actors.

Previous studies have shown that VMs' dual role as car producers and apps providers, result in a competitive edge: since VMs control the source of the in-vehicle data, they are in a position to leverage such control by restricting data access and usage by other competitors. While competition rules will apply to similar restrictions anyway, some data access solutions reduce by far the risk of unfair competition, enhancing, in turn, innovation and consumers' freedom of choice. Remarkably, this is the case of the S-OTP, which provides equal access and interaction to the data, functions, and resources of the vehicle, to all service providers, upon user's consent. Yet, the uptake of the S-OTP, coupled with **existing legislation on liability**, could stir up unrest from VMs, who might fear having to bear (strict) responsibility for causes beyond their control. Rules on liability have sometimes been invoked as an argument to deny ISPs' direct access to in-vehicle data. This has been possible due to the uncertainty that dominates the current legal landscape.

Arguably, today's liability framework is somewhat patchy when it comes to determining accountability for damage caused in the digital context: the surge of new technologies and the related shifting of the innovation focus from products to new forms of services has not been accompanied so far by the rise of a significant new body of rules on liability for damages that may occur. Still, when SPs access in-vehicle data and supply data driven services in the automotive aftermarket, they may face a large number of liability claims. For instance, they could incur in *(a)* tort liability for damages caused, due to their app, to the vehicle, or in *(b)* contractual liability for damages affecting the vehicle or the data service; or even in *(c)* data liability for breach of data related laws, for instance for unlawful processing of personal data, or breach of "proprietary" rights, such as IP related rights or trade secrets.

Due to the lack of tailored provisions on digital service liability, different and layered bodies of law apply to each of the above situations, varyingly allocating responsibilities and defences among the operators. For instance, the recently enacted **Directives on sales contracts for digital content and services**[1] for the first time regulate certain contractual aspects on new technologies and data services for which there were previously no rules, including liability profiles when the digital content or service is not in conformity with the sale/supply contract. Conversely, when the damage is suffered by a third party, allocating extracontractual liability is likely to be more difficult, as either the **Product Liability Directive** ('PLD'), which struggles to apply to new technologies, or other **general tort law**, which is not harmonised across the EU, come into play.

In the first case, there is uncertainty about the extent to which existing strict product liability, revolving around the notion of tangible products, might apply to intangibles and to new products bundled with apps. Moreover, certain concepts and definitions of the current PLD do not fit new realities. For instance, the "*time when the product was put into circulation*", in relation to which the defect shall be assessed under the PLD, is a notion that triggers interpretative questions and uncertain outcomes in the digital context: in fact, while with traditional vehicles development is frozen at the time of launch of the vehicle, when the VM loses his control over his product, this is no longer the case with connected vehicles, which typically host data services that determine the functions of the car and evolve over the vehicle's lifetime.

[1] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods and Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019). They are currently in the phase of national transposition until 1 July 2021 and have be applied as of 1 January 2022.

In the latter case, the unharmonized regimes at national level make it difficult to ascertain and predict each time which rule is applicable if harm occurs, with possible differences relating to the applicable time-limits for action, the party burdened by the *onus probandi,* the circumstances that require evidence (e.g., negligence, duty of care, existing defect, damage suffered, etc.), the existing defences and exceptions, and possibly leading to different outcomes depending on the country where the claim is brought (and consequent risk of "*forum shopping*"[2]).

Ultimately, uncertainties remain regarding who shall bear which risks in the current framework. To fill the legal gap, an exercise of legal interpretation is needed to extend the applicability of the available rules, regardless of their sub-optimal fitness for purpose.

This Study, based on an exercise of legal interpretation of the current EU liability legislation, concludes that:

- Overall, the VM could be deemed primarily responsible for the vehicle security over the vehicle's lifetime ("*cradle to grave*"), but always subject to its possibility to exercise right to remedies against the actual responsible, such as an ISP, after having paid full compensation to the entitled subject.
- If and to the extent a connected vehicle with embedded apps may be considered a 'product' for the purpose of the current PLD, strict product liability may only apply for damages triggered by defects that are already present at the time of putting the product into circulation. This precludes, under today's framework, any possible concern (of VMs or ISPs) on accountability under the product liability framework for evolving or added technologies, i.e., for defective apps released and installed in the vehicle after the vehicle was marketed. However, this assumes that the fault or source for any system failure could be always diagnosed and traced, to assess whether the root-case of the damage lies in flaws in the app, its installation or update, the feeding data accessed, or the vehicle components.
- Pursuant to Type Approval Regulation[3] it is up to the VM to provide a safe and secure environment in the vehicle, also in terms of cybersecurity and for the benefit of apps running on it. However, it is not clear if those apps, such as other motor vehicles' elements, should be subject to the same safety approvals under the responsibility of their developer.

Under any of these interpretations, the party bearing the *onus probandi* (usually the injured consumer/claimant) will likely experience difficulties to single out and demonstrate the chain of causality; if required, the existence of a duty of care on some operator in the supply chain and his failure to observe it (negligence or fault); and, above all, the cause that led to the accident. If an excessive burden lies with the consumer, claims against ISPs or VMs are unlikely to succeed and the consumer risks to suffer the consequences of a damage entirely on his shoulders, without the prospect of any compensation. On the other hand, this uncertainty may hamper innovation, as market operators might be reluctant to delve into the provision of new services or the production of new technological items, if these risks to result in a surge of lawsuits or if they are unable to clearly assess their legal responsibilities up stream.

To address the identified problems, clear regulatory solutions, undertaken at EU level, are needed. As far as already existing *acquis* is concerned, key amendments are critical to urgently update the PLD, making it more apt to cope with the current digital challenges and more consumer friendly[4]. On the other hand, existing competition rules should be applied to non-traditional digital markets, ensuring fair competition between ISPs and VMs. As far as legal gaps are concerned, *ad hoc* rules on digital service providers' liability might be envisaged, parallel to those on producers' liability.

[2] "Forum shopping" refers to the practice of a claimant who chooses the country (and hence the law) where he has his case heard, in order to have appointed as competent the court which is believed to be the most likely to apply the more favorable law and hence to provide a favorable judgment.

[3] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, *OJ L 151, 14.6.2018. Pursuant to Art. 13(5), "Manufacturers shall ensure that their vehicle or vehicle's components and parts are not designed to incorporate strategies or other means that expose them to risks, including in terms of cybersecurity".*

[4] It is noted that, at present, a revision of the PLD and the product safety framework is in the Commission's pipeline.

Additionally, on account of the evolution of the debate on data access and the Commission's formal acknowledgement of the competition problems entailed by some proposed architectures, **the time is right for a decisive step to be taken in the direction of a clear sector-specific EU regulated access regime and resultant revision of the Type Approval Regulation**. Notably, the far-reaching solution of S-OTP, as recommended by vast literature, would lead to an open ecosystem of connected driving, in which the driver can freely choose between the providers performing services directly in the car, thus protecting competition, innovation, and consumer choice. A regulatory proposal on S-OTP should be designed with due account of any safeguards that ensure security and safety of apps, to reduce the risk for liability implications. These include, inter alia, a mandatory logging of data necessary to identify root causes, the strengthening of the obligation for VMs to design vehicles that do not support unsafe and unsecure apps, as well as rules on independent certification or validation processes that avoid the need for VMs to preliminary review and accept all apps or all service providers to be granted write access.

Similar new EU interventions should opportunely take the form of regulations, thus reducing room for divergencies across countries, and be complemented, where possible, by guidelines or other soft law in order to easily adapt to relentless technical developments while addressing doubts of the operators.

SECTION I - BACKGROUND

This section contextualises the Study, briefly presenting new trends in the automotive market and the rise of data driven mobility services. It then recalls the challenge of ensuring fair competition among actors willing to access relevant vehicle data and the main features of alternative data sharing architectures envisaged to this end. Finally, it explains the objective and main purpose of the research.

Chapter 1. CONTEXT OF THE STUDY

In the last decades, transport and mobility patterns and vehicle servicing have been subject to a major transformation due to the rise of Connected and Automated Mobility ("CAM"). Today, more than 60 million vehicles in the EU fleet are connected to the Internet and expected to only grow further in the coming years, paving the way for remote data driven services and interconnected traffic in an era of automotive digitalization.

The automotive sector is already one of the largest data generators. Vehicles can collect individual information via different types of sensors. It is expected that, in the coming years, they will also transmit between each other information about speed, distance ,or upcoming danger and traffic jams. With this proliferation of automotive data comes the potential to support new services, thus creating new opportunities for service providers – such as SMEs, third parties and repairers – wishing to develop innovative mobility solutions. In addition, external data sources (such as street infrastructure, social networks, and online services) can be linked to vehicle data, with vehicles transmitting and receiving data to and from their surrounding environments, allowing for further customised driver-to-service provider interactions.

1.1 Use of data in the automotive sector

One example of these new services is predictive maintenance. Put simply, the data generated from the vehicles could be used to detect the demand for necessary repair and maintenance ("R&M") services remotely. This is done through connected vehicles transmiting information about their condition via mobile data networks; enabling the performance of remote diagnostics to predict whether certain components are failing or will fail and, sometimes, even repair them remotely. This is all to the benefit of the driver who is alerted proactively in case of a failure of the vehicle.

Other examples of similar data-driven services, sometimes also entailing a certain level of automated driving, include find parking or park-and-ride information, theft protection, usage base tax and toll fees or insurance fees, driving style suggestions or driver assistance systems, automatic parking, adaptive speed control or lane-keeping, emergency or breakdown call functionalities, and traffic information.

The advancement in automotive technology already makes it possible for intelligent vehicles to integrate these functions based on different designs. For instance, there can be an on-board telematics platform that not only controls certain functional features such as remote features, but also provides a platform for applications that protect, inform, and assist drivers. Alternatively, already-existing application platforms (e.g. Apple CarPlay, Google Android Auto) make it possible for drivers to connect their smartphones to a compatible Human Machine Interface ("HMI") of the vehicle – the in-vehicle display for example – and access mobile applications from there. The principle is to use the vehicle's HMI as an extension of the smartphone screen, with the addition of the vehicle's system-functionality integration (e.g. controlling volume from wheel controls), without the need for any bespoke platform or component running in the in-vehicle embedded systems.

In terms of actors involved, data-based services can be provided by different operators that enter the future market for mobility services or the repair and maintenance business. The CAM industry presents a high level of diversity in terms of involved market players, which include road authorities, manufacturers (hereinafter also Original Equipment Manufacturers, "OEMs", or Vehicle Manufacturers, "VM"), suppliers, telecom providers, providers of artificial intelligence ("AI") technologies, mobility services platforms, supply chain platforms of logistic specialists, Internet of Things ("IoT") platforms, providers of technology and telematics, big data, content, insurances, etc (all together independent service providers "ISPs").

To allow for a level playing field and fair competition among them –ultimately benefiting the end consumer

through increased market choice – it is key to foster a balanced and equal access to vehicle data and resources for manufacturers and ISPs. This is needed to avoid market distortion, which happens where a potential player has substantial advantage over the others. In fact, anyone who does not have direct access to relevant data loses in attractiveness, as they cannot offer appropriate services to the driver directly in the vehicle.

For instance, in order to compete in the vehicle R&M market, ISPs – such as automobile clubs – must be able to access, among other data, vehicle Repair and Maintenance Information[5] ("**RMI**"). This technical information is increasingly important due to the increasing complexity of vehicles and their interaction with their surrounding infrastructure, their growing number of parts, and use of on-board electronics. In this regard, there is an EU framework on motor vehicle distribution and after-sales agreements[6] that seeks to ensure that ISPs have easy, restriction-free and standardised access to vehicle data, enabling fair competition and consumer choice from a variety of multi-brand aftermarket operators. Among others, the Type Approval Regulation, aiming at reinforcing vehicles' on-board safety, clearly contains a data sharing obligation in the transport sector (established in 2007 and further enhanced in 2018) preventing manufacturers from locking ISPs out of the market.

1.2 Fair competition between OEMs and ISPs

Nonetheless, equal access between OEMs and ISPs to all in-vehicle data is far from guaranteed: there is on-going political discussion at EU level[7] on the argued substantial advantage of OEMs over other potentially interested market players. Unlike other market operators, OEMs can, and usually do, rely on direct access to collected in-vehicle data necessary to provide innovative services to end consumers and, in some instances, control *if* and *who* they share it with. Admittedly, a *de facto* control of data by operators having a very little interest in making data accessible to competitor third parties for developing new apps and services can be a source of competitive advantage: to the extent that the entity controlling the source of the data will likely seek to restrict data access and usage by another party, there is the potential for the owners of this control to distort the market and hamper the provision of data-based services.

For this reason, the Commission has engaged to monitor the situation and consider a range of alternative options for a **framework enabling vehicle data sharing** that supports fair competition in the provision of services in the digital single market, whilst ensuring compliance with personal data protection legislation. While technically a range of solutions exist today – including providing an open yet safe and secure app platform for third parties to access vehicle information and in-vehicle data – a variety of legal hurdles and/or ambiguities may hamper the uptake of any of such solution, or be used by some to leverage the acceptance of one solution

[5] "Vehicle repair and maintenance information" are defined under Article 3(48) of Regulation (EU) 2018/858 as 'all information required for diagnosis, servicing, inspection, periodic monitoring, repair, re-programming or re-initialising of the vehicle and which the manufacturers provide for their authorised dealers and repairers, including all subsequent amendments and supplements to such information. This information includes all information required for fitting parts or equipment on vehicles'.

[6] See Commission Regulation (EU) No 461/2010 of 27 May 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices in the motor vehicle sector, OJ L 129, 28.5.2010 ("Motor Vehicle Block Exemption Regulation") and its Supplementary Guidelines; Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices, OJ L 102, 23.4.2010, where applicable to the motor vehicle sector. Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, OJ L 171, 29.6.2007. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, OJ L 151, 14.6.2018, as amended by Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019, on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC), OJ L 325, 16.12.2019 ("Type Approval Regulation").

[7] Among others, the eCall type-approval Regulation (EU) 2015/758 had focused attention, already in 2015, on the need to put in place the conditions for open and undistorted competition in the use of in-vehicle data, asking the Commission to assess the need of requirements for an interoperable, standardised, secure and open-access platform.

over another, thus reducing fair digitalisation chances.

As such, liability legislation has been sometimes invoked as an argument not to allow ISPs direct access to in-vehicle data. This has been possible due to the legal uncertainty dominating the current landscape, and conflicting views on the applicability of existing tort law *acquis*, both at EU and national level, to new realities. In fact, new legal challenges brought about by the surge of new technologies, and the related shifting innovation focus from products to new forms of services, has not been accompanied so far by a reciprocal rise of liability rules for damage resulting from the use of said new digital technologies. Consequently, the resulting current liability framework is piece-meal when it comes to determining accountability for damages caused in CAM.

That being said, it is stressed that in no case can the existing legal obligation to comply with liability obligations or the uncertainty thereof, be relied on as justification for the monopolistic control over in-vehicle data usage, or for a ban on third party access to said data. This would be an anticompetitive outcome which existing competition legislation already seeks to tackle.

Furthermore this Study starts from the premise that **no proprietary right exist in data**, so as to remove any potential reliance on civil law proprietary protections and infringement claims by market operators controlling data sources[8] against the party that uses data absent any formal permission.

Chapter 2. OVERVIEW OF DATA-SHARING ARCHITECTURES

Back in 2016, the Commission launched GEAR 2030, a High-Level Group for the automotive industry aimed at ensuring a co-ordinated approach in addressing the challenges faced by the European automotive industry[9]. It also established a dialogue with stakeholders and public authorities, the Platform for the Deployment of Cooperative Intelligent Transport Systems ("**C-ITS**") Platform[10], as part of which, the Working Group 6 ("**WG6**") examined the potential ways to give access to in-vehicle data and resources so that service providers can propose services to their customers.

The three different architectures for access to in-vehicle data and resources identified by WG6 are:

- On-board application platform
- In-vehicle interface
- Data server platform

Each of these architectures in principle works within the existing legal framework but has its own implications in terms of level of undistorted free flow of vehicle data, technical issues (inter-operability and portability, required skills) and legal issues (data protection, data ownership, access to use of data, liability, competition), which have been analysed and compared in previous studies[11,12].

On the basis of each of these technical architectures, a variety of applicative solutions were developed in

[8] Data can potentially be protected by the entities that created the data or made investments in it, through the law of confidence and/or as a trade secret, by invoking some pieces of law such as the Trade Secrets Directive (Directive (EU) 2016/943) or the Database Directive (Directive 96/9/EC). However, there is considerable regulatory diversity across countries in terms of whether data can give rise to property rights and the extent to which any proprietary rights in data will arise in respect of in-vehicle data (for example depending on how the data is obtained, verified and presented). See Osborne Clarke LLP, 2016, Legal study on Ownership and Access to Data, published by the European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1.

[9] See http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8640.

[10] See https://ec.europa.eu/transport/themes/its/c-its_en.

[11] TRL, 2017, Access to In-vehicle Data and Resources, published by the European Commission. Available at: https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf ("**2017 TRL Study**").

[12] Deloitte, 2018, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data and liability, published by the European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en ("**2018 Deloitte Study**").

technical literature and, in some cases, implemented. Among those, this Study focuses on the On-board telematics platform ("S-OTP"), developed as an application of the On-board application platform described by WG6. Alternative solutions, which will be mentioned and partially analysed in a comparative exercise *[see below in Section III, chapter 4]* are the Extended Vehicle/Neutral Server, the Shared server and the B2B marketplace, developed as derivatives of the Data server platform architecture.

2.1 On-board application platform and In-vehicle interface

An On-board application platform is embedded in the vehicle and allows hosting and deployment of applications on the HMI of the vehicle (i.e. on-board machine interface). The On-board application platform hence keeps the control of data access inside the vehicle. Applications hosted on the platform need to be tested, verified and certified in way that prevents unauthorized modifications once installed and protects the platform from external threats (such as malware or spyware). Overall, local access control and remote access control maintain the integrity of the applications and data by blocking incoming data from unauthorized parties. A host management controller controls the core and service runtime environments, sends updated applications to the application platform to improve the functional performance, and provides upgraded security patches and policies.

Similarly, the in-vehicle interface is inside the vehicle but allows connection to devices outside the vehicle and access to a standardised set of data (e.g. emissions, fault codes, etc.) in real-time and of high quality.

2.1.1 Secure On-Board Telematics Platform

FIA Region I Security Study[13] outlines the features of the S-OTP, which gives a concrete solution of an On-board application platform for modern telematics services. The S-OTP is designed to achieve a number of goals, namely: protection against cyber-security incidents, data protection, consumer empowerment and freedom of choice, implementation of the Separation of Duties principles, and openness and non-discrimination.

With S-OTP, requested vehicle data is transmitted wirelessly to ISP servers upon users' consent. No OEM backend server links the vehicle and the ISP backend servers on which the data is initially collected and distributed. Applications can directly access the vehicle (both input and output elements) to provide additional services for the driver, at an equal level between the OEM and ISPs. Secure communication to and from outside the vehicle as well as communication of different networks inside the vehicle are implemented by the on-board telematics interface present in each vehicle. Integrity protection of the communication interface ensures that every message undergoes a check for errors or malicious content. The owner/driver of the vehicle is given a central role with complete control over his data, having the power to decide whether ISPs are granted access to it, and, if so, to what extent and for which application(s), through opt-in and opt-out options.

Third party developers must be certified by a standardised procedure to gain access to the on-board platform. The S-OTP entails an external infrastructure with a pivotal role, i.e. the so-called Automotive Gateway Administrator ("A-GWA"), based on a Public Key Infrastructure ("PKI").

The A-GWA, also called Access Control Manager, is an independent entity, not under the control of the VM, who manages and modifies the user/usage profiles and updates in the car, having rights limited to manage and modify the access profiles of the various service providers, authorities, and participants in interconnected road traffic. This entity may not benefit directly from the processed data and enjoys trust by service providers and authorities through specific actions such as SP certification and regular re-certifications using the C-ITS PKI. The Access Control Manager has no read access to transmitted data or content data inside the vehicles and therefore ensures that the Separation of Duties principles are realised.

[13] Tuvit - M. Bartsch, A. Bobel, Dr. B. Niehöfer, M. Wagner, M. Wahner), 2020, On-Board Telematics Platform Security, FIA Region I. Available at: https://www.fiaregion1.com/wp-content/uploads/2020/06/20200615_FIA_vehicle_security_report.pdf. See also, FIA Region I and others, Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach, 2021, Available at: https://www.fiaregion1.com/wp-content/uploads/2021/03/2021-02-S-OTP-Paper-vFin.pdf.

An Automotive Gateway ("**A-GW**") inside the vehicle is responsible for securing the remote access to and from the vehicle, conforming control units (docker) on which ISP apps can run and that can be interacted with by the drivers, owner or occupants through the HMI[14]. The A-GW is used as the central point of access for carrying out software updates as well as diagnostics, repair, maintenance, as well as prognostics tasks. Also, within the S-OTP, the A-GW securely separates the services (the vehicle's external interface) from the information systems relevant to the driver (driver domain) and the safety-related components (safety domain) and processes in advance any information entering or leaving the vehicle, in accordance with specific user and usage profiles[15].

This way, the system creates an opportunity for all *authorised* parties to directly access data functions and resources from the vehicle on a fair and equitable basis and to create a wide range of applications using the vehicle internal resource. It introduces a non-discriminatory and open way to connect the individual car with backend services and with IoT devices like smartphones. Ultimately, S-OTP supports the shifting of data sovereignty from the OEM, as single data controller, to all different stakeholders, granting all market participants the same opportunities as the OEM to market their services to end consumers.

2.2 Data server platform

Unlike the former, Data server platform is a server external to the vehicle where relevant vehicle data is transferred to and made available to service providers. Data server platforms result in a more limited access to the vehicle's HMI, although still achievable should the HMI be accessed via mobile platforms.. The data server platform is further classified into three derivatives, namely: Extended vehicle, Shared server, B2B marketplace.

2.2.1 Extended Vehicle / Neutral Server

The Extended Vehicle concept and the Neutral Server solution have been developed by OEMs (the European Automobile Manufacturers Association, "**ACEA**") in 2016[16]. An Extended Vehicle is a vehicle with external software and hardware extensions for some of its features. These extensions are developed, implemented and managed by the OEM.

The vehicle communicates to backend servers using mobile networks. Data is sent over a secure and encrypted communication channel to a dedicated OEM proprietary backend server, which has a permanent connection to the car. Vehicle data from the server is then made available to stakeholders (third party participants, ISPs) via a standardized interface for data-processing and application development . Each OEM uses their own proprietary software to establish and secure connections and has exclusive responsibility on the maintenance and upgrade of the data interface.

As all data to and from the vehicle flows is intermediated through the OEM server, no direct communication is allowed between the vehicle and the ISP backend servers. Accordingly, the OEM has sole direct control and access to vehicle data, functions (be it read or write) and resources, and determines which, if any, ISP can read data from the vehicle. Controlling the dataflow, OEMs grant access subject tocontractual bilateral agreements between the OEM and the individual market participants which conditions access based on the use-case, the nature of usage and type of data. According to ACEA, the data that can be made available excludes any data imported by vehicle users (e.g. from a mobile phone contact list, selected destinations for navigation) and data received from external sources (e.g. information transmitted by roadside units, other vehicles or vulnerable road users).

Ultimately, as the OEM can decide for itself to whom it forwards or even sells the data, the owner/driver of the

[14] Ibid.
[15] Ibid.
[16] ACEA, 2016, Strategy Paper on Connectivity. Available at: https://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf; and ACEA, 2016, Position Paper Access to vehicle data for third party services. Available at: https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third party_services.pdf.

vehicle and other stakeholders have very limited access rights, their data subjugated to the full control of the OEM, leading to a monopolistic position of the latter.

To address some concerns with the Extended Vehicle concept, an option was consequently introduced to connect a 'neutral server' to the OEM backend systems. Operated by independent third parties, the independent neutral server operator collects data from the extended vehicle OEM's server, merges and processes it, and resells the data to third parties. ISPs may hence obtain data from the neutral server operator, who can negotiate with the OEMs for additional data fields to be included on their servers without revealing by whom and for what purposes this data will be used.

Compared to the normal Extended Vehicle solution, this helps enhance competition as service providers get the choice between accessing data from the OEM or going through the neutral server. In terms of fees, OEMs charge the neutral server provider a fee to access the data, a premium whichs passed to the ISP. Compounded to the access fee is an additional premium charged by the neutral server provider for the maintenance of the server and provision of data to the ISP. This process ensures that the OEM cannot easily monitor the data streams that come and go from the ISPs and identify which competitor is working on the vehicle. As OEMs do not finance nor run the neutral servers, in principle (according to ACEA), OEMs are not able to monitor who is accessing what data except for security reasons and for overall system improvement. In any case, OEMs reserve themselves the right to limit the data accessible to those required for diagnostics, repair and maintenance, and only when the vehicle is stationary. Furthermore, the OEM still maintains their monopolistic position regardless and they remain sole data controller, charging costs to ISPs on consumer-generated vehicle data and deciding which ISP competitor gets access and what type.

These solutions are already being implemented and used by many OEMs across Europe, with secure interfaces in the vehicle allowing connections to the OEM's servers built into today's modern vehicles[17].

2.2.2 Shared Server

The Shared Server is an external data server where relevant vehicle data is transferred from the OEMs and made available to ISPs. It is based on the same technical service platform as the Extended Vehicle, but the OEM backbone server is replaced by a 'shared server' in the sense that it is not run or financed by OEMs, but rather by a mutually agreed neutral server provider, commissioned and controlled by a mixed consortium representing interested stakeholders (i.e. business interests but also interests of the consumer to run the server and certify applications in a transitional phase[18]). Ideally, the server should be based in the EU. The neutral server provider running the server gives access to vehicle data to various providers, based on informed driver consent.

The server is divided to ensure a differentiated access and allow OEMs to access anonymous data and secure communication. As as result, like the S-OTP, compliance with the Separation of Duties principle is upheld, as one of the partitions of the Shared Server is meant for the OEM to ensure safety, security, and environmental protection.

The OEM acts as a system administrator for the transfer of data between the vehicle and the Shared Server. Data available at the standardised interfaces should be of the same quality as the data of the OEM backend.

The Shared Server thus gives equal access to in-vehicle data and anonymizes this access to the manufacturer, thereby addressing some of the shortcomings of the Extended Vehicle and allowing a degree of competition.

[17] However, it is noted that the Neutral Server NEVADA has recently received a serious blow when Volkswagen decided to withdraw from VDA's Neutral Server concept.

[18] See FIA Region I, Policy Position on Car Connectivity. Available at: https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf

2.2.3 B2B marketplace

With a B2B marketplace solution, an independent third party operates access to the OEM's server. Data from the vehicle manufacturer's dedicated server (i.e. the Extended Vehicle) is forwarded to the neutral server from where third parties obtain access.

As explained in the 2017 TRL Study, the commercial platform provider (or neutral server provider) could be a big data/IT company (e.g. Google, IBM etc.) which provides bulk storage of data, keeps track of incoming and outgoing data, and ensures data access demand from independent operators and third parties are met within a stipulated timeframe.

In case of additional request for data not already present on the server, the server provider approaches the manufacturers to obtain access to said data. The identity of the requesting third party (i.e. application developer) is not disclosed to the OEM.

2.3 On-going debate on the different solutions

There is on-going debate on which technical solution is to be preferred and which could hence be ultimately enshrined in new EU legislation on data access.

The ACEA supported the Extended Vehicle solution as the best method to ensure, on the one hand, that third parties (i.e. ISPs) have access to the vehicle data they require to offer services to vehicle owners or drivers; while allowing, on the other, OEMs to ensure vehicle safety, product monitoring, IT security and data protection compliance to prevent any unwanted services, or advertising thereof to reach the vehicle or consumer From the ACEA's perspective, OEM control over in-vehicle data and car access is critical to guarantee the safety and security of the vehicle. Conversely, the direct exchange of in-vehicle data with ISPs would lead to higher risks of cyber-attacks and manipulation as a new external data interface multiplies the potential targets and entry points for malicious actors[19]. Furthermore, some[20] rely on the fact that, under said direct exchange of data with ISPs, OEMs would not be in a position to assume automatic liability for defects or accidents related to applications developed by third parties to argue that the connected card should be a closed system to ensure safety and security.

Obligated to ensure the safety and security of the vehicles they produce, OEMs tend to rule out any technical solution whereby third parties could readily obtain access to vehicle data without any form of control, authorisation or authentication by OEMs[21].

In contrast, numerous trade and consumer associations have claimed that the ACEA's position on access to vehicle data jeopardises competition, innovation and consumer choice. Representatives of automotive dealers, aftermarket operators, and consumers have hence called on the EU to take onboard the proposal for a S-OTP when legislating on access to in-vehicle data, providing technical and commercial arguments sustaining their recommendation[22]. The Extended Vehicle model indeed leans towards a data monopoly and risks preventing a level playing field in the services market. Furthermore, the 2017 TRL Study considered such architecture sub-

[19] Ibid.

[20] W. Kerber, 2018, Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, 9 JIPITEC 310. Available at: https://www.jipitec.eu/issues/jipitec-9-3-2018/4807

[21] Secondly, liability rules would allow OEMs to process data only for the purpose of complying with liability obligations, but not for other purposes. In other words, such rights cannot automatically result in other usages of the data, or in denying access to such data to third parties. For instance, Regulation 2019/2144 on type-approval requirements for motor vehicles, which aims at reinforcing the on-board safety, clearly states that "those security measures should not compromise the obligations of the vehicle manufacturer to provide access to comprehensive diagnostic information and in-vehicle data relevant to vehicle repair and maintenance".

[22] See the detailed document prepared to this purpose: Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach, 2021, Ibid.

optimal, and the 2018 Deloitte Study recognised that aftermarket operators see potential barriers to data access if manufacturers gain full control of a vehicle's data and can negotiate access to that data on their own terms, potentially limiting access to some or all aftermarket (independent) actors, if not excluding their access altogether. Based on these findings, in May 2018, the Commission released a communication[23] where it mentions that centralisation of in-vehicle data on Extended Vehicle data platform servers, currently implemented by several vehicle manufacturers, might not in itself be sufficient to ensure fair and undistorted competition between service providers. The Shared Server solution (which is built on the same technical architecture as the Extended Vehicle solution) is instead seen, by the same authors, as a compromise solution, as it could solve some of the Extended Vehicle issues, providing features more aligned to delivering fairer competition. In the C-ITS Platform final report[24] and in the 2017 TRL Study it is hence proposed on a short-term basis, as an intermediate step, while the on-board application platform is deemed the best medium and long-term solution.

2.4 Solutions for safe and secure vehicles

The need to rely on these specific technical solutions for data sharing serves to minimise liability implications of data sharing and usage. Any technical solution to access and process vehicle-generated data needs to be secure, since a malware attack can have far-reaching consequences on the safety of the driver, passengers, and other users of the road. Debated technical solutions for data sharing seem to present a comparable level of safety and security[25].

In this regard, a particular focus has been placed on safety issues and on the need to ensure the anonymity of the parties involved in the exchange of real-time data[26]. To address safety and security issues while enabling equal data access, the development of a **EU-wide accreditation scheme** to help ISPs to service and repair vehicles in a secure manner has been discussed (Working Group 5 of the C-ITS platform and the 2017 TRL Study[27], among others, have proposed to create an independent accreditation body in charge of defining security standards and any related transparent certification process). Each additional component integrated into the vehicle or installed application could hence be tested, verified, and certified through such a scheme rather than exclusively by the OEM.

In terms of liability, the 2017 TRL Study argued that the implementation of each of the described technical solutions would have significant implications and pose a range of risks, applying almost equally to each of them. In principle, where there is a risk of strict liability falling on the OEMs, they may be unwilling to allow data access to third parties, especially write access. On the other hand, where the party exposed to the associated liability can control risks, this is unlikely to deter the development of a technical solution. According to the 2017 TRL Study, On-board application platform could entail less problems in this regard to the extent the OEM is able to control third party access.

---

[23] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions, On the road to automated mobility: An EU strategy for mobility of the future (COM/2018/283 final). Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0283:FIN.

[24] European Commission, C-ITS Platform, 2016, Final report. Available at: https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf.

[25] The shared server solution and the extended vehicle solution have a similar level of safety and security since they are built on the same technical architecture. As confirmed by reliable literature, the on-board application (and hence the S-OTP) can ensure the same level of safety and security, guaranteeing safe and secure real-time access to in-vehicle data and not only infotainment data. See 2017 TRL Study, p.90; Knobloch and Gröhn, 2018, FIGIEFA, OEM 3rd Party Telematics - General Analysis, p.14. Available at: https://www.figiefa.eu/wp-content/uploads/Knobloch-Gr%C3%B6hn-OEM-3rd-Party-Telematics-General-Analysis-Report.pdf.

[26] European Commission, C-ITS Platform, WG5: Security & Certification, Final Report, ANNEX 1: Trust models for Cooperative - Intelligent Transport System (C-ITS). Available at: https://smartmobilitycommunity.eu/sites/default/files/Security_WG5An1_v1.1.pdf

[27] See 2017 TRL Study; and the 'EU Forum on Access to Vehicle Information', available at https://ec.europa.eu/growth/content/commission-adopts-report-system-access-vehicle-repair-and-maintenance-information-rmi_en.

Chapter 3. PURPOSE OF THE STUDY

The main focus of the Study is the analysis of liabilities that lie with the ISPs when providing vehicle R&M. In particular, the analysis is due to provide an overview of responsibilities and liabilities on the part of the manufacturers on the one hand, and of the ISPs who have write-access to the vehicle and who run apps in vehicles, on the other.

The Study will proceed based on the assumption that S-OTP, as outlined in the FIA Region I Security Study, is implemented at EU level, thus guaranteeing a balance between access to in-vehicle data, functions, and resources on one hand, and a state-of-the-art level of security on the other. The secure S-OTP concept calls for all service providers to have equal access to the data, functions, and resources of the vehicle. This would allow third party apps (including Mobility Clubs and other ISPs) to interact with the vehicle functions and resources providing Remote Diagnostic Support (RDS) or Prognostics. In doing so, they could incur liabilities.

The ultimate aim is to provide arguments for the legislator to implement fair rules that properly balance vehicle liability, security, and unrestricted access to in-vehicle-data, functions, and resources, therefore safeguarding the possibility for Mobility Clubs to offer current and future services to their members.

To this end, the Study will focus on the following main aspects:

- Concept of liability and its implications for ISPs when providing vehicle repair and maintenance.
- Existing legal arguments on why the overall vehicle liability shall remain with the VMs, considering third party apps may interact with the vehicle functions and resources.
- Outlook on responsibilities and future liabilities of Mobility Clubs (as ISPs) when providing independent services (Repair and Maintenance) by means of the secure S-OTP.
- Advantages and disadvantages of the secure S-OTP, in terms of ISPs liabilities, in comparison with the alternative data-access architectures.
- Potential consequences of a reform of the 'product' concept under the Product Liability Directive and the inclusion of the operator's role.

SECTION II – FRAMEWORK ON DATA LIABILITY

This section discusses the applicable legal framework on liability relevant for new technologies and data. The analysis is carried both at EU and national level. As to national level analysis, the Annex turns a specific focus on four case studies, concerning existing rules in Italy, France, Germany, and Spain.

Chapter 1. OVERVIEW AND COMPLEXITIES IN SHAPING THE RELEVANT LEGAL FRAMEWORK

Liability can be defined as the responsibility and accountability of one party for harm and damage caused to another, which may be ground for compensation, financially or otherwise, by the former to the latter. It hence relates to tortious or contractual exposure, towards potential victims, in the event accidents occur. Accordingly, civil liability rules deal with the consequences of a damage caused by an activity that turned out to be harmful, regardless of whether said activity was in principle allowed or not. In doing so, they ensure an economic-efficient balance of competing interests. Therefore, when no outright-prohibition is in place, and an activity is allowed despite carrying some degree of risk, liability rules make sure that damages resulting from it are adequately compensated[28].

Looking specifically at liability issues related to the access and use of in-vehicle data and provision of data-driven services, the existing legal framework within the EU is rather complex, due to three reasons:

(i) Lack of a tailored liability regime and layering of existing rules:

The first issue is the lack of a specific set of rules and existence, instead, ofdifferent measures only partially regulating the subject matter, leaving room for both legal gaps and overlaps. Firstly, there are rules on **harm prevention** (EU Product Safety Legislation, Type Approval Regulation specifically concerning vehicles, but also Cyber-Security Laws), which seek to minimise the risk of harm that products – including those with embedded new technologies – may cause, by requiring that only safe products be marketed. Risks that are not deemed acceptable are thus addressed *ex ante* through these rules, along with the specific technical mechanisms foreseen by the data sharing architectures to guarante safe and secure data access. As this alone does not exclude damage to occur, other rules become relevant, namely on **harm compensation**. Indeed, when the injured party suffers damage, they usually seek compensation. In absence of a specific and tailored liability regime, liability rules most technologies fall, in principle, under product liability law, general tort law (i.e. extra-contractual liability), and contract law (i.e. contractual liability), possibly also in combination with insurance. However, the more complex new digital services and products become, the more difficult it is to identify and apply these multiple frameworks.

(ii) Divergences in national liability regimes:

The second issue is linked to discrepancies that may exist between EU Member States. In fact, only a small part of liability regimes is harmonised at EU level, while all others are regulated by the Member States themselves, with differing general or sector-specific rules. This results in market fragmentation, unpredictability of applicable law, and unfair or inefficient allocation of liability across different countries. Examples of harmonised rules on liability are:

[28] For further information see A. Bertolini, 2014, Robots and liability - Justifying a change in perspective; F. Battaglia, J. Nida-Rümelin and N. Mukerji, 2014, Rethinking Responsibility in Science and Technology, Pisa University Press: 143-166; E. Palmerini and A. Bertolini, 2016, Liability and Risk Management in Robotics. Digital Revolution: Challenges for Contract Law in Practice, R. Schulze and D. Staudenmayer, Nomos: 225-259.

- The strict liability of producers for defective products,
- Some aspects of liability for infringing data protection law,
- Liability insurance with regard to damage caused by the use of motor vehicles,
- Liability for infringing competition law[29],
- The newly harmonised contractual rules on digital goods and services.

As to the last example, it is noted that this key step towards clear-cut and simpler regulation of matters related to new technologies has been accomplished as a result of the Digital Single Market Strategy[30] adopted by the Commission on May 2015. In that context, the Commission had announced a legislative initiative on a package of harmonised rules for the supply of digital content and online sales of goods. This initiative was composed of (i) a proposal on certain aspects concerning contracts for the supply of digital content ("**Digital Content Directive**" or "**DCD**"[31]), and (ii) a proposal on certain aspects concerning contracts for the online and other distance sales of goods ("**Sales of Goods Directive**" or "**SGD**"[32]). As announced by the Commission in its 2015 Work Programme, these two proposals no longer followed the approach of an optional regime and a general set of rules, but contained instead a targeted and focused set of fully harmonised rules. The formal adoption of the two directives, in 2019, marked the end of a long legislative process. As a consequence, some important aspects of contractual liability, not only relating to the tangible durable medium used as a carrier of digital content, but also to data produced and supplied in digital form – such as operating systems, applications and any other software, services allowing for the creation, processing or storage of data in digital form or for the sharing of data – have now been regulated and will be soon harmonised across Member States (as soon as the provisions will be implemented into national laws). It is to be seen how Member States will implement these provisions and what impact they will have on the overall framework for data services.

(iii) Uncertainty about the extent to which existing liability regimes might fit and apply

Finally, the third issue is that, as existing legislation in principle focuses on tangible products, stakeholders cannot be sure whether they can refer to this legislation when they provide data driven services. In fact, while every piece of law may be, in principle, understood by way of broad interpretation to cover factual situations that were not envisaged at the time when it was enacted, this exercise can be very tricky. This is why market players often opt to fall back on contractual liability on a case-by-case basis. Yet, since this is a fast-moving field, it is not always easy to identify and cover all possible situations by means of all-encompassing agreements or stretching the applicability of partial legislation. Concerns hence usually remain about exposure to additional liability or costs.

In order to address these concerns, it is important to take into account where liability might arise and how to avoid inappropriate litigation exposure. As pointed out by the Commission already in 2018[33], the emergence of AI, in particular the complex enabling ecosystem and the feature of autonomous decision-making, requires a determination on the suitability of some established safety rules on and civil law questions on liability. It is therefore paramount to examine whether existing rules at EU and national level on the allocation of liability and on the conditions under which a victim is entitled to obtain compensation for damages caused by products and services driven by emerging digital technologies are still fit for purpose in light of these new challenges. Specifically, technology applied in safety-critical applications such as CAM, calls for an increasing attention

[29] Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, OJ L 349, 5.12.2014.

[30] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe (COM/2015/192 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN.

[31] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.5.2019.

[32] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136, 22.5.2019.

[33] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence in Europe (COM/2018/237 final). Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF.

on whether it should be (further) regulated, and, if so, how and to what extent. To this end, a number of initiatives have been undertaken by the EU e, namely to understand whether the framework continues to deliver an adequate level of legal certainty, or whether there are gaps to be addressed. Among these, it is recalled that, in March 2018, the Commission set up an Expert Group on Liability and New Technologies, operating in two different formations: the Product Liability Directive formation and the New Technologies Formation ("**NTF**"). The NTF was asked to examine whether the current liability regimes are still *'adequate to facilitate the uptake of … new technologies by fostering investment stability and users' trust'*[34]. As a result of its activity, a report was published by the Commission in 2019[35], where it makes recommendations to overcome identified shortcomings. Recommendations were limited to matters of extra-contractual liability, leaving aside in particular corresponding (and complementary) rules on safety and other technical standards. These will be recalled in the last chapter of this Study *[see Section IV, chapter 2]*.

Chapter 2. CONTRACTUAL LIABILITY

As noted, relations between the data chain actors, as well as with the end-user – including about allocation of liability – are likely to be regulated through contractual agreements, especially in so far as specific legislation is not yet in force.

Contractual liability is liability that one party assumes on behalf of another under a contractual agreement. Different arrangements can exist between the parties regulating responsibilities. Each of these contractual relationships may address the allocation of liability arising from particular situations and the limitation of the liability attaching to a particular party.

As a general rule, parties can freely negotiate contractually the terms of their relationships, including liability limitations or exclusions. When the opposing parties – of the driver/user aiming to obtain the possibility to act against the service provider in case of damage related to the use of the service; and of the service provider aiming to limit as much as possible his liability in case of service failure – agree on a compromise, the contract terms will become law between the parties and govern their commercial relationship.

Nonetheless, the parties' freedom to establish contractual arrangements is, to some extent, limited by contract law and case law, particularly in case of a business-to-consumer ("**B2C**") context. Mandatory statutory provisions have been enacted seeking to offset or reduce the imbalance between bargaining positions and between the rights and obligations of the parties to protect consumers.

Furthermore, contractual freedom in a business-to-business ("**B2B**") context, usually perceived to be limitless, is curtailed in certain cases and based on different grounds where the limitations of liability are considered unreasonable.

Restrictions as such may stem from EU legislation or national laws. Consequently, regulatory limits can diverge across countries; hence the knowledge of the specific national frameworks concerned would be necessary and the analysis should be conducted on a case-by-case basis. For instance, liability limitations for gross negligence are prohibited only in some countries and not in others. The effect of the exoneration clause can also differ. In contrast, some rules are widespread and valid across the EU such as the prohibition (and thus invalidation) of the limitation or exclusion of liability in cases of fraud, wilful intent, physical damage, and death.

These existing differences between Member States' contract laws are likely to generate additional cost and legal uncertainty when operating across different jurisdictions.

2.1 Rules on consumer protection in the area of contractual liability

[34] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592.
[35] Expert Group on Liability and New Technologies - New Technologies Formation (2019) Liability for Artificial Intelligence and other Emerging Digital Technologies. Available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.2019 ("**2019 NTF Report**").

By providing a common set of minimum rules of consumer law, the EU has sought to strengthen consumer confidence and reduce difficulties encountered by them in relation to a product's non-conformity with the contract. One example is the Consumer Rights Directive[36], which establishes rules on the information that needs to be provided (e.g. for distance contracts and off-premises contracts), on the right of withdrawal, and on the performance and some other aspects of B2C contracts. Article 14 of the Directive stipulates that '*the consumer shall not incur any liability as a consequence of the exercise of the right of withdrawal*'.

The Consumer Rights Directive also contains definitions on commercial guarantees, after sale customer assistance, and after-sales services, as well as provisions on information to be provided to the consumers regarding their existence and conditions.

Another relevant measure is the Unfair Terms in Consumer Contracts Directive[37], amended in 2011, on contracts concluded between a seller/supplier and a consumer, aiming to ensure that contracts concluded with consumers do not contain unfair terms. To this end, it establishes a non-exhaustive list of the terms that may be regarded as unfair. Among others, the directive considers unfair all provisions '*excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier*'[38].

2.2 New rules on contracts for digital content and digital services

The recently enacted DCD and SGD (hereinafter also "the directives") harmonise some key consumer contract law rules, which had not been regulated at EU or national level so far, thus aiming to make it easier for businesses, especially SMEs, to sell/supply digital content or digital services across the EU by eliminating key contract law-related barriers hindering cross-border trade.

Although the directives are not yet in force – they will become law in Member States by 1 July 2021 and will enforceable as of 1 January 2022 – it seems paramount to report their main features, as, for the first time, they regulate certain contractual aspects on digital content, including liability profiles when the digital content or service is not in conformity with the contract. The directives thus fill the legal gap in the consumer *acquis* at EU level, by covering aspects relating to new technologies and data services for which there were previously no rules.

To this end, they lay down common rules to be followed respectively in contracts for the **sale of goods – including goods with digital elements** – between sellers and consumers, and the **supply of digital content or services** between traders and consumers. They introduce a high level of consumer protection for paid services but also for those providing data in exchange for such a service. Provisions are mostly symmetrical, as the directives are meant to complement each other. These provisions focus on: the conformity of good, digital content or service with the contract, remedies in the event of a lack of such conformity or a failure to supply, modalities for the exercise of these remedies, modification of good, digital content or service, and seller/trader liability. Cloud computing contracts have played a particularly important role in identifying contractual problems relevant for this directive, including issues relating to liability[39].

Under the directives:

- **Digital content** means '*data which are produced and supplied in digital form*';
- **Digital service** means '*a service that allows the consumer to create, process, store or access data in digital form;* or *a service that allows the sharing of or any other interaction with data in digital form*

[36] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011.
[37] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993.
[38] Article 3 and Annex (1)(a) of the Unfair Terms in Consumer Contracts Directive.
[39] Commission's proposal COM/2015/0634 final - 2015/0287 (COD).

uploaded or created by the consumer or other users of that service'.

Both directives are based on the principle of maximum harmonisation, which means Member States cannot deviate from the requirements. However, on some aspects, certain room is foreseen for Member States to go beyond the requirements, especially in view of maintaining the level of consumer protection already applied at national level.

The directives work as '*lex generalis*' in relation to other EU acts governing a specific sector or subject matter (e.g. data protection laws); therefore the latter take precedence and prevails in case they conflict with the directives. They also do not impinge on national rules that do not specifically concern consumer contracts and provide for specific remedies for certain types of defects that were not apparent at the time of conclusion of the contract, namely national provisions which may lay down specific rules for the trader's liability for hidden defects or providing for non-contractual remedies for the consumer, in the event of lack of conformity of the digital content or digital service, against persons in previous links of the chain of transactions, or other persons that fulfil the obligations of such persons[40].

2.2.1 Scope of the directives:

The scopes of the two directives are defined in detail to ensure legal certainty, also by providing a number of practical examples in their Recitals.

- ***Objects (i.e. contractual relations) covered:***

The **DCD** applies to the supply of digital content or digital services, covering namely:

- Data produced and supplied in digital form such as operating systems, applications, and any other software (e.g. music, online video, etc.);
- Services allowing the creation, processing or storage of data in digital form or access thereto, such as software-as-a-service (SaaS) offered in cloud storage, the *continuous supply of traffic data in a navigation system*, or the continuous supply of individually adapted training plans (e.g. in a smart watch);
- Services allowing for the sharing of data (e.g. Facebook, YouTube, etc.) ;
- 'Over the top' interpersonal communication services ("OTTs"), bundle contracts and the processing of personal data are included within the scope of the directive.

The directive also includes digital content supplied through a tangible medium (e.g. DVDs, CDs, USB sticks and memory cards), as well as to the durable medium itself, provided that the tangible medium serves exclusively as a carrier of the digital content.

In contrast, if digital content or services in the aforementioned list are interconnected or embedded in a good, then the SGD applies.

The **SGD** directive covers any sales of goods (including online sales) and embraces both classic goods and goods with a digital component or element, including goods that are yet to be produced or manufactured.

As pointed out in the Recitals, the scope of application of the directive includes those goods where the digital elements have some characteristics, namely:

- Are required or essential for the goods to work (e.g. smart fridge or intelligent watch), where the absence of the incorporated or inter-connected digital content or service would prevent them from performing their functions; and
- Form part of the sales contract (or are deemed as such in case of doubts). To this end, the digital elements should either be explicitly required in the text or be understood as such because they are normal for goods of the same type (and the consumer could reasonably expect them given the nature of the goods and taking into account any public statement or advertisement made by or on behalf of

[40] See Recitals of both directives.

the seller or other persons in previous links of the chain of transactions, e.g. smart vehicle advertised as including a particular mobility application).

The SGD applies **regardless of whether the digital content is pre-installed in the good** at the moment of concluding the sales contract or whether it be installed subsequently or even downloaded on another device and is only inter-connected to the good in question (e.g. smart watch performing its functions only with an application that is provided under the sales contract but has to be downloaded by the consumer onto a smart phone: the application would then be the inter-connected digital element). If the installation of the goods forms part of the sales contract, it has to be carried out under the seller's responsibility.

The same applies **if the incorporated or inter-connected digital content or service is not supplied by the seller itself but rather, under the sales contract, by a third party**, and regardless any licensing agreement with a third party which the consumer has to consent in order to benefit from the digital content or service.

Where the two prerequisites above are not fulfilled – the good can function n without the digital element or the digital element is not part of the contract – the contract for the supply of digital content/service is considered to be separate from the contract, even if the seller acts as an intermediary of that second contract with the third party supplier. This case could fall instead within the scope of the DCD.

Some examples to illustrate this are provided in the directives themselves where it is explained that if the consumer downloads a game application from an app store onto a smart phone, the contract for the supply of the game application is separate from the contract for the sale of the smart phone itself. The SGD will only apply to the sales contract concerning the smart phone, while the supply of the game application would fall under the DCD. Another example would be where it is expressly agreed that the consumer buys a good without a specific operating system and subsequently concludes a contract for the supply of an operating system from a third party. In such a case, the supply of the separately bought operating system would not form part of the sales contract and therefore would fall within the scope of the DCD.

Where a contract includes elements of both sales of goods and provision of services, it is left to national law to determine whether the whole contract can be classified as a sales contract within the meaning of the SGD.

Below is a summary box on the scope of the new rules:

Within the scope of DCD	Within the scope of SGD
• Consumer contracts for the supply of digital content or digital services, where the consumer: a) pays or undertakes to pay a price and/or b) provides or undertakes to provide personal data to the trader (except where the trader does not process this data for any purpose other than supplying the digital content or service or for	• Sale contracts with consumers, including contracts for the supply of goods to be manufactured. • Digital content or digital services which are: a) incorporated in or inter-connected with goods (i.e. tangible movable items) in such a way that the absence of that digital content service would prevent the goods from performing their

complying with legal requirements to which he is subject). • Any tangible medium which serves exclusively as a carrier of digital content. • In cases where the digital content or digital service is developed in accordance with the consumer's specifications.	functions and b) provided with the goods under a sales contract concerning those goods, irrespective of whether such digital content or digital service is supplied by the seller or by a third party. (In the event of doubt as to whether the supply of incorporated or inter-connected digital content or service forms part of the sales contract, the digital content or service is presumed to be covered by the sales contract).
Outside the scope of DCD	**Outside the scope of SGD**
• Contracts covered by the SGD; • Contracts regarding the provision of services other than digital services, regardless of whether digital forms or means are used to produce the output of the service or to deliver or transmit it to the consumer; • Contracts regarding electronic communications service[41], with the exception of number-independent interpersonal communications services[42]; • Contracts regarding healthcare[43]; • Contracts regarding gambling services[44]; • Contracts regarding financial services[45]; • Contracts regarding software offered by the trader under a free and open-source licence, where the consumer does not pay a price and the personal data provided by the consumer is exclusively processed by the trader for the purpose of improving the security, compatibility or interoperability of that specific software; • Contracts regarding the supply of digital content where the digital content is made available to the general public other than by signal transmission as a part of a performance or event, such as digital cinematographic projections; • Contracts regarding digital content provided in accordance with Directive 2003/98/EC on the re-use of public sector information by public sector bodies of the Member States. • Contracts between the same parties including also bundled provision of other non digital services or goods, as far as these non-digital elements are concerned.	• Contracts covered by the DCD; • Any tangible medium which serves exclusively as a carrier for digital content; • Any goods sold by way of execution or otherwise by authority of law. • Second-hand goods sold at public auction (optional); • Living animals (optional).

[41] In the meaning of Article 2(4) of Directive (EU) 2018/1972: "a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services: (i) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120; (b) interpersonal communications service; and (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting."

[42] In the meaning of Article 2(7) of Directive (EU) 2018/1972: "an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans".

[43] In the meaning of Article 3(a) of Directive 2011/24/EU: "health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices".

[44] Namely, "services that involve wagering a stake with pecuniary value in games of chance, including those with an element of skill, such as lotteries, casino games, poker games and betting transactions, by electronic means or any other technology for facilitating communication and at the individual request of a recipient of such services" (Article 3(5)(d) of Directive (EU) 2019/770).

[45] In the meaning of Article 2(b) of Directive 2002/65/EC: "any service of a banking, credit, insurance, personal pension, investment or payment nature".

- ***Subjects (i.e. contractual parties) covered:***

As to the parties concerned, globally, the new provisions regulate the contractual relationship between consumers and sellers/traders (i.e. '*any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered*'). It is observed that platform providers could allso be considered to be sellers/traders under the directives if they act for purposes relating to their own business, and as the direct contractual partner of the consumer for the supply of digital content or a digital service[46].

However, in implementing the directives, Member States remain free to **extend their application to contracts that are in principle excluded from the scope;** for instance to platform providers that do not fulfil the requirements to be considered a 'trader' or 'seller' , to regulate liability claims of a consumer against a third party other than a seller/trader that supplies or undertakes to supply the digital content service such as a developer (which is not at the same time the trader under the directive), or by extending the protection afforded to consumers to natural or legal persons that are not consumers[47].

2.2.2 Obligations of the seller/trader

Acknowledging that there are various ways to supply digital content or services to consumers, the directives set rules as to the modalities and the time for performing the seller/trader's main contractual: making the digital content or service available or accessible to the consumer.

The good, digital content or service should comply with the requirements agreed between the parties in the contract. The directives hence identify some conformity requirements[48], such as functionality, compatibility, interoperability, quality, customer assistance, fitness for purpose, performance, quantity, etc. In addition, the SGD recalls that the **commercial guarantee** terms constitute an undertaking that is additional to the legal guarantee of conformity and stresses that producers (i.e. manufacturer, importers or any person placing his name, trademark or other sign on goods) or sellers are bound by any commercial guarantee statements and associated advertising[49] and will hence be directly liable to consumers under such guarantee for repair or replacement of the goods during the guarantee period.

Particularly, regarding commercial guarantees, the SGD aims to integrate the pre-contractual information requirements set out in the Consumer Rights Directive *[see above in this Section 2.1]* in order to improve legal certainty and to avoid consumers being misled. To this end, it is stipulated that where commercial guarantee conditions contained in associated advertisements are more favourable to the consumer than those included in the guarantee statement, the more advantageous conditions prevail. It also provides rules on the content of the guarantee statement and on the way it should be made available to consumers. Therefore, any undertaking by the seller or producer which falls under the definition of commercial guarantee needs to comply with the harmonised rules of the SGD, while rules on associating debtors other than the guarantor are left to national laws, provided that they ensure a comparable level of consumer protection.

Given that digital content and services are constantly developing, the trader/seller is obliged to ensure that the consumer is informed of and supplied with **updates**, including security updates, that are necessary to keep the digital content or service in conformity, for a set period of time.

---

[46] See Recital 18 of DCD.
[47] See Recitals 13 and 16 of DCD.
[48] Articles 6 to 8 of DCD and Articles 5 to 7 of SGD.
[49] Article 17 of SGD, where 'commercial guarantee' is defined (Art. 2(12)) as "any undertaking by the seller or a producer (the guarantor) to the consumer, in addition to the seller's legal obligation relating to the guarantee of conformity, to reimburse the price paid or to replace, repair or service goods in any way if they do not meet the specifications or any other requirements not related to conformity set out in the guarantee statement or in the relevant advertising available at the time of, or before the conclusion of the contract". An equivalent definition is codified in Consumer Rights Directive, above.

2.2.3 Liability of the seller/trader and right to redress

Specific rules govern the trader's/seller's liability for failure to supply the digital content or service and for lack of conformity[50]. Under the DCD, such lack of conformity may also result from the incorrect integration of the digital content or service into the consumer's digital environment.

The **minimum guarantee period** after supply or delivery of the good with the digital element, during which the trader/seller can be held liable, cannot be shorter than two years. This means that the trader is for any lack of conformity that occurs or becomes apparent within the two-year period from the time of supply or delivery and the consumer must be put in a position to exercise his rights in relation to the lack of conformity apparent over that time. In case of continuous supply for more than two years, the trader/seller is responsible for the entire period during which the digital content or service is to be supplied. The EU leaves Member States the choice to maintain these guarantee time limits or to introduce longer ones.

The trader is free from liability for lack of conformity if the consumer fails to install necessary updates, within a reasonable time, provided that the lack of conformity results solely from the lack of the relevant update and that the consumer had been duly informed.

The DCD leaves to Member States the option to regulate the liability of the trader in the event of force majeure (i.e. consequences of a failure to supply, or of a lack of conformity of digital content or a digital service), where such failure is due to an **impediment beyond the control of the trader** and where the trader could not be expected to have avoided or overcome the impediment nor its consequences[51].

In case of failure to supply or lack of conformity, the consumer is provided with some remedies (e.g. termination of the contract with reimbursement of the price, proportionate reduction of price). The new rules foresee in particular that, if it is not possible to fix defects within a reasonable amount of time, the consumer is entitled to a price reduction or full reimbursement. In addition, rules on the consequences of contract termination, in terms of obligations on both parties, are provided[52].

Where the trader/seller is liable to the consumer because of issues resulting from an act or omission – including omitting to provide updates – by a person in previous links in the chain of transactions, the seller/trader has a **right of redress against the persons liable in the chain of commercial transactions**, meaning that he is entitled to pursue legal remedies against them. Such remedies are determined by national laws[53].

Finally, considering that the trader is not in principle responsible for acts or omissions of a third party which operates a **physical or virtual facility**, such as an electronic platform or a cloud storage facility, that the consumer selects for receiving or storing the digital content or digital service, it should be sufficient for the trader to supply the digital content or service to that third party. However, the physical or virtual facility cannot be considered to be chosen by the consumer if it is under the trader's control or is contractually linked to the trader, or where the choice was the only one offered by the trader to receive or access the digital content or service. If the choice of physical or virtual facility is not attributable to the consumer, then the trader has not discharged their obligation should it be supplied via a physical or virtual facility of which the consumer cannot receive or access. [54].

2.2.4 Burden of proof

The burden of proof on whether the digital content or service was supplied and/or conforms is in principle on the seller/trader any time when the defects (lack of conformity) become apparent within a period of one year from supply of the service or delivery of the good or become apparent during the period of supply.

Article 11 of the SGD specifies that when the lack of conformity becomes apparent within one year, there is a

[50] Article 11 of DCD and Article 10 of SGD.
[51] See Recital 14 of DCD.
[52] Articles 13 to 18 of DCD and 13 to 16 of SGD.
[53] Article 20 of DCD and Article 18 of SGD.
[54] See Recital 41 of DCD.

legal presumption that the defect had existed already at the time when the goods were delivered, unless proved otherwise or unless this presumption is incompatible with the nature of the goods or with the nature of the lack of conformity. It also provides for the possibility for national implementing laws to extend such period up to two years.

Article 12 of the DCD envisages some exceptions where the burden of proofs falls on the consumer (e.g. if the trader demonstrates that the digital environment of the consumer was not compatible with the technical requirements of the digital content or service and the consumer was duly informed of that, or if the consumer fails to cooperate with the trader in order to ascertain that).

Chapter 3. EXTRA-CONTRACTUAL LIABILITY

Liability does not necessarily require there to be a contractual relationship between the parties. It can arise from specific legislation ('statutory liability') or where injury or damage is caused because the conduct of a person or organization falls below a reasonable standard ('fault-based liability'), being governed by general civil law rules.

Extra-contractual liability relates to the civil law responsibility for damage caused outside the context of a contract, the damage being caused by a violation of a right or legitimate interest protected by law. Although there are disparities between jurisdictions as to the principles and procedures that are applied, all EU Member States provide for some form of extra-contractual liability, which can be fault-based (intentional or by a negligent act/omission) or strict:

- **Fault-based liability**: As a general rule, in most Member States, extra-contractual liability regimes are fault-based. This implies that the fault of the author of a wrongful behaviour leading to damage is a necessary element to be proven for the liability claim to be successful. It is typically up to the victim submitting a claim to provide the evidence needed to support their liability claim. Under fault-based liability, the pivotal point is that the tortfeasor's objectionable and avoidable behaviour caused the damage.
- **Strict liability (i.e. liability without fault or liability *in re ipsa*)**: Strict liability is defined as a liability that does not depend on fault or negligence of the respondent. The claimant only needs to prove the damage occurred and the causal link with an event/circumstance. Some forms of strict liability may go even a step further by linking liability simply to the materialization of a risk or making the discharge of liability either impossible or possible only under the proof that the damaging event was caused by an exceptional/unforeseen circumstance that could not be avoided. Some basic policy arguments are given for the imposition of strict liability: the common rationale to which these regimes typically respond to is that the legislator considers it too unbalanced to apply the ordinary regime of proof and wishes to increase the possibility of compensation of the victim, by removing the plaintiff/victim's burden of proving specific acts of negligence (so-called *corrective justice argument*). This is in turn justified as another person (to be held responsible) is in a better position to bear the loss and to protect against the risk, since this person exposed others to the risks of an activity from which he benefited, and which was under his control (so-called *right incentives to avoid harm argument*). The person who controls a risk and its extent (e.g. the owner of a building for damage caused by its downfall or the owner or guardian of an animal for damage caused by the latter) is indeed the cheapest cost avoider or the cheapest taker of insurance. Strict liability has been hence developed as a vehicle of social policy and is geared toward the protection of the public safety. Based on these theories, in most countries, legislators have decided to codify types of situations where a person is deemed liable on the grounds they have not activately sought to impede the realization of a risk and thus avoid damage, despite being in a privileged position to do so. The fault of the liable person is therefore '*in re ipsa*'.

Some forms of strict liability are harmonised at EU level, for example damages arising from defective products – of which their producer (i.e. manufacturer, seller) is held responsible. Product liability is therefore a form of

statutory extra-contractual liability referring to the civil liability of manufacturers. Although existing regimes regulating product liability are not specifically tailored for damages caused by new or disruptive technologies, they '*certainly constitute helpful precedents or points of reference to which one can turn to further a reflection about how to best address, from a normative standpoint, certain distinguishing elements of risks and damages created by the emerging digital technologies*'[55]. This is why they will be extensively discussed in the following chapters.

3.1 Product safety and liability

Motor vehicles consist of highly technical complex systems that must be in strict compliance with road safety regulations, product safety and quality standards.

The EU has high standards in terms of safety and product liability. The framework of reference is the result of several layers of legislation, which aim to protect consumers from damages caused by products. This framework is made up of complementary provisions namely:

- The **EU Product Safety Legislation**, both general and sectorial, which seeks to avoid *ex ante* the verification of damages, by addressing the marketing of safe products to ensure that only safe products are place on the EU internal market. In this context, a harmonised solid body of standards has been developed, providing a presumption of conformity with EU safety legislation. This framework is complemented by the contractual obligations and the commercial guarantees available to consumers *[see above in this section, chapter 2]*, with some rules on cyber-security *[see below in this section, chapter 4]*, as well as the specific technical solutions for safe and secure vehicles *[see above in Section I, chapter 2.5]*, which all co-exist with the applicability of EU directives. Moreover, and specifically focused on motor vehicle safety, the Type Approval Regulation set important EU-wide rules on technical requirements and procedures to ensure that new types of vehicles conform to EU-approved requirements on safety and environmental protection.
- The **Product Liability Directive**[56] **(PLD)**, which comes into play *ex post* when, despite safety rules and standards, the product exhibits defects that have led to a specific damage or injury. It provides for a strict liability regime of producers of defective products that cause damage to natural persons or their property. The regime further includes a 'cascade' system in order to ensure that the injured person can bring theirclaim.

3.1.1 EU Product Safety Legislation

EU Product Safety Legislation aims to ensure that only safe products can be placed on the EU internal market. All products marketed in the EU are covered either partly or fully by safety rules. These include both general and sectorial legislation (covering specific product groups such as toys, electrical and electronic goods, machines, food, medical devices, medicinal products). In some cases, such pieces of law have liability components that, to some extent, overlap with the PLD. More often, they do not contain specific provisions on liability, but expressly refer to the application of the PLD in case of damages caused by a defective product covered by the directive.

Overall, these instruments not only establish the essential technical requirements for products to be deemed safe and commercialized, but also set out specific obligations in the development, marketing and commercialization, and the duties they hold both against consumers, as well as authorities. As a result, when the product is placed on the market or brought into use for the first time, **designers** and **manufacturers** must meet all essential requirements relevant to the specific product based on the state of the art. Relevant national authorities check whether products are compliant. Once the product is placed on the market, producers and

[55] Commission Staff Working Document, Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe (SWD/2018/137 final). Available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137.

[56] 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 OJ L 210, 7.8.1985.

distributors also have the legal obligation to immediately inform the competent authorities and take all the necessary measures – even recalling the product if needed – if they become aware that it poses any risks to the consumer (Articles 5(3) and 8 of General Product Safety Directive 2001/95[57]).

3.1.1.1 General Product Safety Directive

The General Product Safety Directive ("**GPSD**") and the Regulation on the type-approval requirements for motor vehicles[58] define the safety obligations of manufacturers for both before and after the appearance and availability of products on the market.

Specifically, the GPSD sets a broad-based legislative framework with the objective of covering a sector-specific *lacunae* and complementing the provisions of existing or forthcoming legislation related to product safety. It establishes a general obligation upon manufacturers (i.e. producers) to ensure that products, which do not fall within the scope of complementing sector specific legislation, are manufactured in compliance with the general state-of-the-art safety requirements provided therein. It hence works as a *lex generalis* in relation to more specific regimes under EU sectorial safety laws, which work as *lex specialis*.

The GPSD set obligations for both the producers and distributors:

- Producers shall only place products on the market which are safe, inform consumers of any risks associated with these products, ensure any dangerous product presented on the market can be traced, and eventually removed to avoid any risks to consumers.
- Distributors shall act with due care to help ensuring compliance with the applicable safety requirements, participate in the monitoring of the safety of the products, and cooperate with producers and the competent authorities.

Under the directive, a product is safe when under **normal or reasonably foreseeable conditions of use**, including duration and, where applicable, putting into service, installation and maintenance requirements, it does not present any risks or only the **minimum risks compatible with the product use**, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account particular aspects such as: (a) the characteristics of the product; (b) the effect on other products; (c) the presentation of the product; (d) the categories of consumers at risk when using the product.

The concept of defectiveness under the GPSD is therefore the lack of the safety which a person is entitled to expect, thus including the expectation that the products placed on the market do not present risks for the physical safety and health of persons (Art. 2(3)). It is argued that the concept of 'safety' on which the GPSD is based appears to be narrow, and risks failing to protect consumers from the risk of security breaches commonly associated with connected devices. In this regard, a Combined Evaluation Roadmap/Inception Impact Assessment to undertake a Revision of GPSD has been published by the Commission (DG JUST), specifically focusing on updating the legislation to accommodate new technologies, such as AI and digitalisation.

- ***Applicability to GPSD to data and software applications***

The relevance of GPSD for data and software applications has been discussed in legal literature[59]. The GPSD applies to products that are supplied or made available to consumers (and thus not to professional users and businesses) in the framework of service provision for use by them.

Pure information and digital data as such fall outside the scope of the directive. However, material items that use and integrate those data seem affected by the application of the directive.

[57] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002.
[58] Regulation (EU) 2019/2144.
[59] See e.g. 2018 Deloitte Study; and TNO, 2019, Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems, Final Study Report regarding CAD/CCAM and Industrial Robots, ("2019 TNO Study"). Available at: http://publications.europa.eu/resource/cellar/aad6a287-5523-11e9-a8ed-01aa75ed71a1.0001.01/DOC_1.

As to software applications, it has to be seen if they can be considered manufactured products, which, at the time being is not easily solved[60]. In the case of CAM, complexity is given by the possible presence of both a software that controls basic functions of the vehicle and the accompanied software applications that communicate with the vehicle. In case of malfunctioning software in or connected to the vehicle, one of the questions that arise is under which scheme or directive this would fall.

According to the TNO 2019 Study, presuming an application can be considered to be a product that is sold or offered against remuneration, it could fall under the GPSD. However, even if a product can relate to providing a service, it still remains to be seen whether the service provides a separate product (such as a navigation app) as part of a more extensive package, or whether the service itself should be seen as a product. Another argument used by the study is based on the presence of a producer of a software, the person or organization responsible for the design and construction of the software and the accompanying service (usually an information society service, according to the e-Commerce Directive 2000/13/EC).

In any case, the GPSD does not contain any provisions on the consequences of damage and ensuing liability for producers and product distributors.

3.1.1.2 Sector specific safety legislation

Only selected EU sector specific safety legislation which may be relevant for the purpose of the current Study is briefly described below:

- **Radio Equipment Directive** (Directive 2014/53/EU): Provides essential requirements regarding safety and health for electric and electronic equipment receiving radio waves. It aims to ensure the electromagnetic compatibility between products and the efficient use of the radio spectrum. It applies to all products using the radio frequency spectrum including embedded software.
- **Low Voltage Directive** (Directive 2014/35/EU)[61]: Ensures that electrical equipment within certain voltage limits provides a high level of protection to the health and safety to citizens in the EU market. It covers a wide range of consumer and professional products such as household appliances and cables, power supply units, laser equipment, and some components such as fuses.
- **Machinery Directive** (Directive (EC) 2006/42)[62]: Ensures a high level of health and safety for consumers, users, and other exposed persons as regards the products in its scope placed on the market. It covers a wide range of machines and equipment for consumers and for commercial or industrial purposes. It is also the relevant safety legislation for robots. The directive does not address cybersecurity issues related to ICT products. AI and IoT are the two main triggers for the revision of the directive expected in 2021. The revision will update the health and safety requirements for machinery devices implementing these technologies.
- **Motor Insurance Directive** (Directive 2009/103/EC)[63]: Includes well established rules that govern liability insurance with regard to damage caused by the use of a motor vehicle, although without touching upon liability for the accidents themselves. The directive requires all motor vehicles in the EU to be covered by minimum compulsory third party liability insurance and regulates compensation of local victims of accidents caused by vehicles from another EU country as well as claims arising from accidents occurring outside the victim's EU country of residence. While it mentions liability, the directive only harmonises liability insurance, while issues of civil liability including compensation awards

[60] It is recalled a statement of the Commission provided in a different context, where the Commission warned that "due to the fact that both the GPSD and the PDL apply to manufactured products, it is not yet clear if and to what extent they apply to lifestyle and wellbeing apps." This will be further discussed in the following of this Study.

[61] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits, OJ L 96, 29.3.2014.

[62] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), OJ L 157, 9.6.2006.

[63] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability, OJ L 263, 7.10.2009.

and 'comprehensive cover' for physical injury of the driver or damage to vehicles remain outside its scope and are instead decided by the Member States themselves.

3.1.2 Type Approval Regulation

Type Approval Regulation of 2018, applicable since September 2020, contains EU approval and market surveillance measures for new motor vehicles, which update already existing measures formerly set in 2007. Notably, the framework on type approval lays down EU-wide requirements for market surveillance in the automotive sector and the administrative provisions and technical requirements for placing on the market/entry into service all new vehicles and their parts (i.e. systems, components and separate technical units, parts, equipment), **including those that can be fitted to or in a vehicle after it has been placed on the market, registered or entered into service** and may pose a serious risk to the correct functioning of the essential systems of the vehicles.

Pursuant to this act, manufacturers shall hence ensure that the vehicles, systems, components and separate technical units that they have manufactured and that are placed on the market are compliant with specific technical and administrative requirements. Compliance is attested by EU type-approval certificates that manufacturers apply for and checked by relevant authorities.

The procedure whereby an approval authority certifies that vehicle or an element of it satisfies the relevant administrative provisions and technical requirements is called 'type approval' and can assume different forms (e.g. step-by-step, single step, mixed) and can concern either the whole vehicle or one of its comprising elements.

The directly applicable regulation takes into account the technical progress and introduction of new methods or techniques for vehicle diagnostics and repair, such as **remote access** to vehicle information and software. It also notes the particular importance of in-service conformity testing and inspections of vehicles in the context of compliance verification procedures. The selection of the vehicles that are to be subject to compliance verification is based on an appropriate risk assessment which takes into account, among other things, the introduction of vehicles with new technology installed. Compared to the previous framework, the new measures seek to complement the type-approval requirements by introducing market surveillance provisions in the automotive sector, specifying the obligations of the economic operators in the supply chain, the responsibilities of the enforcement authorities, and the measures to be taken when automotive products are encountered on the market that represent serious safety or environmental risks.

Most of the obligations set in the Type Approval Regulation concern manufacturers, or manufacturer's representatives, importers, and distributors. Particularly, manufacturers are responsible for:

- all aspects of the approval procedure and ensuring conformity of production.
- the approval and conformity of production of the systems, components, or separate technical units that they have added at the stage of vehicle completion.
- the type-approval and conformity of production of the modified components, systems, or separate technical units already approved at earlier stages (before modification).
- providing information to manufacturers of the subsequent stage regarding any change that may affect approval of the whole-vehicle or its part.
- **ensuring that their vehicles or vehicle parts are not designed to incorporate strategies or other means that alter the performance exhibited during test procedures in such a way that they do not comply with the Regulation when operating under conditions that can reasonably be expected in normal operation**.
- examining any complaints they receive relating to risks, suspected incidents, or non-compliance issues with the vehicles, systems, components, separate technical units, parts and equipment that they have placed on the market.
- implementing corrective measures if their products are not in conformity with the Regulation or that present a serious risk.
- making available some data to ISPs and other independent operators, without prejudice to commercial secrets and personal data laws *[see below in this section, Chapter 5.1].*

When a complete vehicle is converted or modified in some of its elements after its approval, a new type-approval might be needed and manufacturers of the different stages (if different) shall exchange information to this end. It is up to the approval authority, duly informed of any relevant change occurred, to decide whether that change requires either an amendment (revision or extension) or a new type-approval. Under specific

conditions, the manufacturer may even apply for an EU type-approval in respect of a type of vehicle or vehicle's component incorporating new technologies that is incompatible with the acts listed in the Type Approval Regulation ('exemption for new technology or new concept')[64].

3.2.1.1 Recent novelties in the type approval framework

The 2018 Type Approval Regulation was recently amended in 2019[65], by a new general safety regulation which updated EU vehicle safety requirements, introducing state-of-art safety technologies[66] as standard vehicle equipment and providing the first ever EU legal framework for automated and fully automated vehicles. This new Regulation will apply from July 2022.

As a consequence, manufacturers will now have to ensure that their vehicles are designed, constructed and assembled so as to minimise the risk of injury to vehicle occupants and vulnerable road users. Moreover, under their responsibility, vehicles, systems, components and separate technical units will have to comply with the applicable new requirements including those relating to on-board instruments, electrical system, vehicle lighting ,protection against unauthorised use including cyberattacks, driver and system behaviour, and general vehicle construction and features[67].

3.1.3 Product Liability Directive and related case-law

At EU level, the product liability regime was introduced by the **Product Liability Directive** ("PLD"), which aims to strike a fair balance between the risks to consumers and producers and their respective interests. The PLD frames a regime of no-fault civil liability of the producer (i.e. regardless of whether defects/damages were caused by either negligence or intention) for damage including personal injuries or death or damage to property caused by a defect in his product (Art.1).

Extensive policy and legal literature have highlighted how the acceleration of interconnectedness and autonomy of technology could challenge the product liability framework. Notably, the 2018 Deloitte Study focused on the changing complexities over the lifetime of a product that are no longer controlled by producers (e.g. autonomous, self-learning behaviour, or added software applications) and technologies that can become increasingly intangible. Against this backdrop, in 2017, the European Parliament issued a resolution with recommendations on Civil Law Rules on Robotics of February 2017[68], according to which, '*the concepts of product, producer, damage or the category of exemptions as defined in the Directive (…) could not be apt anymore when dealing with the emerging field of robotics: (…) in the scenario where a robot can take autonomous decisions, the traditional rules will not suffice to activate a robot's liability, since they would not make it possible to identify the party responsible for providing compensation and to require this party to make good the damage it has caused*'. Taking into account the EP Resolution on Civil Law Rules on Robotics and building on a Study carried out by an external contractor ("2018 PLD Study")[69], in 2018 the Commission

[64] Articles 39 and 40 of the Type Approval Regulation.

[65] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, OJ L 325, 16.12.2019.

[66] For instance, intelligent speed assistance; alcohol interlock installation facilitation; driver drowsiness and attention warning systems; advanced driver distraction warning systems; emergency stop signals; reversing detection systems; event data recorders; accurate tyre pressure monitoring; advanced emergency braking systems; emergency lane-keeping systems; enlarged head impact protection zones.

[67] Article 4 of Regulation (EU) 2019/2144.

[68] European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103/INL). Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bTA%2bP8-TA-2017-0051%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN ("**EP Resolution on Civil Law Rules on Robotics**").

[69] Technopolis Group, 2018, Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. Available at: http://publications.europa.eu/resource/cellar/d4e3e1f5-526c-11e8-be1d-01aa75ed71a1.0001.01/DOC_1.

published an evaluation of the PLD and its application, functioning, and performance ("Commission evaluation").

According to the Better Regulation principles, the Commission's evaluation assessed the effectiveness, efficiency, coherence, relevance and EU added value of the PLD and investigated whether it remains fit-for-purpose vis-à-vis emerging digital technologies such as the IoT and autonomous systems and to what extent it has been used in Member States for these purposes, albeit with limited findings. Additionally, the PLD and the GPSD are currently subject to a parallel impact assessment given the need to update both pieces of legislation to accommodate new technologies and the risks associated with their integration into products, as well as services linked to products. The next paragraphs therefore outline the main characteristics of the PLD, taking into account the on-going debate and the discussed options for the upcoming amendment of the directive.

- ***Burden of proof:***

The burden of proof is the central component of the PLD that triggers the right for compensation. In terms of procedural law, liability without fault entails a functional equivalence between the defect and the fault. The injured party who brings the claim against the producer carries the burden of proof, providing evidence on (Art. 4):

- the existence of a defect in the product,
- the actual damage and,
- the causal link between the defect and the damage.

The burden of proof under the PLD has raised significant concerns mostly among **consumers**. This is because 'defectiveness' as laid down in the PLD, as well as the causal link between the defect and the damage, have proven technically difficult to prove by the claimant, especially in cases of complex products.

Difficulties often pertain to the need for consumers to acquire an expert technician's opinion in order to properly assess the damage and causal link, or to accede information on the functioning of the product, which the manufacturers have no interest in disclosing. Such difficulties have been only partially smoothened by a number of the courts' rulings.

In recent years, the EU Court of Justice ("ECJ") and national courts have played an important role in mitigating burden of proof-related difficulties. Rather plaintiff-friendly case law has been delivered, implicitly reversing the burden of proof on a number of occasions and loosening the causal link required to establish product liability. This has led to manufacturers having to demonstrate that their products were compliant rather than the plaintiffs demonstrating the opposite.

While rulings on this matter have mostly concerned claims in the pharmaceutical sector, they can also be applied, to some extent, in other field, such as that of mobility.

Inter alia, the ECJ ruled that:

- Where a product belongs to the same group or forms part of the same production series having a potential defect, they may be classified as defective without any need to establish the defect of the individual product. The cost of the operation that is necessary to remove such a potentially defective product is considered damage within the meaning of the Directive (Cases C-503/13 and C-504/13[70]).
- National rules that make it easier for the injured person to establish the liability of the producer by granting consumers the right to require the manufacturer of a product to provide them with information on the adverse effects of that product can be accepted as they fall outside the scope of the PLD (Case C-310/13[71]).
- The requested proof could be facilitated by accepting national evidentiary rules according to which certain factual evidence may constitute serious, specific, and consistent evidence of a defect of a product and the causal link with the damage, even if there is no conclusive scientific evidence to the matter, as long as this method should not nevertheless result in a reversal of the burden of proof. The ECJ underlines the principle of effectiveness, which requires that national procedural rules do not render practically impossible or excessively difficult the exercise of rights conferred by EU law. Yet, such rules must not undermine the apportionment of the burden of proof established in the PLD. Thus, circumstantial evidence may be allowed in certain cases, to establish such the causal link, and alleviate the plaintiff's

[70] ECJ, Judgement of 5 March 2015, Joint Cases C-503/13 and C-504/13, Boston Scientific Medizintechnik, ECLI:EU:C:2015:148.
[71] ECJ, Judgement of 20 November 2014, Case C-310/13, Novo Nordick Pharma, ECLI:EU:C:2014:2385.

burden of proof. This is assessed on a case-by-case basis and provided that the burden of proof is not practically reversed (Case C-621/15).

It has been argued that this case law, if unchanged, could lead to a system where the manufacturer's liability would be at stake each time it is believed that the technology attached to the product could not really be controlled by the user, eventually resulting in multiplication of litigation and deterring producers from innovating[72].

- ***Time limits:***

A limitation period of **three years**, from the day on which the plaintiff became aware, or should reasonably have become aware, of the damage, the defect and the identity of the produce, shall apply to proceedings for the recovery of damages (Art. 10). In any case, the rights conferred upon the injured person expire after **ten years** from the date on which the producer put the defective product into circulation (Art. 11). This 10-year period is mainly explained by the fact that it balances the higher burden that strict liability puts on producers compared to fault-based liability.

The ECJ has clarified that the expiration 10-year term starts from the moment when the product has been put into circulation by the producer and not by the retailer (Case C-45/13[73]).

- ***Defectiveness and damage:***

Pursuant to Art. 6, a product is 'defective' when it does not provide the safety a person is entitled to expect, taking all circumstances into account, including the presentation of the product, the reasonably expected use, and the time when the product was put into circulation. As pointed out in the Commission's evaluation, this means that a product may not be considered defective for the sole reason that a better product is subsequently put into circulation and it is irrelevant whether the product is fit for purpose or fit for use. Issues of fitness for use pertain to the rules related to the sale of goods, outside of the scope of the PDL.

On the other hand, 'damage', pursuant to Art. 9, covers:

- (a) any damage caused by death or by personal injuries, and
- (b) any damage to, or destruction of, any item of property, provided that:
  - it was intended and used for private use and consumption;
  - it does not exceed 500 euros (the set threshold is meant to avoid litigation in an excessive number of cases);
  - it is a different item from the defective product itself;
  - it is ordinarily intended and used by the injured person mainly for private use or consumption (this excludes therefore damage caused to business property, such as a company car).

The ECJ has observed that the PLD does not preclude the interpretation and application of national law and settled case-law according to which an injured person can seek compensation for damage to an item of property intended for professional use and employed for that purpose (Case C-285/08[74]).

The distinction between professional and private use of products is not clearly stated in the PDL but emerges clearly in Art. 9(b). As noted in the 2018 PLD Study, it is sometimes difficult to distinguish between private and professional use of a product for the purpose of allocating liability, especially with regard to smartphones, cloud technologies and connected devices. Indeed, in at least 150 cases, national courts (especially in AT, DK and FR) allowed the compensation even if the item of property was subject to professional use. On the other hand, 23 claims were rejected because the injured person did not use the product mainly for his own private use or consumption. Accordingly, the Commission noted that the continued relevance of a provision that distinguishes among product's uses is debatable.

Finally, the PLD does not foresee the compensation of **non-material damage**, although this is without prejudice

[72] S. Gallage-Alwis, 2020, Updating The EU Product Liability Directive For The Digital Era, Signature, Available at: https://www.signaturelitigation.com/updating-the-eu-product-liability-directive-for-the-digital-era-sylvie-gallage-alwis.
[73] ECJ, Judgement of 16 January 2014, Case C-45/13, Kainz, ECLI:EU:C:2014:7.
[74] ECJ, Judgment of 4 June 2009, Case C-285/08, Moteurs Leroy Somer, ECLI:EU:C:2009:351.

to national provisions awarding it.

This is also confirmed by case-law, i.e.Case C-203/99[75], where the ECJ ruled that Article 9 of the Directive is to be interpreted as meaning that a Member State may not restrict the types of material damage covered, resulting from death orpersonal injury, or from damage to or destruction of an item of property, while non-material damage whose reparation remains governed solely by national law.

The possibility to extend, in the future, the definition of damage (i.e. to cover non-material damage, economic losses, privacy infringements, environmental damage) in line with the position of many consumer associations, will depend mainly on political choices.

- ***The "producer":***

The PLD provides an all-encompassing definition of 'producer', who is potentially liable for any defect. Liability not only lies with the manufacturer of the final product, but also with the producer of any raw material or the manufacturer of a component part, and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as its producer. The term is deliberately broad so that an injured person easily can find a liable person, ranging from the producer of a product, to its first importer, a downstream supplier as well as to own-branded products.

It has been observed that new technological developments involve numerous actors in the value chain, enabling the technology to function. These span from OEMs to software producers, connectivity service providers, sensor manufacturers, owners of the object, ISPs, etc. In addition, some new products and services allow new features to be added by the user or third parties. In light of this, the Commission's evaluation questioned whether the concept of producer, as defined in the PLD, still fits with the type of responsibilities that may arise in systems encompassing software or data services. In its reasoning, the Commission noted that '*these technologies would have to correspond to certain requirements which give consumers expected safety levels and a producer putting these products into circulation ensures that they meet these expectations, - also with regards to interaction in a connected world*'. In conclusion, the Commission found that the concept of the producer as responsible for his or her products remains relevant, although there may be the need to assess the impact of changing product and service configurations on this concept to see whether it needs any further clarification.

The liability of the producer so identified in relation to the injured person shall not be limited or excluded by a provision of national law (Art. 12).

In case of an anonymous product, the supplier will be held liable unless he discloses the identity of the producer. This means that, where the producer of the product cannot be identified, each supplier of the product is treated as its producer. A mere denial of supplier that he is not the producer is insufficient unless he informs, on their own initiative and promptly, the injured person, within a reasonable time, of the identity of the producer or of their own supplier. The same applies, in the case of an imported product, if the identity of the importer is not indicated (regardless the indication of the name of the producer). In cases where two or more persons are liable for the same damage, they are all liable jointly and severally (Art. 5).

Although the producer cannot rely on absence of intention or negligence to escape liability, they can be released from strict liability where they prove the existence of one of the circumstances listed in the PLD (Art. 7). Member States are obliged to include in their transposition laws such alternative exemptions of liability, namely:

a) that he did not put the product into circulation;
b) that, having regard to circumstances, it is probable that the defect which causes the damage did not exist at the time when the product was put into circulation by them or that this defect came into being afterwards;

[75] ECJ, Jundgement of 10 May 2001, Case C-203/99, Veedfald, ECLI:EU:C:2001:258

The ECJ has clarified that a product is put into circulation when it is taken out of the manufacturing process operated by the producer and enters a marketing process in the form in which it is offered to the public in order to be used or consumed (C-127/04[76]).

c) that the product was neither manufactured by them for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business;

The ECJ has clarified that this does not extend to the case of a defective product which has been manufactured and used in the course of providing a specific (medical) service, if for such service the user (patient) is not required to pay any consideration (C-203/99).

d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities (not instead with voluntary standards);

e) that the state of scientific and technical knowledge at the time when they put the product into circulation was not such as to enable the existence of the defect to be discovered (the so-called *Development Risk Clause* or *State of the art defence*). However, the directive provides Member States with the option to exclude this defence, providing that the producer is liable even if they proves that the state of scientific and technical knowledge at the time when theu put the product into circulation was not such as to enable the existence of a defect to be discovered (five Member States have indeed adopted such an option *[see below in this Section, chapter 6.2]*).

The ECJ has clarified that the state of knowledge is to be judged objectively, taking into account what the producer is presumed to have known. Moreover, the provision is not specifically directed at the practices and safety standards in use in the industrial sector in which the producer is operating, but, unreservedly, at the state of scientific and technical knowledge, including the most advanced level of such knowledge, at the time when the product in question was put into circulation (C-300/95[77]).

f) in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.

Moreover, the liability of the producer may be reduced or disallowed when, having regard to all the circumstances, there was contributory negligence of the user (meaning that the damage is caused both by a defect in the product and by the fault of the victim). This may relate, for example, to inappropriate installation yet warned by the producer, for instance while the vehicle is in motion, installed with inappropriate settings, or installation of incompatible third party software (Art. 8(2)). However, the producer remains fully liable, although possibly entitled by national provisions of a right of contribution or recourse, when the damage is caused both by a defect in product and by the act or omission of a third party (Art. 8(1)).

Finally, the PLD does not affect any other rights an injured person may have according to the rules of the law of contractual or non-contractual liability or existing special liability systems (Art. 13).

As clarified by the ECJ, this means that Member States may not maintain a general system of product liability different from that provided for in the Directive (Case C-52/00[78]). However, other systems of contractual or non-contractual liability based on other grounds, such as fault or a warranty in respect to latent defects, may apply (Case C-183/00[79] and C-310/13).

- ***The notion of product:***

The producer responds for damage caused by a defect in their product. According to Art. 2 of the PLD, the term 'product' is defined broadly ('*movable products including electricity*'), ranging from raw materials to complex industrial products, even though incorporated into another movable or into an immovable (e.g. the airbag of a car). Accordingly, the case law shows that almost any kind of movable can be the subject of product liability. A common application of the directive has concerned motor vehicles[80].

[76] ECJ, Judgment of 9 February 2006, Case C-127/04, O' Byrne, ECLI:EU:C:2006:93.
[77] ECJ, Judgment of 29 May 1997, Case C-300/95, Commission v UK, ECLI:EU:C:1997:255.
[78] ECJ, Judgment of 24 April 2002, Case C-52/00, Commission v France, ECLI:EU:C:2002:252.
[79] ECJ, Judgment of 25 April 2002, Case C-183/00, Gonzalez Sanchez, ECLI:EU:C:2002:255.

[80] According to the information collected by the 2018 PDL Study, between 2000 and 2016, the 15% of cases of PDL application concern

The broad notion of 'product' has been certainly useful, so far, to render the legislation future proof, keeping pace with evolving technologies since 1985 without the need for continuous legislative amendments. However, the circumstance that the PLD is conceived in principle around the notion of movable products, most of which are tangible and regarded as relatively simple physical items, is making it difficult to adapt to the latest technological developments. Specifically, it seems doubtful to what extent new complex products incorporating elements of AI and non-tangible goods, now appearing on the market, may fall within the scope of the directive. Additional complication depends on the nature of new products, such as software, where they are complemented by updates or technical features subsequently installed in, and which the producer is not always able to control.

In light of these perceived difficulties, a debate is ongoing on the need for an enlargement/clarification of the concept of product, to clearly encompass (or exclude) some new technologies. This is particularly relevant where a non-tangible element is not included in the product put into circulation by the producer, but it is installed subsequently as a stand-alone feature.[81]

- ***Applicability of the PLD to services***

The understanding of the broad concept of 'product' may become less evident when there are services that affect the functioning of the product resulting in damage. Indeed, the PLD does not make any reference to the concept of service nor does it provide for any definition of services or guidance on the distinction between products and services. It solely provides for the definition of product, which, as it is, cannot be easily extended to embrace services.

In the ECJ's view (C-495/10[82]), services are excluded from the scope of the PLD. Notably, the ECJ affirmed that the directive does not cover the liability of a service provider, who, in the course of providing services, uses defective equipment or products and thereby causes damage to the recipient of the service. However, without prejudice to the responsibility of the producer, the PLD does not prevent Member States from applying also national rules under which a service provider using a defective product is liable for damage thus caused. The application of such national rules may not impair the effectiveness of the directive.

One of the main issues in relation to the rising of CAM and connected new technological developments is how to classify the (often non-tangible) devices stemming from these technologies and, notably, whether they may, or may not, be considered as 'products'. As noted in Section I, the near future is likely to produce a shift from products to services, with products increasingly coming complemented with the provision of services.

Building on the ECJ case law, some scholars[83] argue that providing data through an IoT system is a **service**, thus falling as such outside the product liability and safety regimes. Yet, the 2018 PLD Study shows that a few Member States rely on a wide interpretation of the PLD to ensure strict liability for services and intangibles too *[see below in this Section, chapter 6.3, & in Section III]*. Views and practices are hence not consistent.

Besides, it is anticipated here that with the increasing overlap between products and services, the distinction between them for the purpose of the PLD becomes difficult, as they are often sold and consumed, or somewhat bundled, together. Therefore, where damage is caused by the supply of erroneous data or by a failure to supply data, allocating liability may become unclear and claims potentially difficult to enforce. For products purchased as a bundle with related services, it is then even more challenging to understand if they are currently covered or not by the PLD.

As it emerges from the Commission's evaluation, stakeholders' views in this regard are not always consistent. In fact, some stakeholders (a minority of producers and the majority of consumers, public authorities and civil society representatives) argue that the distinction between the definitions of product and service has become obsolete and a revised PLD should also cover the damages caused by the latter, thus including new risks. By

motor vehicles.

[81] The suitability of the PLD to encompass new products is mainly discussed in Section III.

[82] ECJ, Judgment of 21 December 2011, Case C-495/10, Dutrueux, ECLI:EU:C:2011:869.

[83] See the Commission evaluation and under Section III of this Study.

contrast, most producers and businesses argue that the directive should not extend to services so as to cover these damages,[84]. In addition, most businesses consider apps, non-embedded software, and IoT components to be products for the purposes of the PLD. Overall, and consistently with the Commission's findings on the PLD's effectiveness, a clarification of what is covered by the directive, and the difference between product and service for the purpose of the PLD, seems necessary to ensure legal certainty.

Chapter 4. REGULATORY FRAMEWORK ON SERVICES AND CYBERSECURITY

4.1 Rules on services

Existing regulatory framework on services consists of:

- The Services Directive[85] (complemented by the Professional Qualifications Directive[86] and the Proportionality Test Directive[87]);
- The Electronic communications networks and services Directives[88];
- The e-Commerce Directive[89]; and, to some extent,
- The General Data Protection Regulation[90] ("**GDPR**") *[see below in this Section, chapter 5]*

As highlighted in a recent European Parliament's resolution[91], the aforementioned acts already cover many policy aspects relevant for services that incorporate automated decision-making processes, including rules on liability. These rules, in the view of the Parliament, should apply to both traditional services and services incorporating automated decision-making processes.

The **Services Directive** establishes general provisions on the freedom of establishment for service providers and free movement of services, as well as on the quality of services. It applies to services supplied by providers, both to businesses and to consumers, offering activities that can involve both services requiring the proximity of provider and recipient, and services provided at a distance, including via the Internet. However, the directive does not expressly govern liability in service providing. It limits to say that any operator providing services involving a direct and particular health, safety or financial risk for the recipient or a third person should, in

[84] Also, the majority of producers of Internet of Things and robotics devices responding to the public consultation on Building a European Data Economy initiative answered that they have never experienced problems in the qualification of the good as a product or as a service.
[85] Directive 2006/123/EC of the European Parliament and of the Council of 12 December2006 on services in the internal market, OJ L 376, 27.12.2006.
[86] Directive 2013/55/EU of the European Parliament and of the Council of 20 November 2013 amending Directive 2005/36/EC on the recognition of professional qualifications and Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System, OJ L 354, 28.12.2013.
[87] Directive (EU) 2018/958 of the European Parliament and of the Council of 28 June 2018 on a proportionality test before adoption of new regulation of professions, OJ L 173, 9.7.2018.
[88] Directive 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC and 2002/58/EC.
[89] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000. In December 2020 a proposal for amending the e-Commerce Directive has been published. To ensure an effective harmonisation across the EU and avoid legal fragmentation, the new rules will be conceived in the form of a Regulation. With regard to the horizontal framework of the liability exemption for providers of intermediary services, it is not expected a huge change on applicable rules: while calling for an ambitious reform of the existing EU e-commerce legal framework, the proposal maintains the core principles of its liability regime reproducing the current provisions on providers' liability exemptions, as interpreted by the ECJ. See European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM/2020/825 final), 2020/0361 (COD).
[90] 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, OJ L 119, 4.5.2016.
[91] European Parliament, Resolution of 12 February 2020 on Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915 (RSP)), ("**EP resolution on Automated decision-making processes**").

principle, be covered by appropriate professional liability insurance, or by another form of guarantee which is equivalent or comparable and that, on the other hand, issues such as liability for providing incorrect or misleading information should be left to be determined by Member States. Also, the directive's scope does not include electronic communications services and networks, and associated facilities and services, with respect to matters covered by the Electronic communications networks and services directives, nor services in the field of transport.

4.1.1 e-Commerce Directive

While the Service Directive deals with the free movement of services, the e-Commerce Directive is somewhat relevant insofar as it deals with the provision of information society services[92] between Member States. However, it establishes rules principally concerning the activity and responsibilities of online intermediary service providers (such as Google, Facebook, Youtube, or any Internet intermediaries such as search engines andsocial media platforms).

For the purposes of this Study, these rules might be of some relevance only as regards as to possible data content on a website, based on which an ISP develops a service[93]. The ISP would hence act as 'recipient of the service', meaning any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible.

The directive contains, among others, measures protecting users (consumers, but also business users) by imposing specific transparency and information requirements upon information society service providers (including general information – such as name, address of establishment, etc. – commercial communications, and information to be provided in contracts concluded by electronic means).

Section 4 (Arts. 12 - 15) is specifically concerned with the liability of intermediary service providers that manage content provided by third parties using the services. The directive harmonises some conditional liability exemptions and limitation of responsibility for intermediaries, which purport to limit their exposure to pecuniary and criminal liability where they merely host (like some types of cloud services), cache or act as a 'mere conduit' (like internet service providers ensuring the very backbone of the network)[94]. Additionally, it states that when providing the aforementioned services, the service provider is neither obliged to monitor information which he transmits or stores, nor to actively to seek facts or circumstances indicating illegal activity.

While focusing on liability of intermediaries for the actions of users, the e-Commerce Directive excludes from its scope issues relating to the processing of personal data – including liability aspects stemming from that – which

[92] As defined in the Single market transparency directive, that is 'any service normally provided for remuneration, at a distance, by electronic means at the individual request of a recipient of services' meaning that 'the service is provided through the transmission of data on individual request' (see Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015).

[93] For purpose of clarity it is underscored that the acronym "ISP" is widely used also for Internet (or intermediary) service provider, and this is often the case in commentaries on the e-Commerce directive. However, under this Study the acronym "ISP" stands for independent service provider, which is the independent third party /operator offering services in the automobile aftermarket.

[94] In the first activity (mere conduit), the intermediary service provider is not liable for the information transmitted, on condition that he (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. In the second activity (caching) the intermediary service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that he (a) does not modify the information; (b) complies with conditions on access to the information; (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. In the third activity (hosting) the conditionality is two-fold: the intermediary service provider is not liable for the information stored at the request of a recipient of the service, on condition that he (a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

remain 'solely governed' by relevant data protection legislation.

4.2 Rules on Cybersecurity

To complete the framework, this subsection briefly mentions rules on cybersecurity. Broadly, cybersecurity can be defined as all the safeguards and measures adopted to defend information systems and their users against unauthorised access, attack and damage to ensure the confidentiality, integrity and availability of data. It involves preventing, detecting, responding to and recovering from cyber incidents, namely, accidental disclosures of information, attacks on businesses and infrastructure, theft of (personal) data[95].

The EU has recently sought to strengthen cybersecurity in order to increase trust in digital technologies. Nonetheless, the current EU legislative and policy framework on the matter appears to be incomplete and challenging, with fragmentation and gaps relating issues such as the IoT, and lack of reference to the balance of responsibilities between users and providers of digital products[96].

Some policy initiatives in this sense include the 2013 Cybersecurity Strategy[97], aimed to streamline the policy response of Member States to address cyber threats and risks,make the EU's digital environment the safest in the world, and following strategies (i.e. 2015 European Agenda on Security, 2015 Digital Single Market Strategy, 2016 Global Strategy).

In terms of legislation, the following can be mentioned:

- 2016 Network and Information Security Directive[98] ("**NIS Directive**") - The cornerstone of the EU cybersecurity strategy - which sets security and notification requirements for operators of essential services in critical sectors and digital service providers. The directive did not have an impact on all the manufacturers of ICT products but only on some manufacturers selling products to operators of essential services and/or digital services providers.[99]
- 2019 Cybersecurity Act[100] - Introduced the possibility for business to certify that their products fulfil EU cybersecurity standards. The act set a framework for European Cybersecurity Certificates for products, processes and services, but does not bind companies with its adoption, introducing instead a voluntary cybersecurity scheme for ICT products placed on the internal market.
- December 2020 Commission proposal[101] for a revised directive on Security of Network and Information Systems ("**NIS 2 Directive**").

Chapter 5. DATA RELATED LEGISLATION

Under EU law, data has been typically understood as information, rather than as property, thus falling outside the scope of rights applicable to tangible property. However, there is sectorial legislation that confers some protection to certain data or datasets, or lays down data sharing obligations, thus regulating to some extent the

[95] European Court of Auditors, 2019, Briefing paper: challenges to effective cybersecurity policy. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.
[96] Ibid.
[97] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN/2013/01 final).
[98] 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, OJ L 194, 19.7.2016.
[99] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN/2017/450 final).
[100] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, (Cybersecurity Act), OJ L 151, 7.6.2019.
[101] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, (COM/2020/823 final), 2020/0359 (COD). See https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

control of, access to, and the existence of other specific rights in data. The conferral of such rights does not entail the acknowledgment of a right of 'ownership' in data, but rather depends on the fact that specific characteristics of some data/information are deemed worthy of special protection. These characteristics leading to special legal protection are, for example, the fact that the data is personal and referrs to particularindividuals (data protection laws), that the data has a a commercial value (trade secrets), that the data results from intellectual original creativity (IP laws), and that the data is collected and stored with a focus on the structure and investment dedicated towards its creation (database laws).

Relevant rules are set by:

- Chapter XIV (Articles 61 to 66) of Type Approval Regulation;
- Directive EU 2016/943 ("**Trade Secrets Directive**")[102];
- Directive 2001/29/EC ("**InfoSoc Directive**")[103];
- Directive 96/9/EC ("**Database Directive**")[104];
- Directive 2009/24/EC ("**Software Directive**")[105];
- GDPR;
- Directive 2002/58/EC ("**e-Privacy Directive**")[106].

5.1 Data access pursuant to the Type Approval Regulation

For the purpose of this Study, in terms of data, a focus is placed on vehicle RMI, that is the variety of technical data relevant in the fields of repairs, mechanics, maintenance and diagnostics (e.g. maintenance history, repair history, vibration data & reports, alignment data & reports, thermography data & reports, ultrasound data & reports, vendor testing results, etc.). They have been defined for the first time under Regulation (EC) No 715/2007[107], which was subsequently replaced in 2018. The current definition is therefore now codified in the Type Approval Regulation of 2018, which explains RMI as '*all information, including all subsequent amendments and supplements thereto, that is required for diagnosing, servicing and inspecting a vehicle, preparing it for road worthiness testing, repairing, re-programming or re-initialising of a vehicle, or that is required for the remote diagnostic support of a vehicle or for the fitting on a vehicle of parts and equipment, and that is provided by the manufacturer to his authorised partners, dealers and repairers or is used by the manufacturer for the repair and maintenance purposes'*. Direct access to raw real-time data is a prerequisite for developing predictive remote repair and maintenance services[108].

Type Approval Regulation disciplines, *inter alia*, the **access to vehicle RMI and to data related to on-board diagnostic ("OBD")** systems and their interaction with other vehicle systems for ISPs acting as 'independent operators' (defined as natural or legal persons other than authorised dealers and repairers which are directly or indirectly involved in the repair and maintenance of motor vehicles, in particular repairers, manufacturers or distributors of repair equipment, tools or spare parts, **automobile clubs**, roadside assistance operators, and

[102] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016.
[103] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001.
[104] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, as amended in 2019 (by Directive (EU) 2019/790), OJ L 77, 27.3.1996.
[105] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111, 5.5.2009.
[106] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC, OJ L 201, 31.7.2002
[107] Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, OJ L 171, 29.6.2007. See Article 3(14).
[108] FIGIEFA, 2016, Memorandum presented as input during the preparation of the Commission Communication on Building a European data economy.

other authorised operators not members of the VM's distribution system)[109]. In this regard, the 2018 Regulation improves considerably the system of access to RMI, for example with (i) the continued possibility to communicate with the vehicle's technical data via the standardised on-board diagnostic connector; (ii) the inclusion into the RMI definition of information needed for preparation of vehicles for roadworthiness testing; (iii) the adaptation of the format of the RMI to the state-of-the-art, with the possibility to obtain it in an electronically processable form.

Manufacturers are required to provide easy, restriction-free, and, where possible, standardised access to vehicle information, including the complete references and available downloads of the applicable software.

Access should be granted in a non-discriminatory manner compared to that of authorised dealers and repairers and also for the purposes of manufacturing and servicing of OBD-compatible replacement or service parts and diagnostic tools and test equipment. As a novelty compared to the former regime, the current Type Approval Regulation mandates that such information be presented in an easily accessible manner in the form of machine-readable and electronically processable datasets. Also, it requires that ISPs have **access to the remote diagnosis services** used by manufacturers and authorised dealers and repairers.

Moreover, the Type Approval Regulation sets a number of additional information sharing obligations upon manufacturers, obliging them to make available training material and provide secure and remote facility to enable independent repairers, including ISPs, to complete operations that involve access to the vehicle security system. To rely on equally precise and updated data, manufacturers shall also make subsequent amendments and supplements to vehicle RMI available on their websites at the same time they are made available to authorised repairers.

To enhance vehicle safety, **access to vehicle security features** used by authorised dealers and repairers shall be made available to ISPs under protection of security technology in accordance with specific requirements in accordance with the state-of-the-art. For instance, ISPs shall be approved and authorised for this purpose on the basis of documents demonstrating that they pursue a legitimate business activity and have not been convicted of any relevant criminal activity, both manufacturers and ISPs need to use security certificates for mutual authentication, and the ISP's private key is protected by secure hardware.

For information concerning **access to secure areas of the vehicle**, the ISP shall present a certificate in accordance with an international standard to identify themselves and their organisation. In turn, the manufacturer shall respond with their own certificate to confirm to the ISP that they are accessing a legitimate site of the intended manufacturer. Both parties shall keep a log of any such transactions indicating the vehicles and changes made to them under this provision.

A **fee** for access to vehicle RMI can be charged by manufacturers provided that it is reasonable and proportionate, in other words that it does not discourage access by failing to take into account the extent to which the independent operator uses it. However, where repair and maintenance records of a vehicle are kept in a central database of the vehicle manufacturer or on its behalf, ISPs shall have access to such records free of charge and shall be able to enter information on repair and maintenance operations they have performed.

Along information sharing and other obligations imposed upon VMs, the Regulation contains communication requirements on OEMs. Notably, OEMs responsible for type-approvals of a particular system, component or separate technical unit or stage of a vehicle, shall communicate to both the final VM and the ISPs, RMI relating to such systems, components, etc. The VM remains, in any case, responsible for providing access to vehicle OBD information and RMI regarding its own manufacturing stage(s) and the link to the previous.

Finally, the Regulation notes the current lack of a common structured process for the exchange of vehicle component data between VMs and ISPs and recalls the need to develop principles for it, reflecting the interests and needs of all interested operators and investigating solutions such as open data formats described by well-defined meta-data to accommodate existing information technology infrastructures.

[109] Articles 61 et seq. of Type Approval Regulation.

5.2 IP-related rules

5.2.1 Trade Secrets Directive

The Trade Secrets Directive lays down rules on the protection against the unlawful acquisition, use, and disclosure of information, hence data, which amount to trade secrets. Both commercial and technical data could benefit from the trade secrets protection if it fulfils the criteria under the directive. The directive distinguishes between lawful (e.g. independent discovery or creation, observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is not legally required to restrict the acquisition of the trade secret; exercise of the right of workers or workers' representatives to information and consultation under EU law and national laws and practices; any other practice which, under the circumstances, conforms with honest business practices, law requirement) and unlawful (e.g. unauthorised access, stealing or copying of documents, objects, materials, substances or electronic files which are lawfully under the control of the trade secret holder; conducts contrary to honest business practices; breach of a confidentiality agreement or other requirement not to disclose; breach of a contractual or other duty to limit the use) acquisition, use, or disclosure of a trade secret.

Remedies are foreseen in case a third party uses or shares confidential information without permission or misappropriates a trade secret. Indeed, the directive mandates Member States to allow trade secret holders, victims of the illegal acquisition, use and disclosure, to apply for civil law fair, effective, and dissuasive remedies that ensure redress is available to them. Despite some room for differences among national remedies implemented, all of them shall foresee: (i) a limitation period for claims not exceeding 6 years; (ii) the award of damages; (iii) injunctions prohibiting the defendant from using or disclosing the information; and (iv) the recall of infringing goods from the market.

5.2.2 InfoSoc Directive; Database Directive; and Software Directive

Intellectual property ("**IP**") rights, and in particular copyright and database rights, can be invoked to protect, to a certain extent, non-personal and commercial data or datasets, and obtain exclusivity. The protection of the database is achieved by copyright as literary works, as set out in the Software Directive, or through database rights under the Database Directive. Database rights arise where a party has invested in obtaining, verifying or presenting the contents of the database. Copyright in databases only arises where the selection or arrangement of the contents make it the author's own intellectual creation. In both cases, the database owner would need to show that the database was more than a by-product of another process. Also, individual data, understood also here as pieces of information, should fulfil the conditions set out in the relevant legislation in order to benefit from copyright protection. These are for example, fixation in a tangible form, originality, etc. The eligibility for protection needs to be examined on a case-by-case basis and in light of the particular rules and case-law in each country.

5.3 Rules on Data Protection

On the topic of data, there are different regulations that touch upon or have a say on what can and cannot be shared or transmitted. Currently, the main pillar of the data protection legal framework in the EU is the GDPR, complemented by the e-Privacy Directive.

5.3.1 GDPR

Under the GDPR personal data can only be gathered under strict conditions and for legitimate purposes. The Regulation clarifies what constitutes personal data, identifies the main actors and sets out rights and obligations upon them, and lays down the principles, rules and procedures to be followed by any actors involved in collecting, using, and managing ("**data processing**") personal data related to individual natural persons residing in the EU, or any personal data processing by actors established in one or more EU Member States.

Almost any operations involving the use of personal data (such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) is considered by the GDPR (Art. 4(2)) as 'processing' of personal data. This is so irrespective of whether the processing is done manually, by automated means, or by autonomous systems such as AI. The definition of processing is, in fact, intentionally broad in order to cover as many types of data processing as possible.

The ECJ has clarified that data is to be considered as personal data for any company having access to the data and being able

to link such data to an individual (Case C-582/14).[110]

- ***Core principles***

When personal data is involved, it is mandatory for data controllers (meaning who, alone or jointly with others, determines the purposes and means of the processing of personal data) to abide with the seven core principles of data processing (Art. 5), which apply whenever personal data is processed, including when dealing with a mixed dataset. They are:

- *Lawfulness, fairness and transparency:* Personal data must be processed in a lawful and transparent manner, ensuring fairness transparency towards the individuals whose personal data is being processed. Personal data processing is lawful only if and to the extent at least one of the legal bases for processing set out by Art. 6 of the GDPR applies[111].
- *Purpose limitation:* Personal data may be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. There is a set of purposes, for which further processing is deemed compatible with the original purpose; these include archiving purposes in the public interest, scientific or historical research, and statistical purposes.
- *Data minimisation:* Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- *Accuracy:* Personal data must be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- *Storage limitation:* Personal data is stored for no longer than necessary for the purposes for which the data is processed. Longer keeping may be permissible for archiving purposes in the public interest, scientific or historical research, and statistical purposes.
- *Integrity and confidentiality:* Organisations handling the data must use appropriate technical and organisational measures that ensure an appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- *Accountability:* Organisations handling the data are able to and responsible for demonstrating compliance with the above principles.

- ***Other provisions***

The Regulation describes in detail the rights of the data subject, which correspond to obligations upon the data controller. Many duties concern information and communications; others are on access, rectification and erasure, restriction of processing, portability.

Specific provisions concern decision-making based solely on wholly or partly automated processing, including profiling[112]. In such cases, data subjects have the right to be provided with meaningful information about the logic involved in the decision[113]. Data subjects also have the right and not to be subject solely to automated decision-making, except in certain situations[114].

Chapter 4 of the GDPR defines the relation among and the responsibilities of the data controller and processor

[110] ECJ, Judgment of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779.
[111] Processing is lawful when, alternatively, "(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."
[112] Article 2 of the GDPR.
[113] Articles 13 (2) f), 14 (2) g) and 15 (1) h) of the GDPR.
[114] See Article 22 of the GDPR.

(i.e. who processes personal data on behalf of the controller) including, for instance, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation, or to ensure a level of security appropriate to the risk (pseudonymization and encryption, integrity), to maintain a record of processing activities, to cooperate with the supervisory authority, to carry out data protection impact assessments, and to designate a data protection officer.

- ***Liability of data controllers or processors***

Chapter 8 encompasses provisions on liability and fines or penalties: each data subject is granted the right to an effective judicial remedy where they considers that their rights have been infringed as a result of the processing of their personal data in non-compliance with the law. The competent courts for proceedings against a controller or a processor are those of the Member State where the controller or processor has an establishment, or where the data subject has their habitual residence[115].

The right to compensation and liability is defined under Art. 82: where alleged infringement of the GDPR cause material or non-material damage, the victim is entitled to compensation from the controller(s) or/and processor(s), having joint and several liability (meaning that each of them respond for the entire damage paying full compensation to the data subject)[116].

Under the provision:

- A controller (i.e. any controller involved in processing) is liable for the damage caused by processing which infringes GDPR;
- A processor (i.e. any processor involved in processing) is liable for the damage caused by processing only where:
  - they have not complied with obligations specifically directed to processors or
  - they have acted outside or contrary to lawful instructions of the controller.

Exemption from liability is possible for both of them if they prove the lack of any responsibility for the event giving rise to the damage.

A right to redress exists in case a controller or processor has paid full compensation for the damage: in such case they areentitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.

5.3.2 e-Privacy Directive

The e-Privacy Directive complements the EU data protection framework by providing a privacy protection framework for transmission and processing of data in connection with use of public communication networks (such as Internet, mobile, or telephone networks). The e-Privacy rules apply not only to personal data and data of natural persons, but to any data in electronic communications (including other traffic data and metadata) and also data of legal persons. Therefore, anonymization/de-identification removes data from the scope of the GDPR but not from that of e-Privacy rules.

In terms of interplay with the GDPR, the e-Privacy Directive is a *lex specialis* as its provisions serve to 'particularise and complement' the GDPR as regards data that qualifies as personal data, meaning that all matters concerning the processing of personal data not specifically addressed by ePrivacy rules remain governed by the GDPR.

The directive imposes obligations on providers of publicly available electronic communication services (mobile network or internet connection providers), but also to persons who make use of information related to end users' terminal equipment.

The applicability of e-Privacy provisions in the context of automated transfer of data and information between

[115] See Article 79 and 82(6) of the GDPR.
[116] Article 82(1) and (4) of the GDPR.

devices or software-based applications and IoT systems – which could be considered as 'electronic communication services' when they channel data over public networks such as the Internet – is doubtful. In general, OTTs, such as internet-based services enabling inter-personal communications (Voice over IP, instant messaging and web-based e-mail services) are not subject to the current EU electronic communications framework, including the e-Privacy Directive. Based on this void of protection of communications conveyed through new services, a proposal for a new e-Privacy Regulation was published in 2017 but, after four years, is still pending[117]. Although the proposal is undergoing a long legislative debate, it is important to keep it monitored, as, when approved, it may contain rules limiting the processing of a broad array of both personal and non-personal data, with added relevance for data-based services.

Compared to the current directive, the proposal introduces a number of changes. In the first place, the new act is in the form of a regulation, rather than a directive, thus reducing the room of country-specific differences among implementing rules.

Furthermore, the draft regulation aims to fill application gaps as regards the inclusion of machine-to-machine ("M2M") communication services and IoT services, by making it clear. The principle of confidentiality enshrined in the new e-Privacy rules will therefore also apply to the transmission of M2M communications, as the latter involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. The draft regulation also clarifies that electronic communications data should be treated as confidential, prohibiting any interference in or interception of communications data and associated metadata, whether by human intervention or through the intermediation of automated processing by machines, absent a consent of all the communicating parties. It regulates further types of data processing activities, such as use of helpful metadata for wider benefit and clarifies the rules on the use of the processing and storage capabilities of users' terminal equipment (such as automated or connected vehicles) or access to information stored in such equipment.[118]

Finally, while the current e-Privacy Directive cross-references to Directive 95/46/EC (hence, now, to GDPR) for matters of judicial remedies, liability and sanctions, the future regulation should contain a dedicated chapter with a newly designed set of penalties for infringements of e-Privacy rules. This should be without prejudice to the application of liability rules of intermediary service providers in Articles 12 to 15 of the e-Commerce Directive.

Besides, under the current framework, while most provisions deal with public communications services, which are outside the scope of this Study, Art. 5(3) of the directive, as a general provision, does not only apply to them but also to every entity, private or public, that places on or reads information from a 'terminal equipment' without regard to the nature of the data being stored or accessed. Connected vehicles and devices connected to it can be considered as a terminal equipment if they fall in the definition provided by Directive 2008/63/CE[119]. If this is the case, then the directive applies where relevant. The directive also addresses the use of **location data** for the provision of value-added services. In this regard, data subjects are to be informed about the processing

[117] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM/2017/10 final, 2017/0003 (COD)).

[118] Under the existing directive, this is only possible with the user's consent or where the user requests a provision of a service (Art. 5), while in the latest e-Privacy Regulation proposal of March 2020 (available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=EN) there should be a new legal ground for processing that is based on legitimate interest pursued by the service provider, except in some cases (e.g. processing for user profiling purposes or information that contains special categories of personal data, or other fundamental rights and freedoms of the end-user that overrides the service provider's interest). Data thus processed can only be shared with third parties if anonymised. Non-consent-based processing of equipment-emitted information should be also allowed, subject to further safeguards, in physical movements' tracking services. Other types of information processing related to terminal equipment (such as IoT-related services that need terminal equipment-emitted information to enable it to connect to another device) remain subject to end-user's consent.

[119] Pursuant to Article 1(a) of Directive Directive 2008/63/CE, 'terminal equipment' is an "equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment".

of the data and transmission to third parties, requested their consent for the processing, and enabled to withdraw it either temporarily or permanently.

Notably, Art. 5(3) provides that, as a rule, and subject to some exceptions (below), **prior consent** is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user. To the extent that the information stored in the end-user's device constitutes personal data, this provision takes precedence over Article 6 of the 6 GDPR with regards to the activity of storing or gaining access to this information. Any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must have a legal basis under Art. 6 GDPR in order to be lawful[120].

Exemptions where informed consent is not required are the storing or accessing information for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. Where criteria for the exceptions are met, the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal bases as provided the GDPR.

Chapter 6. NATIONAL RULES ON LIABILITY

This chapter provides an overview of liability regimes at national level, focusing on the implementation and application of the PLD and on the concrete applicable law in liability claims. In addition, in-depth description of liability framework in Italy, France, Spain, and Germany, with a focus on data, is provided in the annex.

6.1. General remarks

Usually, on a national level, there are no liability rules specifically applicable to damage resulting from the use of emerging technologies. Specific rules for the deployment, or even simple testing, of CAM are being enacted or discussed in some EU countries, such as Germany and the UK, leading to the revision of their respective national liability regimes. However, these mostly pertain to liability for damage caused by unmanned or autonomous vehicles.[121]

[120] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.

[121] For example, the UK (UK Automated and Electric Vehicles Act 2018 (c 18), Section 2. Available at: http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted) has revised the national liability regime by holding the insurer liable in the event of damage incurred by the insured party or any other third party in an accident involving an automated car. In case the vehicle is uninsured, however, the owner is still held responsible (see 2019 NTF Report, Ibid.). Similarly, Spain is working to expand rules for self-driving vehicles, as well as adding modifications to insurance laws to offer an overall legal framework for the technology. Additionally, in some countries, although the specific rules and regulations for the use of semi-autonomous or fully autonomous vehicles on public roads are still to be adopted, new legislative proposals have been recently submitted or approved regarding the testing of autonomous vehicles, in some cases containing specifications on liability. For example, a 2017 legislative reform introduced in Hungary (see Hungarian NFM Regulation No. 11/2017) the new legal category of "autonomous vehicle for development purposes" and laid down rules on security and liability, clarifying that operational liability for the autonomous vehicle lies with the developer of the autonomous vehicle. The same year, a new ordinance was adopted in Sweden (Swedish Ordinance (2017:309) on Trial Operation with Self-driving Vehicles that allows trial operation with self-driving vehicles to take place) conferring upon the Swedish Transport Agency the responsibility for authorising and supervising permits to carry out trials at all levels of automation on Swedish roads. Under the law, the party that has been granted such permission is legally responsible for the operation of autonomous cars and for the damages caused by such vehicles operating in self-driving mode. However, in those cases when vehicles operate at lower levels of automation or manually, criminal and civil liability is borne by the driver. Autonomous transportation remains a core topic also in the Netherlands (The Netherlands, according to KPMG second Autonomous Vehicles Readiness Index published in 2019 (https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/kpmg-2019-autonomous-vehicles-readiness-index.PDF) is the best-prepared country, among the 25 analysed, in terms of policy and legislation, technology and innovation, infrastructure and

Varying domestic rules on contractual liability and tort law hence apply, taking different forms with regard to scope, conditions and burden of proof. Given such differences in domestic frameworks, the outcome of cases might change depending on the competent jurisdiction.

In most EU countries, there is a special liability regime for accidents involving motor vehicles. As mentioned before, while liability insurance for damages caused by motor vehicles is harmonised, civil liability itself is not, hence different rules apply. Usually, when damage is caused with a vehicle, national law imposes liability on the owner/keeper of the vehicle[122] and/or on the driver, although there are systems which introduce direct claims against the insurer regardless of any other person's liability. Some jurisdictions rely on **fault-based** liability, while others adopt a **risk-based** approach, which is in general more appropriate for cases concerning AI and autonomous vehicles (AV).[123]

Another difference is that only some (most) jurisdictions allow the victim to bring **concurrent claims** based on contract and on tort alternatively, while under some others this is not possible, such as France**.** Jurisdictions that allow concurrent claims in practice shift tort cases into the realm of contractual liability (e.g. by creating 'quasi-contractual obligations') with the purpose of allowing the plaintiff to avail of the benefits of a contractual claimant.[124]

Furthermore, the **prescription periods** (i.e. time-limits to file a claim) vary. It has been observed that, in some countries, time limits are very short when it comes to extra-contractual liability claims, especially for damages caused by traffic accidents (one-year in Spain; two years in Switzerland, Greece, and Italy; three years in Croatia, Germany, Hungary, and Sweden; and three years in Luxembourg and Netherlands but limited to the insurer) even if, depending on the circumstances, longer time-limits may be applied. This may affect the rate of success of a claim involving new technologies or complex products, cutting off the claim prematurely, before the technology could be identified as the source of harm. [125]

Where damage is caused by a defective vehicle, product liability (i.e. producer's liability) may apply. As extensively described in the previous chapters, manufacturer's liability holds for cases where damage is derived from the product's use. In this regard, a degree of uniformity has been attained with the PLD (and its implementing rules), but they only pertain to certain aspects of tort law hence national tort law traditions and practice remain important. Also, in some cases (typically in systems with strict liability for motor vehicles) the liability of the producer only becomes relevant at the redress stage, as the vehicle's owner/keeper is deemed liable anyways, despite the presence of a proven defect in the vehicle. This explains why it is usually up to the motor vehicle insurer to pursue the product liability claim.

6.2 Overview of PLD implementation and application

consumer acceptance) where, in July 2019, the autonomous driving law entered into force (Dutch Experimental Law for testing self-driving vehicles on public roads of 1 July 2019) allowing, for the first time, trials of automated vehicles without a driver physically present. In terms of the allocation of liability, recent Dutch case law ruled that drivers remain fully liable when their vehicle is operating on Autopilot. Consistently, and also in line with the previous law of 2015, the new act places liability with the 'legal driver', that is the person in the driver's seat or the person operating the vehicle remotely.

[122] By way of example, France (see French Decree n° 2018-211 of 28 March 2018 on experimentation with automated vehicles on public roads which relies on the Loi Badinter of 5 July 1985 (n°85-677) (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036750342&categorieLien=id) and Germany (§ 7 of the German Road Traffic Act (Straßenverkehrsgesetz) as amended in 2017 by the Autonomous Vehicle Bill (https://www.gesetze-im-internet.de/englisch_stvg/index.html) rely on a strict liability regime for the driver (keeper) of the vehicle.

[123] As noted by the NTF, exclusion of strict liability in the case of a third party intervention may prove problematic, particularly in the context of cybersecurity risks, such as where a connected AV has been hacked, or where an accident has been caused because the ICT infrastructure sent the wrong data.

[124] As an example, AT introduced the concept of 'contract with protective duties in relation to third parties', which is used to pursue direct claims of the victims of defective products against the manufacturer alongside the strict liability regime of the PLD.

[125] Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs Legal Affairs, 2016, Cross-border traffic accidents in the EU - the potential impact of driverless cars, p.10-11. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU(2016)571362_EN.pdf; 2019 NTF Report, Ibid.

Until the adoption of the PLD in 1985, Member States had no specific legislative regime in place to protect victims o defective products but relied instead on tort law – liability of the producer based on the fact that the product was defective and damaging, upon proof of negligence from the part of the producer – or contract law. Even now, the PLD co-exists with and does not affect any rights which an injured person may have according to the laws regulating contractual or non-contractual liability as well as any other existing special liability system (Article 13 PLD). The latter may differ at national level, as each country can have its own rules on liability allocation, to the extent and within the limits they are not harmonised under existing EU directives.

The analysis of national legislation transposing the directive carried out by the Commission shows that the PLD, and its amendments brought by Directive 1999/34/EC, has been uniformly transposed in all EU countries.[126]

As noted in the 2018 PDL Study, the harmonisation of the rules and the judgments of the CJEU contributed to a harmonised environment for businesses by preventing distorted competition in the internal market and providing a level playing field across the EU. Nonetheless, in pursuance of Art. 13 PLD, which allows the co-existence of different product liability rules, national provisions implementing the PLD have been generally applied alongside other regulations on contractual, non-contractual or other types of liability. In addition, the directive leaves some matters to national law, including the ceilings for damages resulting in death or personal injury by identical items (Art. 16 (1)), the development risk defence (Art. 15.1 (b)), and the rules related to non-material damages (Art. 9).

The Commission has continuously monitored the transposition activities. Infringement proceedings have been launched in 2000 for incorrect transposition of the PLD. They concerned respectively the fact that the thresholds for material damages was lower than EUR 500 (Case C-52/00) and the grounds of a national provision providing that the supplier were liable under the same conditions than the producer (Case C-327/05[127]).

In terms of **options** adopted, only five Member States (namely FI, FR, HU, LU, ES) have adopted, although with some differences, the derogation for 'Development risk clause' under Art. 15(1)(b), providing that the producer shall be liable even if they prove that the state of scientific and technical knowledge at the time when they put the product into circulation was not such as to enable the existence of a defect to be discovered. Among these, LU and FI have decided to adopt the derogation without any limitations, thus applying it to all categories of producers and products, while the others only exclude some categories of producers and products. Notably, in LU the law does not make any distinction, hence the producer can invoke the clause for any products, regardless of their nature. In FI, according to the Government proposal regarding the enactment of the Product Liability Act and the implementation of the Directive, the extent of the derogation has not been explicitly defined yet, so it should be interpreted to apply to all products according to the PLD. In contrast, in other countries the derogation applies with some limits: In HU it does not apply to pharmaceutical products[128]; in ES it does not apply to medicinal products, foodstuffs or food products intended for human consumption[129]; in FR it does not apply to products derived from the human body[130].

In terms of complementary and additional provisions, the 2018 PLD Study found that seven Member States (EE, EL, HR, LT, LU, MT and FI) have not introduced any measures, procedures, or burden of proof provisions for the application of the Directive in addition to those expressly provided for therein, while:

- AT, BE, IT, CY, and CZ have introduced a criterion to determine when a product is 'put into circulation'.

[126] See https://eur-lex.europa.eu/search.html?DB_NATURAL_DIRECTIVE=1985,374&qid=1519146702874&DTS_DOM=NATIONAL_LAW&type=advanced&lang=en&SUBDOM_INIT=MNE&DTS_SUBDOM=MNE.

[127] ECJ, Judgement of 5 July 2007, C-327/05, Commission v Denmark, ECLI:EU:C:2007:409

[128] Pursuant to the Hungarian Civil Code states the producer of any pharmaceutical products is liable even if the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable detection of the existence of the defect.

[129] See the Spanish Royal Legislative Decree 1/2007 of 16 November 2007, under which producers of medicinal products, foods or foodstuffs intended for human consumption cannot invoke the exemption provided under Article 15 §1(b) of the PLD.

[130] See French Law n° 98-389 of 19 May 1998 modifying Art. 1386-12 of the Civil Code stating that the producer cannot invoke the exemption when the damage has been caused by an element of the human body or by products derived from it.

The precise identification of the time when a product is put into circulation has, in fact, proven difficult in some instances, especially concerning the pharmaceutical sector.

- ES, HU, PL, PT, and SE have specified the 'reasonable time' by which the supplier of the product must inform the injured person of the identity of the producer or of the person who supplied them with the product where the producer of the product cannot be identified, so as not to be treated as its producer.
- DE has specified the nature of damages that can be indemnified.
- NL has specified the term for recourse against the producer held liable for a defect.
- RO has extended the definition of producer to any person who imports from another Member State a product for sale, hire, lease or any form of distribution in the course of his business.
- DE, ES, FR, NL have interpreted the sum of EUR 500 in Article 9 as a threshold, whereas others as a deductible from the compensable damage.

As to the **application** of the PLD, the analysis conducted by the 2018 PLD Study shows that from 2000 to 2016 there have been at least 798 claims to court invoking the PLD and only one case (published), in BG, concerning new technological developments and, specifically, on damage consisting in loss of data – i.e. loss of stored information, due to defects in the external hard disk – without any material damage occurring.

The Bulgarian case[131] involved a defective product (storage unit) in which software and apps from different sources can be installed after purchase. The resulting damage was the loss of stored information due to defects in the external hard disk. However, the claimant could not provide evidence that the information had been stored on the external disk prior to the occurrence of the defect and also to prove the damages caused to him by the loss of the information.

It seems therefore that the national judge did not consider the loss of the information as a damage *per se* subject to compensation, but required instead the proof of an economic damage linked to the loss of data, confirming the exclusion of non-material damage by the scope of the (national law implementing the) PLD and endorsing a reading where data is not deemed having a value in itself.

Despite the alleged burden of proof related difficulties, especially affecting consumers, most claims have been upheld by the national courts in favour of the injured person, sometimes based on the directive, while some other times on a different legal basis such as tort law or contract law even if the claimant had invoked the PLD. The prevailing ground by far for rejecting claims, ruling instead in favour of the producer, is the claimant's failure to either prove the defect or to link it with the damage.

6.3 Rules on extra-contractual liability for damages caused by services

The 2018 PLD Study also investigated national rules on extra-contractual liability in place to protect consumers from damages caused specifically by defects of either intangibles (such as software) or services. It reported that overall, 18 Member States (AT, BE, BU, CY, CZ, DK, ES, HR, HU, IE, IT, LV, LU, PL, PT, RO, SE, UK) do not have any, while nine Member States (DE, EE, GR, FR, LT, MT, NL, SI, SK) ensure an extra-contractual liability to protect consumers from damages caused by defects both of intangibles and services (no information was found for FI).

In DE, EE, MT, NL, SI, SK and to some extent FR, the protection of consumers from damages caused by defects of either intangibles or services stems from the interpretation of general rules to include services or intangibles. In FR, in addition to the application of general rules on tort law, there are also specific sectorial rules, providing for the liability of a service provider (in the field of health), who, regardless, remains entitled to recourse against the producer when the producer is liable under the PLD[132].

In contrast, in GR and LT, legal doctrine stretches the rules set forth in the PLD implementing law to ensure strict liability of all relevant parties – i.e. the manufacturer of a finished product, the producer of any raw material, the manufacturer of a component part, the person presenting himself as the producer by putting his distinguishing feature on a product, the importer, the supplier, the software developer, the software owner, the software

[131] Bulgarian case no. 20942/2012.
[132] See ECJ Case C-495/10, above.

licence distributor, the service provider, the subcontractor of the service provider – for services and intangibles too, provided that such services are strictly relating to the products. However, the Study reports that, to date, no court cases have been registered which provide for the application of the PLD to services/intangibles. In LT the law (Civil Code) expressly regulates not only the liability for compensation for damage caused by defective products, but also by defective services, where 'service' refers to activities that meet users' specific tangible or intangible needs, with the exception of health care, legal, educational, thermal energy, gas, water supply, sewage disposal and transport services. Through this, all the PLD rules apply to such services.

Finally, for products purchased as a bundle with related services, the service part is only considered a part of the product in some Member States (in FI and LU they are considered products while this is not the case in GR, IT, MT, NL and UK). This possibly creates different levels of consumer protection and of producers' liability across the internal market.

6.4 Rules on applicable law

Due to discrepancies in Member States laws, an issue can be the identification of applicable rules and competent jurisdiction (that is the law applicable to the liability claim) in case of cross-border situations or elements (e.g. when the damage occurs in a country different from the country where the product is marketed or where the producer resides, or the user resides in a different country than the producer). EU law also therefore provides for a conflict of tort laws framework: these private international law rules are necessary to ensure legal certainty and predictability, striking a balance between the concerned parties.

The Rome II Regulation[133] sets forth the conflict-of-law rule in matters of product liability by means of a cascade system, where the first applicable law is considered the one of the country of residence of the injured party where the damage occurred, if the product was marketed in that country; otherwise the law applicable depends on the place where the product was marketed. However, this does not preclude that, where both the person claimed to be liable and the person sustaining damage have their habitual residence in the same country at the time when the damage occurs, the law of that country can apply.

The Brussels IA Regulation[134] sets rules applicable to claims under the PLD: it provides that a person domiciled in a Member State may be sued in another Member State in matters relating to tort, delict, or quasi-delict. The court with jurisdiction is the one in the country where the harmful event occurred. Where a manufacturer faces a claim of liability for a defective product, the place where the harmful event occurred (that is the place of the event giving rise to the damage) is the place where the product was manufactured[135].

In the case of consumer contracts, the applicable law is that of the Member State in which the consumer is habitually resident.

Brussels IA Regulation also applies also in the digital environment (the Regulation has, in fact, been adopted quite recently, thus the implications of the Internet were considered closely during the legislative process).

[133] Regulation (EC) no 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007.
[134] Regulation (EU) no 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012.
[135] See ECJ Case C-45/13, Ibid.

SECTION III – RULES APPLICABLE TO ISPS

After having singled out the relevant legal provisions (Section II), this section aims at interpreting and applying the identified framework, focusing on the liability incurred by ISPs in the automotive aftermarket when accessing data, especially RMI (technical information, replacement parts, multi-brand diagnostic tools and test equipment, etc.) and other information, to provide mobility services, such as remote R&M, by means of secure S-OTP.

Chapter 1. OVERVIEW AND COMPLEXITIES IN ALLOCATING LIABILITY AMONG PARTIES CONCERNED

The Section above shows that **specific tailored provisions on digital service liability are currently lacking.** As a result, if a technology failure leads to an accident, a number of legal issues arise for identifying the root cause of the damage and fairly allocating responsibility between the different operators in the value chains. Ultimately, who shall bear which risks remain **unclear** under the current framework.

To fill the legal gap, an exercise of legal interpretation is needed to extend the applicability of the available framework, regardless its sub-optimal fitness for purpose. The fact that existing product liability concepts and rules are based on tangible products whose characteristics do not change over time definitely adds a layer of complexity to this exercise. At the same time, some specificities of the context render the allocation of liability challenging, namely:

(i) Lack of precedents

In the first place, as this is an emerging market, quantitative data is lacking since there is not much experience on practically testing how R&M (as well as other similar) services will work and evolve and how liability rules might apply to the situations at issue. While there is some legal literature on related topics, judicial precedents to rely on are missing.

(ii) Characteristics of the 'product'

The fair allocation of liability could be challenging due to **specific features** of technological items such as the:

- interdependency between different layers and components interacting with each other (e.g. the tangible parts or devices, the data itself, the data services, and the connectivity features);
- modifications through updates, self-learning, or added software applications;
- limited predictability and controllability by initial producers;
- data-drivenness (i.e. reliance on external information that is not pre-installed but generated by built-in sensors);
- intangibility.

Notably, these characteristics challenge the applicability of the product liability framework and also make it difficult to apply the general principles on extra-contractual liability, normally grounded on the notion of fault: for instance, where a third party software is involved or defects are linked to additions or changes to the product that are outside of the producer's control, it is possible that the damage is not directly attributable to one of the manufacturers or that the causal link is hard to trace due to the inherent complexity of the devices in circulation.

(iii) Number of operators in the supply chain

In addition, difficulties may stem from the **number of market players involved**: the vehicle manufacturer and vehicle's components and parts manufacturers; the producers of software or IoT device, either by manufacturing it from scratch or assembling it from pre-existing components, both manufacturers of physical components and providers of the operational logic (i.e. software providers); the product or service providers who offer a product or service in the market consisting of or using the robot or IoT device, including direct vendors and importers, the same vehicle manufacturers, ISPs; the end users, possibly matching with the driver; the different Internet and infrastructure service providers; the injured parties who suffer harm, which may be the driver, owner or user of the product/service, but even simply a bystanders who is involved in an accident. Being a transversal concern that touch upon businesses' situation at different stages of the value chain and in different sectors, liability can apply differently and simultaneously for different players.

(iv) Types of data

A further complexity may come from the different types of data involved, such as personal data; specially protected personal data; non-personal data; mixed datasets with either distinguishable or inextricably linked personal and non-personal data; (business) confidential data, subject to an obligation of professional secrecy; trade secrets; aggregate data; anonymized/de- identified/pseudonymized data. The distinction among types of data is paramount to understand what law is applicable: for example, when dealing with non-personal data or personal data which is anonymized, the GDPR ceases to apply, but e-Privacy rules may still be applicable. While in principle the distinction seems easy to grasp, in practice it can be challenging. For instance, even in some circumstances where only non-personal data is at issue, data protection laws could still apply where such data is matched with other information which functions as an 'identifier' of an individual, and thus revealing even sensitive data of the data subjects.

(v) Types of defects

Another key aspect to consider before allocating responsibilities among the parties is the origin of the damage. In case of an accident involving a vehicle connected to a cloud service, it may be sometimes very difficult to establish the source of the accident. Two kinds of harms might arise in relation with new digital products:

- Damage arising from **defects in the *product*** (e.g. vehicle), which is regulated at EU level. The EU high standards in terms of safety and product liability remain relevant insofar defectiveness is proven to relate to a product. The definition of product and its limits becomes here crucial.
- Damage arising from **defects in *data quality and availability of in- data-based services*** not falling in the definition of product: data can be essential for the good functioning of digital technology products and services that generate (e.g. via sensors) and/or process data (e.g. through actuators, algorithms). New products could collect corrupt or improper data which might hamper their functioning. The potential for injury or damage arising from access to datasets that suffer from deficiencies can be considerable.

All that is likely to affect the current process in which liability is established, making it '*difficult, costly, and time consuming to decide against whom to bring a liability claim (the owner of a car or its liability insurer on the one hand, or a car or component manufacturer on the other)*' in the event of a traffic accident involving connected cars[136]. As a result, the consumer risks suffering the consequences of damage entirely on their own account, without the prospect of any compensation; while producers and service providers may face market barriers. These uncertainties could result in a surge of lawsuits.

Chapter 2. POSSIBLE RELEVANT LIABILITY CLAIMS

Responsibilities when providing R&M as well as other independent services, could depend on issues in:

- the data used,
- the product they run on or are embedded with, and
- the service itself.

A) Issues in products

In this first case, regardless of the correct functioning of the digital (remote R&M, or any other similar) service running on the vehicle, problems could occur due to defects in the **vehicle components** – caused by error or malicious intention – which may translate in deficiencies in the resulting decisions or render the vehicle malfunctioning. Insofar as the vehicle components are tangible products, they are encompassed by the product (safety and) strict liability framework, which revolves around the PLD, in addition to possible contractual liability and other rules.

[136] Ibid.

- B) Issues in service:

In this second case, a defect could lie in the (R&M) **service/application**, which does not depend on the vehicle where it is installed on, nor on incorrect feeding data, but rather on issues in the development or management of the service itself (e.g. error in coding, error in reading correct data). Similar defects may cause a physical injury, damage to some item of property, or even damage related to personal data (e.g. a security flaw in a piece of software leads to loss or theft of personal data of the driver, stored in their mobile phone, which is connected to the vehicle's S-OTP).

- C) Issues in data:

Finally, as any other **datasets**, RMI and other relevant vehicle data may potentially suffer from deficiencies in various properties. Any (R&M) service provided on the basis of inadequate, low quality, non-accurate, incomplete, out-of-date, inconsistent, unclear, irrelevant, corrupted, or defective data whatsoever may translate in deficiencies in the resulting decisions or amplify them and lead to non-compliance with regulatory standards and liability. Liability issues may be notably linked to the risk of:

- Acceding or using incorrect data and providing a wrong service to the end-user based on that, resulting in a range of sub-optimal outcomes and direct or indirect damage;
- Unfair and non-transparent handling of personal data, if any, which impacts on data subjects' right to privacy (and breaches GDPR).
- Sharing data with third parties who could misuse this data, potentially also infringing on third party IP rights.

Chapter 3. LIABILITY OF ISPs WHEN PROVIDING AUTOMOTIVE AFTERMARKET SERVICES

In the absence of a concrete legal framework specifically dealing with liability of ISPs, the latter will be assessed by the conventional legal rules, which may vary, to some extent, across countries and based on the adopted interpretation of legal doctrine (court decisions on the topic being practically non-existent). In light of this, this Study offers one possible reading of the topic.

Both rules on contractual and extra-contractual liability could in principle apply depending on the nature of the relation which links the parties concerned and the protected interests. While businesses currently tend to take a case-by-case approach to liability through detailed contractual arrangements, it is noted that despite and in addition to contractual rules, regulatory provisions may also apply along the contractual provisions, adding complexity to the issue.

Contractual	Extra-contractual (tort law)
Liability assumed by ISPs in relation to a contract, due to failure to perform in accordance with the agreed terms. • ***Relation between parties:*** prior relation based on a contract, parties already entered into contact and decided to govern their relationship by mean of an agreement. • ***Protected interest:*** interest in that the opposite contracting party complies with its obligations and perform them in accordance with the contract terms. Guarantees on contractual performance can be either inferred by express provisions agreed in the contract or implied, according to Member States or EU law. • ***Harm:*** breach of contract guarantees / obligations. • ***Example:*** a data service fails to perform as agreed between the ISP and the car manufacturer or the final user, not meeting the performance standards promised in the contract. The former will be contractually liable to the car manufacturer or the	Liability for damage caused to an injured person (third party) outside the context of any contract that may exist between them, due to intentional or negligent acts or omissions. • ***Relation between parties:*** no prior relation legally relevant. Relation comes to existence only when one party causes damage to the other party. • ***Protected interest:*** interest in freedom from various kinds of harm. The duties of conduct which give rise to them are imposed by law, and are based primarily on social policy, and not necessarily based upon the will or intention of the parties. • ***Harm:*** damage to property or to physical integrity. • ***Example:*** *(i)* a connected car's sensor mechanism fails to detect a pedestrian, who is run over as a result. The driver of the car will be liable to the pedestrian for failure to control the vehicle, assuming that no legislation is in place exempting a driver from the obligation to control a vehicle when driving a connected car. | *(ii)* a connected

final user.	car's sensor mechanism fails to properly detect its lanes, causing it to deviate from the road and have an accident, the driver – assuming that he might reasonably expect that the auto piloting function should have been capable of keeping the vehicle in lane – can claim damages from the car manufacturer on the basis of statutory liability (i.e. product liability legislation).

Accordingly, there are a number of ways liability claims can be structured based on whether the ISP (as any other operator in the value chain) is called to assume liability on a contractual or extra-contractual basis, or both. As observed above *[see above in Section II, chapter 6]* many jurisdictions allow the victim to bring concurrent claims alternatively. As also noted by the NTF, drawing the line between liability in tort and contractual liability might be difficult, but it is key, especially in jurisdictions that do not allow concurrent claims under both regimes.

In any case, it is recalled that the addressee of the victim's claim, charged to pay full compensation, is usually entitled to seek recourse against another person deemed responsible, exercising their right to redress. For example, the seller called to indemnify the consumer can redress to the manufacturer of the product they sold. In turn, the manufacturer of the final product – who is typically singled out as the primary person to address product liability claims to, under the PLD – may have a contractual claim against the producer of a single component or against the third party service provider.

3.1 Damage occurring due to vehicle/service operation

Any damage caused to third parties (i.e. party not covered by a contract), such as the vehicle's passengers, (R&M) service users, or other incidental victims, falls under non-contractual liability regimes. This may cover harm in the form of accident or possible theft of personal data.

For traditional road vehicles, the vehicle's owner or driver is usually recognised as the most appropriate person to be liable in case of accident, where damage is caused by the vehicle's operation (i.e. driving). Some national regimes are grounded on driver's negligence in operating the vehicle, while others hold the vehicle's owner liable regardless his intent or negligence. This is based on the ground that the vehicle's owner has the highest degree of control of the risk by deciding when, where, and how to use, maintain, and repair the vehicle, and is therefore the cheapest cost avoider and taker of insurance.

In contrast, to the extent that modern and future vehicles rely on decisions (including on R&M) taken by algorithms or software applications provided by the car producer or by a third party (like an ISP), the latters may be more appropriately deemed in control of the risk and hence in the position of avoiding it. As a consequence, in terms of *lex ferenda*, they may be called to respond in the first place, envisaging a system of strict liability borne by them rather than by the vehicle owner (without prejudice to right to redress to another liable party). In fact, despite the fact that the digital service is sold to the individual vehicle user or owner who operates it on the frontend, there could be a central backend provider who, on a continuous basis, defines the features of the technology and provides essential backend support services and/or data. This backend operator may have a good degree of control over the operational risks others are exposed to and, on this basis, could be held liable. However, **rules in this regard are not (yet) in place**. As a result, reasoning in terms of *lex lata*, it is likely that, for any damage caused by any connected vehicle, regardless of its attributability to a defect in the software, feeding data or vehicle component, the **vehicle driver/owner** will remain prima facie strictly liable for incidents caused with his car, as it is with standard vehicles, under the current (non-harmonised) framework on road liability. This is without prejudice to their right to redress to another liable actor, be it the producer or supplier of the service or of the vehicle.

For this reason, the victim (which is likely to be the vehicle owner/driver, personally damaged by the

vehicle/vehicle service, or legally called to compensate a third party injured by the vehicle's operation and willing to redress to those actually responsible) will have a key interest in identifying the root-cause of the damage to ascertain if it stems from the product/product component, the embedded technology, the update in the technology, etc. – and to provide proof of that cause. A similar exercise might end up being extremely difficult[137].

Once the cause of the damage is determined, **depending on the applicable jurisdiction and law**, the claimant is likely to be required to provide evidence of the actual **damage** suffered and the **source of the damage**, where the latter can consist of either (i) the proof of an existing defect in the product and the causal link between such defect and the damage (strict liability) or (ii) the proof of negligence or fault of a responsible person having a duty of care toward the injured party.

In the absence of a clear dedicated framework and of judicial guidelines on how to apply the existing rules, the identification of applicable provisions, and consequent evidence requirements (i.e. who must establish what in order to pursue or defend a claim), but also time-limits to file a claim (i.e. the period of time after which a claim may no longer be compensated); defences and exceptions, and other procedural rules, becomes very challenging.

This high level of uncertainty on suitability for the digital era of extra-contractual liability rules in place has been extensively discussed by legal literature and institutional players[138]. A prevailing focus has been committed to the issue of liability for damage caused by unmanned vehicles or vehicles with AI embedded devices, functioning with a degree of autonomy, rather than the liability implication for mobility app developers linked to the accurateness of data when one relies on such data in his systems or provides services on its basis. However, the proximity of these two topics allows concluding that similar findings hold for both of them. Notably, legal doctrine and EU legislators acknowledge that when harm is caused by emerging digital technologies existing rules on liability in general, and on product liability in particular, may produce unsatisfactory results since resulting loss might not be allocated to the party who is the most appropriate to bear that loss. This is mainly because modern technological products and services might differ substantially from traditional ones, which the existing framework has been designed for. As previously noted, to avoid stepping into a legal grey area, businesses largely seek to rely on contractual arrangements, where possible. In the absence of that, doctrine and stakeholders seem to agree that it is difficult to identify which EU or national provisions should be used.

3.1.1 (A) Liability for damage caused by defective vehicles

In all cases where the accident/damage can be traced back to a **defect in the vehicle or tangible vehicle component**, the current PLD, holding VMs in principle liable, seems certainly applicable to some new complex products, such as connected cars. However, such a use-case is of less relevance for this Study because it does not touch upon ISPs, which do not take part in the manufacturing of the vehicle.

Still, it is recalled that demonstrating the existence of a defect in the product design, which transcends from the concurrent operation of a digital service possibly intertwined with it, and determining that this was the cause of the accident, might be extremely problematic for the victim and, depending on the value of the claim, economically inefficient.

Also, with a specific focus on R&M services, it is noted that, compared to other independent services, they could entail additional issues insofar their inherent main purpose is of ensuring that the vehicle functions correctly in the first place. This could arguably render even harder the ascertainment of who is responsible for the accident, whether the R&M service is functioning correctly(e.g. not allowing repairing or replacing of necessary devices or equipment in the vehicle), or the vehicle itself already is flawed and possibly prevents the correct installation of

[137] European Parliament, Directorate General for Internal Policies Policy, 2016, above.

[138] See, inter alia, European Parliament EPRS, 2018, Study on A common EU approach to liability rules and insurance for connected and autonomous vehicles, European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf; Commission's communications mentioned in this Study; European Court of Auditors (2019), Ibid.; 2019 NTF Report, Ibid.

remote R&M services.

Finally, while strict liability will typically channel liability onto the producer (in this case the VM), they will retain the right to seek recourse from others contributing to the damage, such as an ISP who embedded a service into the vehicle (product). This way, the introduction of strict product liability offers victims easier access to compensation, without at the same time excluding a parallel fault or different liability claim if its requirements are fulfilled.

3.1.2 (B) Liability for damage caused by defective intangibles or services

In some circumstances, the damage could be instead inherent to the digital service, such as the software, application, or update running on the tangible device (i.e.installed on the vehicle), as opposed to a material component of the vehicle. For example, a software application for R&M remote service may affect the safe and secure functioning of the car, resulting in personal injury and damage to property. When damage stems from a **defect in intangibles or services**, in the absence of a clear pathway, rules on extra-contractual liability may be inferred either:

- by the interpretation of general (varying) tort law (this is the approach chosen by prevailing literature in DE, EE, MT, NL, SI, SK, FR[139]); or
- by stretching the rules set forth in the PLD to ensure strict liability (according to the approach chosen by prevailing literature in GR and LT[140]).

In terms of the implications of these two options, the difference basically lies in the claimant's burden of proof, which is, in theory, less onerous when strict liability is relied upon. In terms of choice, it could be affected by the reading and understanding of specificities of the national frameworks in place.

- Existing views on the applicability of PLD in case of damages stemming from software applications

In general, consistent legal doctrine argues that strict product liability and product safety rules seem somewhat unfit for a data economy which revolves around the use of data as a service (and not as a product). Absent a material carrier to which the data can be linked, the very applicability of such provisions is arguable, as it largely depends on whether data as such – absent a carrier – can be considered a 'product' and whether the software application can be distinguished from the hardware element. If a software application is considered as a service, the applicability of the PLD might be excluded (on the grounds of previously mentioned ECJ case law). This entails that standard rules on liability would apply, implying possible variation across different jurisdictions and, often, the burdensome necessity, for the victim, of proving the fault of the defendant and the causal link between fault and damage.

In this concern, different approaches have been taken by scholars, who alternatively advocated or opposed the PLD's applicability to services and intangibles. For example, some literature considers software as a movable item, and therefore a 'product' endowed with its own undoubted 'materiality' and covered by the PLD[141]; others (this is the rather prevailing view) argue that it is covered, but only as long as it is embedded into a tangible object[142]; others consider that it is simpler and more logical to see it as a service, and as such not falling in the PLD scope, as the opposite view would entail many legal and practical challenges[143]; others differentiate, holding that bespoke or custom-made software specifically is not covered, since the PLD aims at regulating mass-produced items, while other type of software could be considered as a product[144]; or finally there are those who

[139] See 2018 PLD Study.
[140] Ibid.
[141] See e.g. Italian judges (Pretore Monza 21 March 1991, Giudice istruttore di Torino, 12 December 1983) who have relied on the objective existence in the program of the "different orientation given by the magnetic particles constituting the surface state of the disc".
[142] See inter alia 2018 Deloitte Study; P. Rott, 2018, Rechtspolitischer Handlungsbedarf im Haftungsrecht, insbesondere für digitale Anwendungen, Available at: https://www.vzbv.de/sites/default/files/downloads/2018/05/04/gutachten_handlungsbedarf_im_haftungsrecht.pdf.
[143] M. P. Chatzipanagiotis, 2020, Product Liability Directive and Software Updates of Automated Vehicles, Department of Law University of Cyprus Nicosia. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3759910.
[144] D. Fairgrieve and R. Goldberg, 2020, Product Liability, 3rd ed., Oxford University Press, Oxford.

distinguish between software updates, which are services, and software upgrades, which are separate 'products', the difference being that upgrades add functionalities to the previous software versions[145].

Diverging interpretations also appear relating to the applicability of the PLD to products **bundled** with services: in some jurisdictions, the service purchased as a bundle with the product is considered by legal scholars interpreting their national implementing laws as a part of the product; in some others the service is considered as a separate entity which should fall under distinct liability rules *[see above in Section II, chapter 6.3]*.

At EU level, the ECJ has for some specific cases contributed to the classification of software, which for instance is to be considered a medical device (i.e. a *product*) when intended by the manufacturer to be used specifically for one or more of the medical purposes set out in the definition of 'medical devices'. This requires a case-by-case analysis. (see e.g. Case C-219/11 and C-329/16[146]).

However, **absent any specific case law on the matter**[147]**,** there is too limited information available at this stage on the functioning and performance of the directive with new technological developments, and there is no picture on whether and to what extent courts would endorse existing doctrinal interpretations.

- Reasoning on the outcomes of applicability of PLD in case of damages stemming from software applications

As previously noted, the very distinction between tangible product and intangible service may be very blurred with regards to new technologies, especially where the service is purchased as a bundle with the related product. Even from a cybersecurity point of view, the difference between embedded and non-embedded software might fade once a vehicle is connected (for example, when applications, such as navigation software or in-car entertainment, seen as non-embedded and non-trivial for the car's performance however reach and manipulate trivial parts of the software)[148]. Therefore, both embedded and subsequently added software applications or other specific technical features may be seen either as an integral component of a product, or as a separate element, subject to a specific, different, legal discipline.

In the view of the Commission, which can be considered an 'authentic interpretation' (that is an official and authoritative interpretation of a statute issued by the legislator of that statute), '*since the producer is responsible for the safety of the **final product as a whole**, … **for products which include software at the moment they were put into circulation by the producer, the PDL could address liability claims for damages caused by defects in this software***'[149].

Therefore, regarding software applications **already incorporated in the vehicle** and not altered since their release, it seems that courts could well endorse the interpretation according to which an intangible is a 'product' in the meaning of the PLD and, as such, falls within the strict liability regime to the extent it (A) runs on and blends in with a material object, and (B) is already defective at the point at which it is put into circulation.

If product liability law applies, then liability would in principle lie with:

- The manufacturer of the vehicle (producer to the software incorporated in the vehicle, even if it has been developed by a third party);
- Third party developing the software, if different;
- AV importers;
- Potentially car sellers or retailers.

[145] Minutes of Meeting of the Expert Group on "Liability and New Technologies – Product Liability Formation. 2019. Available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=31014.
[146] ECJ, Judgment of 7 December 2017, Snitem and Philips France, ECLI:EU:C:2017:947.
[147] The 2018 PDL Study shows that from 2000 to 2016 there has been only one case (published), in BG, concerning new technological developments (see above, Section II, chapter 6). Extensive desk research has been carried out under this Study for the purpose of updating this finding, focusing on most recent case law. While the finding seems confirm (no relevant case law has been detected) it is stressed that no consultation activity has been conducted, which could have allowed a more in-depth scrutiny of national systems judicial framework.
[148] TNO 2019 Study, Ibid.
[149] See the Commission evaluation of the PLD, Ibid.

It is recalled that the notion of damage for the purpose of the directive (that is of compensation) has some limits. Damage is indeed only actionable under certain requirements, and the directive does not cover damage to the defective product itself. If the PLD is applied basing on the reasoning that the vehicle and the software (at least the basic software which enables the execution of applications provided by ISPs, if not even software updates/applications) are the same product made up of intertwined parts, then any damage caused to the vehicle or software are to be excluded by the compensation.

Things seem more complicated as to software updates or applications later developed (by third parties such as ISPs, or, alternatively, by the same VMs) and installed by the user/driver after the vehicle, with its integrated software, is already on the market.

The same Commission, in its PLD evaluation adds, to the former statement that '*the more open nature of new products, where the producer is no longer able to control software or other technical features subsequently installed in or learned by the product, may however pose a challenge for establishing claims*' under strict liability[150].

There are, in fact, different options here:

- (i) One option would be to understand software application/service as a piece of the software and therefore apply the same regime as the basic software already incorporated in the vehicle. If the software embedded in the vehicle is understood as a 'product' as it is considered intertwined with the tangible part of the vehicle, the same could be for applications subsequently added, seen in their merge with the end-product, that is the vehicle.
- (ii) A second, intermediate, option would be to consider applications or software upgrades as separate products, in that they add functionalities to the previous in-vehicle software; while simple software updates as services to the basic software[151].
- (iii) A third, opposite, option would be to consider all applications and software upgrades and updates as services to the basic software and therefore excluded, under the current framework, from the PLD scope.

(i) Option relying on strict product liability:

If and to the extent software applications (and, eventually, also updates) are deemed products, the PLD applies, although not free from practical and legal challenges.

Even where courts would concede that all software applications/services, regardless of when and by whom they are developed, can be understood as products in the meaning of the directive, they would actually appear as components of a more complex end-product (vehicle), as they embed in and bundle with it (under the PLD 'product' means '*all movables, (…) even though incorporated into another movable*'). When a component part malfunctions, it seems reasonably clear that the manufacturer will be accountable for the resulting injury. Nonetheless, the liability of a component part manufacturer may create problems in the determination of responsibility for injuries. In fact, unlike other product components, software applications/services or updates may not be already present when the end product is put into circulation, being instead only added at a later stage. This entails uncertain outcomes where the current PLD provisions are relied upon.

In fact, the time that the product is put into circulation becomes particularly critical since, by virtue of Art. 7(b) of PLD, strict liability is only imposed for defects that existed at that time, meaning '*when the product is taken out of the manufacturing process operated by the producer and enters a marketing process in the form in which it is offered to the public in order to be used or consumed*' (C-127/04). It results that the producer does not respond for defects that arose after his product leaves the production process operated by him and is offered in the market. The putting into circulation of a product depends on the producer's **loss of control** over that product,

[150] Ibid.
[151] See Minutes of Meeting of the Expert Group on "Liability and New Technologies – Product Liability Formation, 2019, above.

for instance if it occurs when the product is transferred to a person over whom the producer does not have any authority or enters into the chain of distribution[152].

This means that, under the current framework, producers may not be strictly responsible for damages caused in 'evolving' products (new self-learning technologies, applications which develop based on new inputs or features automatically installed, etc.) unless the defect was already present since its initial release, which seems very hard to demonstrate. This applies both for evolving applications/services already embedded and released with the car, but also for those later installed, if these are deemed 'products' in the meaning of the PLD. In fact, while the strict liability theory does ease some of the burdens on the plaintiff, it is not intended to impose absolute liability on producers or sellers or make them insurers of their products. A manufacturer or seller is not subjected to liability solely because he put an initial product into circulation, and it was involved in an injury-producing event outside his control[153].

If the term 'product' is understood as encompassing both the vehicle and the added application as a unique entity (this reading would be justified by the fact that the requirement of tangibility enabling the application of the PLD is only met where the intangible application/service is seen in its enduring link with the tangible vehicle), then any service provider (VM or ISP) – 'producer' in the mean of the directive – is likely to always escape liability by invoking the exception of Art. 7(b). This is because the release of the (possibly defective) application/service usually occurs after the vehicle and its basic operating software are put into circulation , such as the release of a defective update coming after the release of the application. In other words, it is the very modification to the initial safe 'product', which occurs only after purchase, that introduces the risk and consequential defect, which was previously inexistent, as it pertains to the new (intangible) component that was not there before.

Two options are hence possible to ensure some kind of protection for defects in aftermarket applications, should one still want to rely on product liability: both of them require to consider the term 'product' in Art. 7(b) with a narrower meaning, that is encompassing, either only the material part (vehicle) – sub a – or only the added application, seen as a distinct end product – sub b.

a) While product liability is applied to already embedded applications already present in the vehicle[154], if any, the aftermarket application could be considered as a 'service', not falling in the remit of the PLD, to the extent it is regarded as a distinct (intangible) entity compared to the vehicle it runs on, rather than as its component. Other regimes of extra-contractual (normally fault-based) liability would hence apply to it. The resort to fault-based liability, or other specific regime envisaged for service providers, would be justified by the lack of materiality of the software application no longer considered as a component of the final vehicle, but as an intangible item different from the movables encompassed by the PLD. Yet, while filling the legal void, this would entail an unjustified difference in treatment between damages stemming from (VMs' or ISPs') *added* applications (i.e. aftermarket applications put into circulation after the vehicle), and those stemming from (VMs') *already present* in-vehicle applications (i.e. put into circulation together with the vehicle and not altered since then); with the former falling under fault-based liability and the latter under strict liability. Accordingly, VMs could easily escape strict liability by delaying the release of software applications to a later moment, in view of enjoying the more favourable fault liability regime.

b) The aftermarket application could be considered as an end product in itself; distinct from the vehicle it runs on and despite its incorporation into another complex product. Under a similar reading, the VM would not be able to rely on the exception under Art. 7(b) anymore, since the producer of the software application (the ISP as much as the VM, here actig as OEM) would be accountable since its release, regardless of the time when the other vehicle components or vehicle itself have been put on the market. In turn, the manufacturer would escape joint liability in all cases where the software application is developed by a third party such as an ISP: the manufacturer could indeed argue that he did not put

[152] See, inter alia, Case C-127/04.
[153] R. E. Byrne, 1974, Strict Liability and the Scientifically Unknowable Risk, Marquette Law Review, Vol. 57, Issue 4.
[154] As that they could be easily monitored by the VM.

the 'product' (only referring to the app and not the vehicle it runs on) into circulation - exception under art. 7(a); or that the 'product', in the same narrower meaning, was neither manufactured by them for sale or any form of distribution for economic purpose nor manufactured or distributed by them in the course of his business - exception under art. 7(c). **However, this reading is not supported by the current wording of the directive, where the foundation for relying on strict product liability rules is the materiality of the product and, accordingly, is the very bundling with and incorporation into a tangible object (vehicle) which justifies the argument supporting the PLD's applicability to intangibles**. In other words, the understanding of the software application or any other intangible that runs on a tangible product as part of a unique final tangible product (or product component), is the necessary premise for the application of strict product liability, given the current link with materiality. Moreover, the reading that considers aftermarket applications as end products, distinct from the vehicle they run on and ignoring their incorprotation in another complex product (vehicle), seems to clash also with the type approval logic, under which manufacturers are ultimately responsible to ensure security and regulatory compliance of their vehicle, which includes all systems, components and separate technical units.

Hence the outcome, if courts decide to apply the PLD to the case at issue, seems paradoxical as it implies a legal void of protection for damages stemming from added software applications, or a different treatment for defects alike depending on the time of put into circulation, or inconsistency with the PLD current wording.

This being said, it remains that the ascertainment of the source of damage in complex products as such may be extremely challenging. Therefore, it is not excluded in practice that the VM becomes the subject of consumer claims under the directive, as liability lies initially with the VM if the system within the car exposes it as a whole to a safety risk; thus, the potential concern for VMs, highlighted by some literature[155]. Nonetheless, concerns that manufacturers would be eventually ruled liable for incidents caused by third party code which is not in their control should be mitigated by the (demanding) need for proving defect and causality and the related difficulties on the victim, as well as on the VM's possibility to redress to the actual responsible in the unlikely case that they are called to fully compensate the victim for a damage for which they are not accountable.

(ii) Option relying on strict product liability or extra-contractual service liability according to intangible device's features

As to the second interpretative option, it considers software applications or upgrades as separate products, in that they add functionalities to the previous in-vehicle software, while simple software updates as services to the basic software. It has been claimed[156] that such distinction risks permitting the software developer to determine at will whether it will be subject to the PLD remit or not, by characterizing a piece of software as an update or an upgrade and ultimately resulting in legal uncertainty. Besides, remote R&M and similar services would arguably be encompassed in the first group (i.e. software applications or upgrades that add functionalities to the previous in-vehicle software) hence the same reasoning as above applies *[see here above, point (i)]*.

(iii) Option relying on extra-contractual service liability:

The final proposed view considers mobility services (i.e. software applications or updates) as services to the basic software. Under this reading, they would be excluded from the PLD's current scope, as interpreted by the ECJ, and would instead fall under national specific rules in place on service provider responsibility, if any, or under general national extra-contractual clauses which acts as *lex generalis*.

For example, some countries (such as ES or GR) could use their special regimes of liability for flawed services, based on a presumed fault on the service provider's part.[157]

In other legal systems, relatively open tort law provisions (tort of fault/negligence, breach of statutory duty),

[155] Inter alia, diffusely in 2017 TRL Study, Ibid.
[156] Michael P. Chatzipanagiotis, 2020, above.
[157] 2019 NTF Report, Ibid.

expressly or by way of interpretation, can go beyond product liability by covering defective ancillary digital services, or failures in product surveillance or monitoring (and hence 'evolving' products).

Also, in some other countries (DE, AT, or GR, and to some extent DK) where tort law provisions are narrower, as an alternative workaround for deficiencies of the extra-contractual law regime, similar solutions are obtained by extending contractual liability, under certain conditions, even in the absence of a contract[158]. In fact, when the user is contractually tied to the ISP, the latter may be liable in contract to the user for damage caused by non-performance *[see below in this Section, chapter 3.2].* When contractual liability is extended, the contract is deemed to establish duties to also protect third parties, who must be foreseeably close to the contracting partner, confronted in a similar way with the danger stemming from non-performance (such as family members or guests). Said third party is allowed to invoke a contract they were not privy to, suing for compensation in cases of breach. Any kind of contractual liability is, however, usually subject to the contractual (and sometimes also statutory) limitations previously mentioned.

Similar rules are to be assessed case-by-case, with possiblly different outcomes depending on the jurisdiction that comes into play. Given the widely discussed lack of harmonisation of extra-contractual liability rules, it is not possible to anticipate here which provisions would be typically applicable, as this would largely depend on the country where the claim is brought.

Overall, it is recalled that usually the claimant must prove:

- that a duty of care to the injured party existed;
- that the duty of care was breached by conduct falling below a reasonable standard;
- that damage was caused by a negligent conduct (or by intention); and
- that loss was consequently suffered by the claimant.

Variations among the national laws may exist, notably, in relation to the burden of proof, hence evidence listed above might be burdened on the defendant disprove. Moreover, there will also be regional disparities pertaining to time-limits and defences to negligence claims, such as contributory negligence or voluntary assumption of risk by the claimant, or the fact that harm was caused by some intervening external event (e.g. force majeure).

3.1.3 (C) Liability for damage caused by defective data

Any data-driven service may also malfunction due to problems with data rather than with the service itself. Liability from access to and use of data could cover, in principle, a wide range of data: such as data generally transmitted by the vehicle to other vehicles and the surrounding infrastructure, data otherwise made available to external operators via the in-vehicle interface, and data transmitted directly from external sources to the vehicle (either implemented by the vehicle or picked up by the in-vehicle systems) such as RDS signals picked up and displayed by the infotainment system. Compared to the situations previously examined (under (A) and (B)) on responsibility for the functioning of the carrier (vehicle or vehicle component) and for the data driven service provided, respectively, responsibility for data used and processed is quite affected by the chosen technical architecture for data sharing. This chapter focuses on expected liability implications when secure S-OTP is used. In the next chapter analysis on expected outcomes using alternative architectures is proposed.

3.1.3.1 RMI and remote repair and maintenance services

For the purpose of this Study, in terms of data, a focus is placed on vehicle RMI, which is a type of **technical data**. While additional data will come into play for the purpose of mobility applications, RMI are particularly relevant in the fields of repairs, mechanics, maintenance and diagnostics, also including data related to on-board diagnostic systems for remote services and their interaction with other vehicle systems, defined in Regulation (EC) No 715/2007 *[see above, Section II, chapter 5.1].*

As previously showed, EU rules set standards in terms of non-discriminatory, unrestricted, and standardised

[158] Ibid.

access to vehicle RMI from ISPs and independent operators such as automobile clubs. Provisions also aim to guarantee that operators in the aftermarket can rely on precise and update data, which, to this end, should be amended and supplemented by VMs when needed. Under the perspective of the current rules, it is hence assumed that the VM acts as a data supplier, possibly even charging a fee for RMI access.

While current legislation reasons in terms on RMI data accessed via a physical connection in the vehicle, this data is now increasingly accessible remotely, opening up the possibility of providing access to real-time information and allowing for remote repair and maintenance services *[see above, Section I, chapter 1 and Section II, chapter 5]*. A dedicated study on RMI of October 2014[159] concludes that, in general, the scope of vehicle RMI is likely to include at least some information transferred wirelessly, but the precise definitions and means for data exchange will need to be further clarified and included in the RMI Regulations to ensure fair access to information. In addition, increased technical complexity of vehicles capable of connecting with the infrastructure and with other vehicles will require a harmonised approach, which should be reflected in specifications and standards as envisaged in Articles 6 and 8 of Directive 2010/40/EU ("**ITS Directive**")[160].

Future rules and standards as such should hopefully facilitate the determination of liabilities and faults when transferring or using vehicle data, including RMI, as they would clarify when data or data-transfer is deemed accurate/complete/secure, thus setting benchmarks against which deviations, and hence responsibilities, are assessed.

3.1.3.2 Liability from acceding or using incorrect data

If ISP accesses and uses biased, poor quality, or incorrect data, they risk providing a defective service to the end-user, possibly also resulting in sub-optimal outcomes or damage.

Various situations may occur: the ISP may (i) access and use already damaged or inaccurate data or (ii) overlook a data breach originating from the application downloaded by the driver. As a result of the use of low-quality data, they may in turn have the quality of data-based mobility services affected and, ultimately, (I) not be able to correctly supply the service to meet promised contractual standards, or even (II) cause damage, thus endangering the safety of the vehicle, its passengers, and the surrounding environment. The first alternative options (i and ii) pertain to the source of the problem, which is to be investigated and proved by the part burdened by the onus of proof (i.e., usually the consumer). The second (I and II) affects the type of liability regime triggered, that is respectively contractual or extra-contractual.

If inaccurate data leads to lack of performance of the service and data is supplied under a contract as part of a specific obligation of one party (ISP) toward the other (user), the situation in relatively easy as the terms of agreement will govern parties' relationship. Recently enacted regulatory provisions for consumer contracts involving digital services enhance legal certainty in this regard, by complementing contractual provisions and guiding the parties in allocating their mutual obligations. However, while they certainly cover the situation where data and digital services are provided to consumers, they are not necessarily applicable to other situations where no party is a consumer (this will depend on national implementing choices) *[see above under Section II, chapter 2.2, & below in this Section, chapter 3.2]*.

By contrast, claims for non-contractual liability in cases where reliance on inaccurate data leads to damage are much more difficult to bring successfully. This might depend, among other things, on the difficulty in applying the general principles of non-contractual liability, such as establishing the data provider's duty of care and the chain of causation, but also on the fact that data processing takes place in a complex ecosystem, shaped by the presence of actors of the digital economy, road infrastructure managers and telecommunications operators, on top of the traditional players of the automotive industry.

[159] Ricardo-Acea & TNO, 2014, Study on the operation of the system of access to vehicle repair and maintenance information, European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/c2c172a5-3f49-4644-b5bb-c508d7532e4a ("**2014 RMI Study**").

[160] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L 207, 6.8.2010. In its work programme for 2021, published on 19 October 2021, the Commission announced an upcoming revision of the ITS Directive.

It is recalled that, in any case, regardless the existence of a contractual claim for the parties concerned, ISPs could potentially be exposed also to extra-contractual liability claims from injured parties damaged by the use of inaccurate data.

On average, lacking specific rules, there is a high degree of uncertainty and no agreement on who should be held responsible, in principle, for the **quality of the data**. Previous studies have explored the topic, also trying to gather stakeholderss views, for instance, on who should primarily be held responsible if an application downloaded to a car from a manufacturer-approved site — or linked smartphone — has a cyber-security vulnerability and puts the safety of the car or personal data at risk[161].

Responsibility is likely to lie on the **party providing (access to) the data** (depending on the data sharing architecture, but currently mostly the manufacturer, also in line with Type Approval Regulation's information sharing obligations) but also on the **app developer/provider of data-based mobility service** (ISP or/and VM), depending on when the defect appears. For instance, data could be provided by one actor to another in the supply chain free from defects but then becomes inaccurate at a later time due to hacking, lack of updating, etc. It is recalled that, regardless, under data protection laws, data controllers (e.g. the ISP) are always responsible for personal data accuracy, which entails the obligation of keeping it up to date. On the other hand, under the new Type Approval Regulation as amended in 2019 (applicable from 2022), manufacturers are ultimately responsible to ensure that their vehicle, systems, components and separate technical units placed on the market or entered into service are type-approved and remain always compliant with the applicable new requirements **including on protection against cyberattacks**. This entails that vehicle security over the vehicle's lifetime (cradle to grave) remains the responsibility of the VM.

In principle, the ISP providing a service to a user is responsible to that user for the good provision of such a service, and hence of the correctness of data relied upon, regardless of the fact they had collected and used publicly available data and developed a service based on it, or that the data had been supplied data from another actor in the supply chain such as the manufacturer. The exact scope of ISP's responsibility to the service user is likely to be shaped by contractual terms on service supply – freely agreed within the boundaries of relevant laws on B2C – also including, expressly or implicitly, warranties on data quality.

When the ISP compensates the user and, in turn, had previously received already flawed data from a different data provider, they are entitled to redress against the latter, often based on a contract stipulated between the ISP and data provider.

If the data is, instead, directly accessed but from a device controlled by a different actor (e.g. the vehicle produced by VM generates data which is freely taken and processed by ISP to provide new services) – without any warranty on their part regarding data accuracy or quality – it seems much more difficult to have a successful claim against the VM. In fact, outside a contract, it could be maintained that, as long as data remains under an operator's control, they remain responsible for the related risks (duty of care and monitoring). This is, however, extremely hard to assess and prove, considering that even precise data may change over time and become inaccurate, due to intervention or even lack of intervention.

By contrast, if a warranty exists relating to vehicle data quality, this can be contractually enforced as it is a legally binding commitment which binds a party to perform in a specified way. Depending on the particular national contract law and case law, warranties may also be statutory or implied, if they do not arise from express representations.

3.1.3.3 Liability from incorrect processing of personal data

The process of (RMI and other) data needed to provide mobility services to users will be subject to data protection requirements only to the extent that data collected and used is personal data.

- Data subjects and data controllers

[161] Inter alia, D. Brown, 2016, Responsibility for Vehicle Security and Driver Privacy in the Age of the Connected Car, IDC, Available at: https://www.veracode.com/sites/default/files/Resources/Whitepapers/idc-veracode-connected-car-research-whitepaper.pdf

As set out previously *[see above in Section II, chapter 5.1]*, data protection laws give rights to the **data subjects**, which are likely to be drivers or vehicle owners, passengers who use on-board services, road users and pedestrians who interact with the vehicle and whose data is collected, etc[162]. On the other hand, **data controllers**[163] – required to ensure that the processing complies with data protection laws – will be any entity that determines how or why the data processing (broadly defined). This is likely to be any manufactuer, vehicle retailer, service provider, platform providers, application providers, etc, even jointly[164]. It follows that the ISP may qualify as a controller or processor, if they are involved in the processing of personal data.

- Personal or technical data:

Nonetheless, the distinction between personal and non-personal data in the context of connected vehicles is not always straightforward and discussion is ongoing on whether car-generated data should be classified as personal data (as defined by Article 4(1) of the GDPR) or technical data. **Personal data** encompasses all information that relates to an identified or identifiable natural person. This includes for instance, a name, an address, an IP address, navigation destinations, the user's address book, personalised access to third party services, infotainment settings, personalised in-car settings, as well as any information that can be used to evaluate, influence the status or behaviour of that person or that is otherwise likely to have an impact on the individual's rights or interests. On the other hand, **technical data** would be data mostly generated within the vehicle unit control, vehicle performance data such as tyre pressure, vehicle speed, oil level, fuel consumption, mileage, wear and tear on vehicle parts, battery charge status, etc[165].

Despite this theoretical distinction, although data collected by vehicles are usually directly linked only to its technical aspects and features, it ultimately concerns the driver or the passengers of the car: **any apparent technical information, if connected to the data subject or personal circumstances of the data subject, and thus related to a specific driver or car owner, should be considered personal**. For example, as confirmed by several national data protection authorities in the EU, the Vehicle Identification Number ("**VIN**") – and any data combined with it – is considered an identifier relevant to the GDPR[166]. It follows that **in-vehicle data is always personal data** because technical data and metadata produced by natural persons using the vehicle as a terminal, by cross-referencing with other files such as the VIN, can be related to a natural person and permit identification of a potential plurality of users. As a result, data protection provisions are always relevant and shall be abide with, when processing in-vehicle data.

This finding remains valid even though most actors in the automotive industry argue that the majority of vehicle-generated (personal) data can be anonymised, therefore having less relevance to data privacy law[167]. Data that has been aggregated or anonymised in such a way as to prevent an individual being identified will, indeed, not constitute personal data and so its use will not engage data protection laws[168]. Nonetheless, most after-sale services cannot rely on anonymised data because they are targeted at specific individuals based on features about their activity and/or vehicle (e.g. information on vehicle driving behaviour/vehicle usage, distance

[162] See Article 4(1) of the GDPR.
[163] See Article 4(7) of the GDPR; and the European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR
[164] See Article 26 of the GDPR. In case of joint controllers, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information.
[165] O. Clarke, 2017, What EU legislation say about car data, Study prepared for FIA Region I. Available at: fiaregion1.com/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf
[166] Inter alia, the CNIL in France (see https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf). See also, consistenly: FIA Region I, 2017, What EU legislation says about car data, Legal Memorandum on connected vehicles and data, Osborne Clarke. Available at: https://mycarmydata.eu/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf
[167] See e.g. VDA, 2016, Position – Access to vehicle and vehicle generated data. Available at: vda.de/en/topics/innovation-and-technology/network/access-to-thevehicle.html; ACEA, 2015, Principles of Data Protection in Relation to Connected Vehicles and Services. Available at: www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to--connected-vehicles-and-se; ACEA, 2016, Strategy Paper on Connectivity. Available at: www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf; SMMT, 2017, Connected and Autonomous Vehicles – Position Paper. Available at: www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf
[168] 2017 TRL Study, above.

covered, driving style, location, etc.).

Given the possible difficulties in distinguishing data for which the GDPR protection applies, especially in case of mixed datasets where personal and anonymized data are inextricably linked, the basic principles for legal, fair and transparent data processing may be recommended for management of any data, including non-personal, adopting the so-called **precautionary principle** as recalled by the ECJ. By virtue of this principle, where applicability of a stricter legal standard is unclear to the matter at hand, the stricter standard should be followed. Accordingly, when it is unclear whether a mobility service is based on personal or non-personal data (or a mix), it should be assumed that personal data is at stake and the data process should be fully compliant with the GDPR. This should reduce the room for liability claims related to data privacy and protection. A similar approach, by enhancing the vigilance exercised with regard to the use of data (e.g. incorporating the protection of personal data dimension from the product design phase, ensuring that car users enjoy transparency and control in relation to their data, etc.), expresses the importance of complying with personal data protection legislation. As a result, it is likely to help strengthen user confidence, and thus the long-term development of new technologies.[169]

Data protection authorities have started to develop guidelines on how data protection rules (both at EU and national level) apply in the framework of connected cars.[170] Notably, on 9 March 2021, the European Data Protection Board (EDPB) adopted **Guidelines on processing personal data in the context of connected vehicles and mobility related applications**[171], intended to facilitate compliance of the processing of personal data carried out by a wide range of stakeholders working in this environment. The scope of the EDPB Guidelines focuses in particular on the personal data processing in relation to the non-professional use of connected vehicles[172] by data subjects with the personal data: (i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or (iii) collected locally in the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.

While some main principles are recalled henceforth, it is stressed that the EDPB Guidelines can represent a valid reference when trying to understand the extent of data protection and privacy related obligations to abide with, offering a reliable interpretation of applicable laws, examples of privacy and data protection risks, general recommendations to be followed when dealing with data, as well as practical case studies which provide useful examples to rely upon.

- Applicable rules

In terms of applicable law, the GDPR and, to some extent, the e-Privacy Directive play a key role. From both frameworks, the notion of user consent (Article 6 GDPR and 5(3) e-Privacy) becomes central.

As remarked by the EDPB, Article 5(3) of the e-Privacy Directive comes into play where the vehicle and devices

[169] In this regard, see also FIA Region I Campaign "My Car My Data"; http://www.mycarmydata.eu/

[170] For instance, in 2016, the Conference of the German Federal and State Data Protection Authorities and the German Association of the Automotive Industry published a common declaration on the principles of data protection in connected and not-connected vehicles (https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf). The following year, the UK Centre for Connected and Autonomous Vehicles (released a guide stating principles of cyber security for connected and automated vehicles in order to raise awareness on the matter within the automotive sector (https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated- vehicles); and the French data protection authority, CNIL, released a compliance package for connected cars in order to provide assistance to stakeholders on how to integrate data protection by design and by default, enabling data subjects to have effective control over their data (https://www.cnil.fr/en/connected- vehicles-compliance-package-responsible-use-data).

[171] EDPB, 2021, Guidelines on processing personal data in the context of connected vehicles and mobility related applications ("**EDPB Guidelines**").

[172] The connected vehicle definition for the purpose of the EDPB Guidelines is a broad concept encompassing any "vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle (for example, relying on the sole use of the smart phone) to assist drivers is included"

connected to it are deemed 'terminal equipment' as per the definition inDirective 2008/63/CE and regardless of the nature of the data being stored or accessed. Under the e-Privacy Directive, the controller shall seek consent for the storing or gaining of access to information, informing the data subject about all the purposes of the processing, including any processing following the aforementioned operations (meaning the 'subsequent processing'). Under the GDPR, there are a limited number of exceptions where consent to the processing of data may not be necessary, notably, where the processing is necessary to **carry out a contract with the data subject**, protect the vital interests of the data subject or another natural person, comply with a legal obligation to which the controller is subject, public interest or exercise of official authority, and legitimate interests pursued by the controller or a third party. Otherwise, when personal data is at stake and is to be used for a commercial purpose, consent will be necessary and ISPs (or any other service provider) should obtain it from the data subject.

Consent required by the e-Privacy Directive and that needed as a legal basis for the processing of data under the GDPR for the same specific purpose can be collected at the same time. Where consent is necessary, the notion in the e-Privacy Directive remains as in the GDPR and must hence meet all the requirements of the consent as provided by Art. 4(11) and 7 GDPR. It must be therefore freely given, specific, informed and unambiguous.

In the view of EDPB, consent under Art. 6 of the GDPR will generally be the most adequate legal basis to cover the processing of personal data following such operations (as far as the purpose of the following processing is comprehended by the data subject's consent). Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the subsequent processing of personal data.

Indeed, when assessing compliance with Art. 6 GDPR, controllers must take into account:

- the fact that processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection;[173]
- the impact on data subjects' rights when identifying the appropriate lawful basis in order to respect the principle of fairness.[174]

It follows that Art. 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by Art. 5(3) e-Privacy Directive.

In addition, when data is collected on the grounds of Art. 5(3) e-Privacy (or on one of the exemptions provided therein), and subsequently processed in accordance with the GDPR, the initial consent does not legitimise further processing, as consent needs to be informed and specific. Therefore, on such occasion, it can only be further processed by seeking additional consent for this new purpose (or by demonstrating that it is based on EU or national law to safeguard the objectives referred to in art. 23(1) GDPR). Each application available on the S-OTP has indeed the potential to make use of the personal data in a way not previously informed and consented to by the data subject (for instance some of the data collected for maintenance purposes may not be disclosed to motor insurance companies without the users consent for the purpose of creating driver profiles to offer driving behaviour-based insurance policies). Where this is the case, **further consent** may hence be required. Equally, as remarked by WG6, if a VM wishes to disclose in-vehicle data to an ISP, the data subject's consent is likely to be needed.

The EDPB considers that further processing on the basis of a compatibility test according to art. 6(4) GDPR is not possible in such cases, since it would undermine the data protection standard of the ePrivacy directive, which needs to be specific and informed.

Besides,secure S-OTP, by definition, is designed to ensure data protection and supports the shifting of data sovereignty from the VM, as single data controller, to different ISPs who can directly access the vehicle and offer their services to the final consumers (i.e. data subjects); requested vehicle data is hence transmitted wirelessly

[173] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.
[174] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

to ISPs servers *upon users' consent*. The data subject is therefore supposed to hold complete control over their own data.

- Main responsibilities of data controller

When the ISP acts as a data controller, he is responsible for **data accuracy**, which entails the obligation of keeping it **up to date**. Additionally, its main obligations include[175]:

- obtaining, unless not required by law (i.e. contract), user consent and limit data processing to the extent of the original consent given by the data subject.
- ensuring that appropriate technical and organisational security measures are taken to prevent unauthorised and unlawful processing;
- ensuring their service complies with the 'privacy by design' principle;
- allowing, at the data subject's request, data portability (i.e.e.g. transferring data to another service provider);
- deleting data when data subjects withdraw their consent or data is no longer necessary for the purpose for which it was collected.
- providing information about their identity and purposes in processing the personal data.

Data subject rights can be enforced either by the data subjects themselves or by national regulators. In this regard it is noted that, unlike the previous framework, the GDPR sets that service providers are liable for their use of personal data even where they use it solely on the instruction of the data controllers. This will mean that service providers such as software vendors will also be directly subject to data protection laws.

3.1.3.4 Liability from infringements to third party IP-related rights

Liability for devices and services using data might relate to classification of data as property, hence giving rise to IP rights and trade secrets implications. However, as noted *[see above in Section II, chapter 5]* the current legal framework (and case-law[176]) at EU level does not recognise an actual 'ownership' right in data (while national laws and courts decisions on the matter are quite inconsistent). Conversely, data has been typically understood as information, rather than as property, thus falling outside the scope of the rights which apply to tangible property. One reason for this is that, when referring to data, the term 'ownership' in its traditional legal meaning entails certain difficulties due to data characteristics (such as its limitlessness and non-expendability, non-rivalrousness, with an intrinsic and/or added value as a by-product of information processing, its needing to be updated). Liability in connection with data 'ownership' is therefore, meant without any legal connotation, to assign responsibility and accountability for specific databases or intellectual works, without implying any transfer of or licence over property as such.

This scenario could pose liability concerns for ISPs when the data (information) is characterised by multiple overlapping legal rights which may affect their acquisition, use, and disclosure. In this respect, as observed above, the main rights in data, aside from data protection laws and specific contractual rights, stems from copyright law, business confidentiality/trade secrets, and database rights. Accordingly, there may be different risks for different data, depending on how that data is protected.[177]

A breach scenario potentially arises when data, in which third party rights subsists, ends up being used by ISPs without the required authorisation (e.g. where some OEM's proprietary information, which falls outside the scope of access to vehicle RMI legislation, is used).

However, the relevance and likelihood of similar claims is arguable. For example, as to database protection specifically – where the EU legal regime is twofold, with copyright protection granted to creative databases and

[175] See also Article 5 of the GDPR.

[176] Although, according to some interpretation, the Court paved the way for a discussion on ownership in intangible goods - to be possible applied to other digital goods in future decisions - in its judgment of 3 July 2012, Case C-128/11.

[177] On this topic, see also T. Bond, N. Aries, 2018, Forbidden Fruits: third party rights in AI training data, a European Perspective, Bird & Bird News Centre.

to databases for which substantial investment have been made – it is noted[178] that:

- on the one hand, copyright protection is granted to creative databases if they are viewed as creative works (i.e. an author's own intellectual creation) in relation either to the *selection* or to the *arrangement* of their contents. However, the copyright protection for databases does not extend to the content (i.e. data) as such. Hence, even if the data is included in a copyrightable database, such copyright protection would not extend to that data.[179]
- on the other hand, *sui generis* database protection granted based on 'substantial investment' may apparently provide a better basis for protecting the data in the world of IoT, but there are limitations on both the subject-matter and the scope of protection.

Similarly, as to trade secret protection, its relevance can be argued. It is doubtful if data created by vehicles or sensors could fall within the scope of the Trade Secret Directive, and who would be the person entitled to such protection in cases of data generated in networks where different entities are connected. Additionally, it has been observed that the directive does not protect against any wrongful use of data, but against unlawful conduct, which can be regarded as 'contrary to commercial practices'[180].

It is hence argued that such frameworks are not always applicable and apt to new data services, as they are based on a static technology concept that no longer corresponds to the use of data in the era of IoT, failing to adequately respond to the features of constantly changing datasets and real-time data services.

In any case, space for liability related to any 'proprietary' right in data (overall), if existing, is reduced to situations where the data to be accessed and used is carefully selected and agreed upon, also by means of contractual arrangements, between the parties concerned and is also dependent on the technical architecture used.

3.2 Failure/lack of performance of the (R&M) service resulting in lack of conformity with contractual terms

Particularly relevant contractual relationships are likely to be:

- Between the VM and S-OTP provider or A-GWA (i.e. neutral party which provides the necessary infrastructure for the inbuilt device).
- Between the S-OTP provider and ISP (or other application providers): to determine the terms on which third party application providers could develop applications and the terms on which users could install and access such applications on the platform.
- Between the VM/ISP and the user (i.e. subscriber to the specific service that relies on data).

A specific contract between the ISP and VM seems needed if the VM acts as a data provider to the ISP.

When relationships between relevant actors are regulated by contracts, it is typically easier to establish responsibility. This is compounded by the fact that national and EU legislative frameworks that apply to consumer contracts in the data ecosystem have been recently updated and should now be more apt to cope with digital challenges and the performance of the data value chain contracts.

The accrued facility in allocating liability depends on the fact that a contract's terms usually include an express obligation to sell the product or provide a service free of defects. As a result, any damage is considered as a result of breach of contract.

In practice, this means that any party is bound by the obligations assumed toward the other party when signing

[178] E.g., J. Drexl, 2017, Designing competitive markets for industrial data – between propertisation and access", Journal of Intellectual Property, Information Technology and E-Commerce Law. (8), 4.
[179] Art. 3(1) and 3(2) of the Database Directive.
[180] Ibid.

the agreement. Relevant contractual terms to abide with include both:

- explicit statements in which the party delineates its obligations and/or liabilities and warranties;
- implicit obligations resulting from the application of the law, including implicit or statutory warranties.

Despite and in addition to any agreed term on contractual liability, the law (PLD) currently assigns liability to producers for any vehicle's parts that malfunction. For this reason, it has been contended that providing direct access to in-vehicle data to ISPs could possibly increase VMs' liability[181]. While this is arguable, it could result that, even where the data provider is distinct from the VM, the VM would still try to limit its liability by influencing contractual terms between the data provider and ISPs, for instance, by including in its contract with the data provider a requirement that the latter pass on particular terms to the ISP and the ultimate user[182].

As observed in Section II, parties' freedom in governing their own liability is sometimes limited by other regulatory provisions, especially in B2C contracts. These may be contracts between the ISP/VM and the end user, which are likely to fall under the definition of 'consumer' (as opposed to between the ISP and the VM or them and the S-OTP provider or other data access provider).

As seen above, applicable legislation on B2C contracts includes the recently enacted DCD and SGD. As they regulate terms for the supply of digital content (i.e. data which is produced and supplied in digital form such as operating systems, applications and any other software) and/or services (i.e. a service that allows the consumer to create, process, store or access data in digital form, such as software-as-a-service offered in cloud storage, the continuous supply of traffic data in a navigation system; or the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service) they are likely to apply to the contractual relationship between ISPs and consumers using the applications and between the VM and consumers using the vehicles. The new directives protect both consumers who pay for a service and those who provide data in exchange for a service.

Since these new EU provisions have been provided in the form of directives, with some room for choice left to national discretion, directly applicable rules will be set at national level (by 2022) through implementing legislations. New rules will be applicable along with other frameworks providing for specific remedies for non-consumers, or for hidden defects or providing for non-contractual remedies for the consumer against persons in previous links of the chain of transactions. Additionally, it remains to be seen if Member States will decide to extend the protection afforded to consumers also to natural or legal persons other than consumers, by extending the applicability of these directives, being allowed to do so. In such a case, implementing provisions might become relevant also for the purpose of contracts between ISPs and manufacturers, or them and the S-OTP provider, even with all of them acting in the capacity of professionals/businesses.

Therefore, to have a complete view of the applicable framework, it is necessary to wait for the enactment of national implementing rules. Despite the specific delineation of future national rules still to be adopted, some preliminary comments are outlined below:

The directives apply to contracts between consumers (e.g. purchaser of a vehicle or vehicle part, user of a mobility app) and '*any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including* indirectly *… for purposes relating to … trade, business, craft, or profession, in relation to contracts covered*' and including *platform providers*. In so far as VMs and ISPs could fall into such a broad definition, previously described rules on seller's/trader's liability and right to redress, as well as on the burden of proof *[see above in Section II, chapters 2.2.3 and 2.2.4]* are applicable to them.

While the DCD, on the supply of digital content and services, seems particularly relevant in the relation between the ISP or the VM and the end user, the SGD appears less relevant for ISPs (insofar as they do not usually sell material components of the vehicle or vehicle itself but only the app).

The SGD will be instead of use in the relation between the VM or seller and the user, because it covers the sale

[181] 2018 Deloitte Study.
[182] 2017 TRL Study.

of goods, for example a vehicle or vehicle's component with embedded digital elements which form part of the sales contract (either explicitly, or implicitly if the consumer could reasonably expect the digital element given the nature of the goods and taking into account any public statement or advertisement made – by or on behalf of the seller or other persons in previous links of the chain of transactions – such as a smart vehicle advertised as including a particular mobility application).

The SGD is applicable irrespective whether the mobility application or operating system (digital element) is

- pre-installed in the vehicle at the moment of the conclusion of the sales contract, or
- to be installed subsequently, or even
- downloaded through another device and being only inter-connected to the good (e.g. vehicle performing its functions with an application that is provided under the sales contract but has to be downloaded by the consumer onto a smartphone).
- supplied by the seller itself,
- supplied, under the sales contract, by a third party, such as an ISP (regardless of any licensing agreement with a third party which the consumer has to consent in order to benefit from the digital content or service).

In all such cases the SGD is applicable. If the installation of the digital parts of the vehicle forms part of the sales contract, which is assumed under the law, it has to be carried out under the seller's responsibility ,which might be the VM.

The VM selling the vehicle is also responsible for **any lack of conformity of the vehicle sold by him, including if resulting from an act or omission of a third party, such as an ISP, without prejudice to the right to redress** (pursuing legal remedies against the actual responsible). The details for exercising the right to redress, in particular against whom and how such remedies are to be pursued and whether the remedies are of a mandatory nature, are left to the relevant Member State's laws.

Likewise, **the SGD leaves to national laws to stipulate whether the consumer can also raise a claim directly against a person in previous links of the chain of transactions (e.g. the ISP), except in cases where a producer offers the consumer a commercial guarantee for the good**.

As a result, in case of non-conformities of the connected vehicle resulting from an act or omission of an ISP:

- Where the vehicle does not conform with the legal guarantee, the consumer could be allowed by national law to raise a claim either agaist the VM or directly agaist the ISP.
- Conversely, where the vehicle does not conform with undertakings falling under the definition of a commercial guarantee, the guarantor remains primarly responsible, despite any intervention of an ISP delivering digital services or content which affects the guarantee. The consumer will therefore always bring his claim agaist the VM (guarantor), who, in turn, and only after having paid full compensation, will be able to pursue remedies against the ISP, or any other person responsible in previous links of the chain of transactions.

However, Member States are allowed to set additional rules on associating debtors other than the guarantor (meaning that they could foresee forms of sole or shared responsibility), provided that they ensure a comparable level of consumer protection. Such rules would only be valid at national level.

Ultimately, both directives, albeit to different extents, also include digital content supplied on a tangible medium, as well as to the durable medium itself, which could be a smart vehicle. However, if (a) the vehicle functions even without the digital element or (b) the digital element is not understood as part of the contract, the contract for the supply of digital service (mobility app) should be considered to be separate from the contract for the sale of the good (vehicle / vehicle's component). In principle, and subject to different implementing choices adopted by Member States, the DCD will apply to the first contract, while the SGD to the second. This is even if the seller acts as an intermediary of the contract with the third party supplier (ISP).

3.3 Conclusions

The previous paragraphs propose a reading of existing regulatory and doctrinal framework, portraying and analysing the different interpretations that may have some relevance for ISPs in their activity of providers of mobility services, such as remote R&M.

What mainly emerges from the assessment conducted is a widespread uncertainty on the suitability and

therefore applicability of existing provisions. Absent solid court precedents to rely on, the outcome of liability claims involving mobility services offered by independent providers is extremely uncertain. The lack of uniformity of these rules across countries in fact hampers legal predictability. This is all the more if, as this Study suggests, judges will resort to extra-contractual liability rules and standards, set at national level, in order to bypass the legal hurdles that the application of current strict product liability rules entails, despite their uniformity.

In any case, in current EU legislation, the producer is fully responsible for the safety of the **final product as a whole** – possibly including products possessing software at the point when they are placed on the market – and remains fully liable even when the damage is caused *both* by a defect in the product and by the act or omission of a third party, such an ISP who accesses the car and provides a defective service. Still, if and to the extent the application or the device is considered a 'product' for the purpose of PLD, strict product liability may only apply for damages triggered by any defect present ***at the time of putting the product into circulation***. This should relieve, under today's framework, any possible concerns (of VMs or ISPs) on liability under the product liability framework for evolving or added technologies.

However, it is recalled that motor vehicles and all their elements, as well as any important[183] alterations to their original form ***after the product has been placed on the market, registered or entered into service***, are subject to safety approvals under the responsibility of their developer. It is hence well possible that mobility applications become subject to such regulatory approvals, pursuant to Type Approval Regulation. Also, it is currently up to the VM to ensure that its **vehicle or vehicle's components *are not designed to incorporate* strategies or other means that alter the performance exhibited during the type approval procedure when operating under normal conditions, exposing the vehicle to risks or cyberattacks**.

In line with this framework, the new SGD stipulates the VM's responsibility for any lack of conformity of the vehicle sold by him, including if resulting from an act or omission of a third party. For example, the lack of conformity under the VM responsibility could relate to an app or update provided by the ISP and needed by the vehicle to perform its functions and included (or presumed to be included) in the sale contract, even if installed in the vehicle at a later time and by the consumer himself. Unlike the product liability, which only encompasses **damages caused *by* the vehicle**, this framework on contractual liability also covers the case of **damages caused *to* the vehicle** by the embedded app's bad functioning, lack of update, or wrong installation.

In light of all this, it can be argued that vehicle security over the vehicle's lifetime ('cradle to grave') remains the prime responsibility of the VM, but subject to his possibility to later exercise right to remedies to the actual responsible, if different (e.g., the ISP), after having paid full compensation to the entitled subject.

A summary of possible liability claims against the VM under the current framework is proposed below:

VM				
Interested party	in the quality of seller of the connected vehicle	in the quality of seller or producer of the connected vehicle	in the quality of producer of the connected vehicle	in the quality of service provider
Liability towards	the consumer, purchaser of the connected vehicle	the **consumer**, purchaser of the connected vehicle	any **injured person** (or the **driver**, although when not directly injured, if called to respond with strict liability for road accidents and to compensate the victim)	*[see table below]*
Liability for	**Lack of compliance with legal guarantee of conformity** of the vehicle *including if resulting from an act or omission of a third party.* Notably: A) **incompatibility of:** ▪ **the description, type, quantity and quality, functionality, compatibility, interoperability and other features - including in relation to durability, functionality, compatibility and security**	**Lack of compliance with** additional undertakings assumed, notably: A) **commercial guarantees terms** and B) undertakings implied in **associated advertising** available at the time, or before the conclusion, of the contract also including non-conformities	**Material physical damage** caused by a defect in the vehicle or vehicle component, or app*. **Material economic damage** caused by a defect in the vehicle or vehicle component*, consisting in destruction or deterioration of items of property other than the vehicle, intended for private use or consumption.	

[183] I.e. those which may pose a serious risk to the correct functioning of the essential systems of the vehicles.

	(i) with that described in the sales contract; (ii) with that shown in the sample or model that the seller has made available before the conclusion of the contract; (iii) with that normal for goods of the same type and the consumer may reasonably expect (given the nature of the goods and any public statement* made by any persons in previous links of the chain of transactions, particularly in advertising or on labelling). ▪ **the fitness for purposes** (i) with that for which goods of the same type would normally be used (taking into account, where applicable, any existing law, technical standards or industry codes of conduct); (ii) with that for any other particular purpose that the consumer requires and has made known to the seller and that the seller has accepted; ▪ **the accessories and instructions** (i) with that stipulated by the sales contract (ii) with that that consumer may reasonably expect to receive; ▪ **the provision of information on and supply of updates** (i) with that stipulated by the sales contract (ii) with that that consumer may reasonably expect to receive; ▪ **the correct installation of the good**; B) Restrictions which prevent or limit the use of the connected vehicle, resulting from a violation of any (IP) right of a third party.	related to the digital element/app, if covered by the commercial guarantee provided by the VM.	*[*ONLY IF the judicial interpretation endorsed is that the the digital component/app present in the car when marketed is to be encompassed in the definition of 'product', as opposite to a service.]*	
Relevant moment for assessing liability	Non-conformities existing at the **time when the good was delivered or at the time/during the time when the digital element is supplied**, if the physical component was delivered earlier or in case of continuous supply.	Non-conformities existing at the **time when the good was delivered or at the/during the time when the digital element is supplied**, if the physical component was delivered earlier or in case of continuous supply.	Defects existing at the **time when the good is put on the market.**	
Main burden of proof	VM (with few exceptions)	VM	Injured person	
EU law applicable	SGD	SGD	PLD	

A summary of possible liability claims against digital service providers under the current framework is proposed below:

ISP					
Interested party	in the quality of service provider responsible in previous links of the chain of transactions			in the quality of trader (i.e. supplier of a digital service, "app")	in the quality of data controller or processor
Liability towards	The **VM** (who has previously compensated, in his capacity of **seller**, the consumer and exercises the *right to redress*) The **consumer** (purchaser of the connected vehicle) *only if foreseen by national law*	The **VM or OEM** (who has previously compensated, in his capacity of **producer**, the victim and exercises the *right to redress*)	The **VM or any other proprietary right owner**	The **consumer** (to whom the app is supplied under a contract)	The **data subject** (app user, vehicle driver, vehicle passenger, others)
Liability for	**Lack of legal conformity** of the vehicle *(see previous table)* if resulting from an act of omission of the ISP, such as the omission of an update, including a security update, which would have been necessary to keep the connected vehicle in conformity.	**Material physical or economic damage** caused by the vehicle or vehicle component due to a defect in the app. *Or any other damage foreseen by national law if a specific regime on service provider liability exists*	**Breach of IP rights**, e.g. occurred when developing the app.	**Lack of conformity** of the app with the contract terms, including regulatory requirements. Notably, regulatory requirements include A) **incompatibility of:** ▪ **the description, type, quantity and quality, functionality, compatibility, interoperability and other features - including in relation to durability, functionality, compatibility, continuity and security** (i) with that described in the supply contract; (ii) with that shown in trial versions or previews made available prior conclusion of the contract; (iii) with that normal for services of the same type and the consumer may reasonably expect (given its nature and any public statement* made by any persons in previous links of the chain of transactions, particularly in advertising or on labelling).	**Incorrect processing of in-vehicle or other personal data**, including A) processing without consent or lack of other legitimate purpose; B) incomplete information provided to data subject and other non-transparent processing; C) handling of non-relevant, inaccurate or superfluous data; D) lack of update or erase of data;

				▪ **the fitness for purposes** (i) with that for which goods of the same type would normally be used (taking into account, where applicable, any existing law, technical standards or industry codes of conduct); (ii) with that for any other particular purpose that the consumer requires and has made known to the seller and that the seller has accepted; ▪ **the accessories and instructions** (i) with that stipulated by the supply contract (ii) with that that consumer may reasonably expect to receive; ▪ **the provision of information on and supply of updates** (i) with that stipulated by the supply contract (ii) with that that consumer may reasonably expect to receive; ▪ **the additional undertakings** (i) with commercial guarantees provided (ii) with associated advertising available at the time, or before the conclusion, of the contract. B) **Lack of integration** of the app into the consumer's vehicle (if under the ISP's responsibility or due to issues with instructions given by the ISP) C) **Restrictions which prevent or limit the use of the app, resulting from a violation of any (IP) right of the VM or other third party**	F) storage of data for longer than the original purpose; G) lack of compliance with privacy by design or by default principles or lack of measures apt to guaranteeing security, avoidance of unauthorized access, accidental loss, destruction or damage of data. H) any other breach of GDPR or other data protection law.
Relevant moment for assessing liability	Depending on national law / contract between VM and ISP	Depending on national law / contract between VM and ISP	Varying according to applicable law	Non-conformities existing at the **time of supply**	Any time during data processing
Main burden of proof	Depending on national law / contract between VM and ISP	Depending on national law / contract between VM and ISP	Varying according to applicable law	ISPs (with few exceptions)	ISP
Law applicable	SGD referring to national law)	PLD and ECJ case law referring to national law	Trade secrets Directive; InfoSoc Directive; Database Directive; Software Directive	DGD	GDPR; ePrivacy Directive

Overall, what remains under each interpretation that may be endorsed, is the difficulty of whatever party will be deemed burdened with the *onus probandi* (usually the injured consumer/claimant) in singling out and demonstrating the chain of causality; if required, the existence of a duty of care on some operator in the supply chain and his failure to observe it (negligence); and, above all, the cause that led to the accident, which could be a defect in the vehicle, in the service attached, in the data relied on, but also a failure of the various systems involved, such as connection and infrastructure.

When the source of the defect is traced back to data, complications arise from the fact that data may change over time, due to action or even inaction; therefore liability will probably be better allocated by contractual means, especially in light of the new regulatory framework adopted at EU level.

When the source of defect is traced back to a 'product' (be it a vehicle, vehicle component, or even, in some readings, the mobility application/service), product defectiveness equally encompasses cases (a) where the manufacturing of the single *specimen* deviates from the intended design (e.g. failure of mass-production techniques), (b) of erroneous design of the device which is defect in the way the product was conceived (e.g. it does not provide necessary safety or it is unreasonably dangerous), or (c) where warnings about the potential dangers arising from the use of the device were not adequately signalled. The more technologically complex the product, the harder satisfying such evidence requirements – especially under (b) – is going to be.

In general, satisfying the burden of proof, both in cases of product and contractual liability, will entail accessing the information regarding the functioning of the device, or other data, which is not always possible, as it may include proprietor information or trade secrets. If such a burden is on the consumer, the latter will need to acquire an expert technician's opinion, and is anyway likely to fail, as the producer has no interest in sharing such information. Moreover, manufacturers in most countries might usually advance the development risk defence and maintain that the status of technical and scientific knowledge at the time the product was designed was such as not to allow the defect to be identified and addressed, substantially lowering the standard of liability.

In brief, the fact that compensation requires proof of a fault or defect, despite digital services/products non-deterministic autonomy and the complexity of proving causality, undermines the effectiveness of current liability laws, **dramatically lowering the chances of consumer's success in claims against manufacturers and/or ISPs**. By contrast, when the burden is on the seller of the product, or on the trader of the service (as it is under the

recent SGD and DSD) these may well use their technical information in order to gather the needed evidence, e.g. on their product or app conformity, functioning, security, etc., leading to a more balanced outcome.

Despite courts' rulings relieving the burden on the claimant, it remains that, in practice, the prevailing ground by far for rejecting claims has been the claimant's failure to either prove the defect or to link it with the damage, when product liability is invoked. Accordingly, claims under contractual law are expected to be favoured by claimants; sometimes, if allowed by the concerned jurisdiction, brought together with concurrent and more uncertain claims based on tort or product liability.

To conclude, it is recalled that the success of a claim is not impeded by an incorrect choice of applicable instrument: as noted, most claims have been in practice upheld by the national courts in favour of the injured person, sometimes based on the PLD, while other times based on a different legal basis, such as tort law or contract law, even if the claimant had invoked the PLD. Knowledge of and clarity toward the relevant surrounding framework is rather useful to predict legal outcomes and shape legitimate expectations.

Chapter 4. LIABILITY IN DIFFERENT DATA-ACCESS MODELS

With all data sharing solutions, damages caused *to the vehicle* seem to remain covered by contractual legal guarantees, with the burden of proof alternatively falling on the VM, ISP, or the consumer, pursuant to the SGD and the DCD; while for damages caused *by the vehicle* there is more uncertainty.

Under S-OTP, the direct access to data, granted to ISPs, while reducing the competition deficit vis-à-vis the VMs, seems not to entail major modifications in terms of liability allocation compared to alternative data sharing solutions, except a somewhat cutback of some VMs responsibilities.

In fact, in alternative solutions, vehicle resources and data access are filtered by the VM, who, for this, absorbs most responsibilities. In fact, as outlined in the 2017 TRL Study, all other solutions, by design, prevent any direct access to the vehicle and vehicle's systems by ISPs. In this respect, they attribute VMs a competitive edge concerning access to resources. As a counterweight, the **Extended Vehicle** provides clear security and safety responsibility wholly on the VM, who, placed as a privileged observer of transactions between the vehicle user/driver and the ISPs, is the best positioned to assume all monitoring obligations, and becomes accountable for that. The information asymmetry between VMs and service providers is mitigated under the **Shared Server** and **B2B marketplace**. Just like the S-OTP, under these, the VM gives up his position of 'gatekeeper' responsible for third parties' access and, with it, part of related responsibility. By relying on the Shared Server and B2B marketplace solutions, VMs would in fact transfer data from the vehicle to a third party's server managed by a neutral group of stakeholders. Consequently, they would not have any control over transactions with specific ISPs. However, the VM still remains the exclusive source of access to the car[184], therefore some room for related liability might remain on him, for instance toward which data (quantity or quality) is made accessible to the independent server, and how. In any case, depending on the practical arrangements with Shared Server, B2B marketplace or other systems, outcomes in terms of liability may vary to some extent: as an example, there could be room for more responsibility of the server provider, which reduces in turn that of VMs or ISPs.

Inversely, the intermediation of VMs fades with the S-OTP, since requested vehicle data are transmitted wirelessly to ISPs servers, upon user's consent. At first glance, the main difference with alternative models is hence that, only **under the S-OTP, responsibilities of VMs and ISPs are comparable**, as both are regarded as equal service providers. The secure S-OTP concept calls indeed for all service providers to have equal access and interaction to the data, functions, and resources of the vehicle.

[184] W. Kerber, 2018, Data Governance in Connected Cars: The Problem of Access to In-vehicle Data. Available at: https://www.uni-marburg.de/fb02/makro/forschung/magkspapers/paper_2018/40-2018_kerber.pdf

However, this mainly concerns liability for data access and/or data quality which, under alternative solutions is mostly on VMs, while with the S-OTP this is not necessarily so, as any certified service provider may freely accede the needed data, choosing which and how many. Only under the S-OTP, data liability may therefore attach **equally to the VM or the ISP, although this assumes that the fault or source for any data failure could be diagnosed and traced**.

Yet, the user, even where entrusted to autonomously decide on which data to share or which app to let enter the vehicle, cannot take on all responsibility for damages eventually caused by or to his vehicle, due to malfunctioning apps or due to the wrong interaction of apps in the car.

In cases where (i) due to the app, **the vehicle ceases functioning**, it is to be seen if the consumer was warned or sufficiently informed on how to install the app or on the need to update it. In any case, contractual terms and commercial guarantees from the VM or ISP could cover a wide range of hypotheticals, varyingly allocating responsibilities, including where the app was previously certified, correctly installed or updated, and yet ends up damaging the car or its software e.g. as it badly interacts with other apps[185].

In contrast, where (ii) due to the malfunctioning app, **an accident is caused with the vehicle** (personal injury, or damage to properties other than the vehicle), and the case is not covered by specific contractual guarantees, a tort action is liklely to be brought against the VM, by the driver – either directly, if the driver (or car's holder) is also the injured party, or as a redress, if the driver (or car's holder) has beared strict responsibility for the accident and has compensated a different injured party, such as a pedestrian or car's passenger. The reason why action could be brought agaist the VM is that, under the current framework and regardless the chosen data sharing solution, they have a specific 'duty of care' regarding the overall safety of the vehicle. In fact, compared to mobile phones, smart watches or computers and any other devices which may embed digital elements, vehicles are considered inherently more dangerous and are subject to additional safeguards and regulations, such as the requirements on type approval. As a result, the VM could remain accountable for authorising the introduction of risks in the vehicle, since this would imply infringing their duty of care, confirmed in the Type Approval Regulation, in the express obligation of ensuring that their vehicles are designed not to incorporate strategies or other means (broadly defined and possibly including apps) that alter the performance of the type approved vehicle exposing it to risks or cyberattacks (Art. 5).

Still, VMs' concerns of possible liability attaching to them for causes beyond their control can be relieved because:

- it has been argued that, despite uncertainties, **strict producer liability** would not cover risks added after the product is marketed [see above in this Section, chapter 3.1.2].
- the alternative **fault based extra-contractual liability** regime requires by definition proving the negligence of the VM in authorising a risk (non-respect of his duty of care), which should not emerge where the app is previously certified and authorised by an external certification body.

A 'filtrating' role taken on by the A-GW/A-GWA structure or, alternatively, by an independent public authority, similar to (or matching with) a type-approval authority, which authorises apps (and major updates) to run on the car would therefore enable to avoid that VMs review all the applications before being allowed onto the vehicle. The certification process should be initiated under the responsibility of any service provider (ISP or VM), willing to certificate their app or update and to verify its compatibility with existing softwares, similarly to the current system which requires manufacturers to apply for type approval of specific products.

On the other hand, previous certification under the S-OTP would also avoid that the user's consent is used to shield market operators from all responsibilities, despite the user is often not informed of (or able to understand) all consequences and possible technical issues triggered by consenting apps access.

[185] The SGD or DCD apply.

SECTION IV – Way forward

This Section anticipates the expected challenges and impacts of the discussed revision of the PLD and proposes a set of recommendations to properly balance vehicle liability, security, and unrestricted access to in-vehicle-data, functions, and resources, and, ultimately, to guarantee equal possibility for ISPs and OEMs to offer mobility services.

Chapter 1. EXPECTED IMPACT OF PRODUCT LIABILITY DIRECTIVE'S REVISION

1.1 The on-going revision

Thanks to its technologically neutral nature, the PLD has not required revision for more than three decades, being applied by courts to a wide range of products over the years, many of which did not exist when the directive entered into force in 1985. Nevertheless, in the face of the increasing challenges brought about by digital transformation and the development of the digital economy, there have been increasing calls to revise the PLD to respond to new challenges brought by technologies and data driven services.

The 2018 Commission evaluation, the first comprehensive evaluation of the directive, paid specific attention to the impacts of some relevant provisions of the PLD, including the definition of 'product' and 'defectiveness' and the allocation of the burden of proof on the injured person for obtaining compensation. The key objective of the evaluation was the very assessment of whether current definitions and provisions are still fit for purpose, especially in the context of technological developments.

Already identified legal gaps concern data ownership and the liability of automated systems and robots. During the Commission's evaluation, 657 stakeholders were consulted across the EU. Also, on 22 January 2020, the European Parliament Committee on Internal Market and Consumer Protection held a public hearing to discuss such issues with a range of stakeholders that set out their perspectives on the topic. The consultation revealed varying opinions. On the one hand, according to most businesses' feedback (particularly producers and insurers), there is not actual need to update the PLD in light of new developments as the directive is technologically neutral and liability issues are better addressed contractually[186]. A similar view had also emerged during consultations on possible amendments of product safety legislation relevant to product liability (such as the Machinery Directive, the Low Voltage Directive, the Radio Equipment Directive), where some industry stakeholders seemed to favour accommodating new technologies and risks associated with these technologies through harmonised standards representing state of the art, cautioning against substantive regulatory changes.

On the other hand, the vast majority of consumer organisations tended to view current rules as not being suited to accommodating new technological developments and favoured a revision of the PLD. However, stakeholders overall agreed as regards the expansion of the definition of 'damage' to include also **damages to data** or **digital assets**. Also, some stakeholders in previous studies have suggested that the fitness for purpose of the directive varies depending on whether the products concerned are aimed at consumers or professional users, although there is a considerable blurring in the delineation between the two.

In light of the changing technological landscape and the risk that products placed in the market evolve in ways that were not originally envisioned by the manufacturers, the European Parliament recommended[187] to maintain a risk-based approach (i.e. strict liability) to the regulation of liability, while reviewing some aspects to reflect the

[186] PLD Commission evaluation, Ibid.
[187] EP 2020 resolution on automated decision-making processes, Ibid.

challenges that AI poses. This is in line with the conclusions of 2019 NTF Report. Furthermore, the Commission, working in the same direction, through the NTF, is reviewing liability for emerging digital technologies under existing laws in Europe, pointing out that the future product liability regime in the EU will have to increasingly contend with a series of key features that will affect the production and distribution of products with new embedded technologies.

1.2 Expected challenges

There are a number of aspects a review of the PLD is expected to touch upon. Without the aim to be exhaustive, a few expected challenges and related outcomes are discussed hereinafter.

In the first place, the value chain dimension will be key to examine. Presently, the PLD allocates responsibilities to producers and suppliers within the supply chain using a terminology that may be considered somewhat out-dated compared with the NLF, which refers to 'economic operators' as a generic term, encompassing manufacturers, importers, distributors and authorised representatives. It is hence expected that key terms and definitions currently provided by the PLD will be reviewed in light of ongoing technological developments. Among others, the term 'defect' and 'product' might be updated, respectively:

- to include cybersecurity or other data risks, considering that cybersecurity vulnerabilities can result both in material and immaterial harm. Currently the damage focuses on the safety expectations of users which tend to refer instead to physical risks. One of the major challenges in defining safety expectations and security measures for IoT is the entailed complexity related to the heterogeneity of application areas.
- to include non-tangible items and clarifying if the term also incorporates software and apps and therefore to which extent the Directive is applicable to new technological developments and whether the strict liability rule applies to all kinds of software.

Other aspects touched by the revision may concern the application of liability in the case of refurbished and repaired products, especially in terms of determining who is the manufacturer and time-limits and exceptions to liability. Regarding the latters, the 10-year rule for the expiry of claims might be extended and the development risk defence redefined as it currently offers limits to the liability for products using new technologies[188]. Also, possible reshaping of the burden of proof might have a key impact on the whole framework, as the very balance between strict liability, on one part, and *onus probandi,* on the other, grounds the entire system. Legislative review is expected to take into account the ECJ rulings delivered so far on the topic.

A key challenge will be the allocation of responsibility for damages stemming from **products potentially changing their characteristics and functions throughout their lifetime**, for instance, as they (i) embed various technical features, applications or software from different sources that are subsequently installed and/or updated after the product has been placed on the market, or (ii) integrate an AI system that learns over time or performs automated tasks based on algorithms. In these cases, single ownership of key product components can be very uncertain and the application of the PLD might be problematic in particular due to product complexity and degree of automation.

If the directive's scope is enlarged as to clearly encompass also such kind of evolving products, without any substantial change in the liability mechanism, then a potential concern is that vehicle manufacturers and component suppliers might respond not only for defects in the material product but also in data, including wrong prediction based on it. Due to the large amount of data to be processed, including real-time data, operators are unlikely to be able to ensure constant and timely monitoring and early detection of irregularities in all vehicles using their components, especially where there is read and write access to the vehicle's systems and the vehicle is modified over time becoming *de facto* a new product.

[188] BEUC, 2020, Product Liability 2.0 - How to make EU rules fit for consumers in the digital age. Available at: https://www.beuc.eu/publications/beuc-x-2020-024_product_liability_position_paper.pdf

It is argued that attaching liability to VMs in this case might be unfair, especially where it is the third party technology added to the vehicle that exposes the vehicle as a whole to a safety risk and not a product component already present and under the VM's actual control. If the VM would bear the risks of any consequence of changed or added technologies in vehicles manufactured by them, they are likely to advocate for the possibility to test and certify, and ultimately select, applications before letting them be downloaded or installed in the vehicle, as risk appropriation goes hand in hand with risk management.

Likewise, if applications would be deemed 'products' under the new revised framework, then ISPs are likely to bear the risk coming form any third party alteration or update which ends up being defective on the ground of a presumed negligence in allowing unsafe changes to their service.

In so doing, the PLD would *de facto* end up **creating an after-market obligation to continuously monitor the product**, which today does not exist, since the producer is currently only liable for defect which exist at the time the product is put on the market, therefore solely for defects that are clearly under his control.

To justify a similar stricter regime, the legislator could argue that they are in the best position to control and maintain the correctness of data they rely upon, as well as to prove, if needed, that a dataset was already inaccurate due to negligence or fault of a previous operator in the supply chain, and obtain compensation from them. Strict liability usually responds, indeed, to a logic of identification of the better/cheapest cost avoider and taker of insurance or best positioned to avoid a risk. Whereby VMs and ISPs define, on a continuous basis, the features of the technology and provide essential backend support services, or decide when, where and how to use, maintain and repair the vehicle or update the application, duly informing the end user, they could be deemed in good control of possible risks, and hence in a position of avoiding harm. On this ground, VMs and ISPs may be called to respond in the first place, envisaging a system of strict liability borne by them.[189]

This is why it is paramount to have rules addressing the safety and security of S-OTP in the first place (or other data-access systems) – such as authorising, by means of a transparent and impartial mechanism, access to vehicle data, and applications or updates to be installed, and providing some warranty on the reliability of vehicle data freely accessed. Besides, it is recalled that, by definition, the S-OTP foresees that every third party developer is certified by a standardised procedure to gain access to the platform. This would offer a defence to allegations of liability arising from the inclusion of new services or updates in the vehicle, or from using vehicle's information freely accessed and relied upon, which turn out to be flawed. Incidentally, a similar objective is pursued by the type approval system legislation for motor vehicle components; requiring a certification mechanism is in line with existing framework on safety approvals which motor vehicles and their systems, components, separate technical units, parts and equipment are already subject to.[190]

It is clear that the more sophisticated a product – which may have embedded technology developed by a different operator – and a technology itself – which may develop thanks to continuous updates – the less actual control over the operation may be exercised by a single actor in the supply chain. Often, more than just one person may be deemed as having control, in a meaningful way, on the technology or complex product.[191] As a result, responsibility may lie across multiple economic operators in the value chain. It could therefore be expected that the new framework envisages some forms of responsibility for data processors or data controllers, and ultimately shifts from individual to shared responsibility, where several parties are held liable.

It is possible that a specific regime providing for a different degree of liability (strict, fault-based or mixed system) depending on whether the technology is deemed high risk or not is proposed. With shared responsibility, liability could be attributed to all operators, be it front-end or back-end. That is to say, both the operators who exercise a certain degree of control over a risk associated with the operation and functioning of the technology and who benefit from its operation; and those who, on an on-going basis, define the

[189] 2019 NTF Report, Ibid.
[190] See Type Approval Regulation.
[191] Or even none, in edge cases where the technology brings about a high level of automation, with resulting lack of possibility to effectively control the operation.

characteristics of the technology and provide the essential back-end data and support service, thereby also exercising a degree of control over a risk associated with the operation and functioning of the digital technology.

The operator identified as strictly responsible for damage or harm caused by his service would ensure that the operations of that system are covered by appropriate liability insurance[192], on the other hand, he should always be entitled to prove his noninvolvement in the causality chain, and/or redress to a different operator.

Also, as a consequence of an extension of the PLD scope, covering software updates or applications installed on a vehicle, time limits might be affected. If digital technologies added after purchase of the basic product will be deemed separate products, then a separate ten-year (or different) period running for each one of them is expected. However, it is not clear whether this would lead to an extension of the total time for filing a claim against the VM (as end manufacturer).

A further connected consequence would be the need to clarify on the concept of 'expected safety' (i.e. the current criterion which the PLD rely on, of the safety '*which a person is entitled to expect*'). Notably, in the context of evolving digital services and products, it is uncertain how legitimate safety expectations should be understood, so a review of this criterion might follow the scope enlargement, but the impact of a similar modification is difficult to anticipate.

Finally, the burden of proof on the victim, under a new framework, is expected to be further relaxed, possibly endorsing recent case law position, up to a shift upon the producer/service provider, if they are seen by the legislator as the more apt to locate and assess the source of defect, relying on their proprietary information and industry knowledge.

1.3 Possible impact:

Despite the argued flows of the interpretative option considering digital applications installed in the vehicle after purchase as products covered by the strict PLD regime, the possible implications for ISPs if courts would endorse this theory, or if legislator would codify this under a revised PLD clearly encompassing all kinds of technologies, are discussed below.

If the law or courts would consider the (remote R&M or other) software application developed by the ISP as a product, the ISP, in the capacity of its manufacturer, would bear strict responsibility for any material damage suffered by the injured person (i.e. the service user, driver, random bystander involved in an accident). This is without prejudice to additional liability claims ISPs may face due to contractual obligations they have with parties, in the capacity of suppliers of services or traders/sellers *[see above in this Section, chapter 2.3]* or due to general tort law or other relevant provisions, e.g. in relation to other types of damages[193]. The EU product liability regime would therefore serve as an additional route to claim for damage.

It would normally be on the injured person to demonstrate the actual damage; the defect in the software application/update; and the causal relationship between defect and damage, provided that this is not subject to review. As shown, courts (both at EU and national level) have shown some flexibility in this. For example, the requirements to prove the causal link or the defect have been relaxed. As for the defect, the injured person need not prove the exact flaw in the product that caused the injury. An unexpected failure in a product with no obvious alternative explanation is sufficient[194].

Concerning the damage to be proven by the injured person, the ISP would only be strictly liable for those damages defined in Article 9. The ISP may however respond in parallel also for other damages to the extent they are covered by national provisions (under strict or fault-based regimes). Damage under the PLD is (i) physical

[192] 2019 NTF Report, Ibid.; BEUC, 2020, Ibid.
[193] As per Art. 13 of the PLD.
[194] See e.g. Jurisdiction of ENgland and Wales, Case of 28 April 2008, Ide v ATB Sales Ltd, EWCA Civ 424.

damage to persons (death or personal injury); or (ii) destruction or deterioration of items of property other than the defective product, provided that they are intended for private use or consumption. It is argued that this does not include damage consisting in the loss or theft of personal data as a consequence of a defect in the software, as it does not amount of damage to 'a property item' nor 'physical injury'. Indeed, while physical damage also covers economic losses, such as incapacity to work, financial damage does not cover pure economic losses (i.e. a pecuniary loss not consequential upon injury or damage). As a consequence, and also in line with the Commission evaluation's findings, **infringements of privacy** cannot be regarded as damages covered by the PLD. It seems more appropriate to consider such cases as an infringement of personality, for which non-material damage under the applicable national law is due. This is also confirmed by the previously mentioned Bulgarian case[195] *[see above in Section II, chapter 6.3, box]*.

On the other hand, the ISP would be entitled to escape liability by demonstrating one of the exceptions reserved to the producer under Article 7. Notably, where the ISP's software application is regarded as a product component (by contrast to an end product), the ISP would also escape liability arguing that the defect is attributable to the design of the vehicle or embedded software designed by the VM, in which the R&M (or other) app has been installed or to the instructions given by the VM (exception under art. 7(f))[196].

It also stems from the PLD provisions (Articles 5 and 8) that:

- The ISP liability may be reduced or even disallowed when, having regard to all the circumstances, there was contributory negligence of the user, meaning that the damage is caused both by a defect in the 'product' (i.e the software application in this proposed reading) and by the fault of the victim; this may relate, for example, to inappropriate installation warned by the producer, e.g. while the vehicle is in motion, inappropriate settings or installation of third party software that is incompatible).
- The ISP remains fully liable when the damage is caused *both* by a defect in his 'product' and by the act or omission of a third party, such as the VM or/and the data supplier, who will respond jointly and severally for the whole damage. In this case, the ISP will retain the right to seek recourse from others contributing to the damage, according to the national provisions on right of contribution or recourse.

Whereas the software application would merge and interact with the rest of the software, operating as a whole with it, it may be very challenging to distinguish it from the rest of the already installed in-vehicle software and prove the source of a damage (i.e. what part of the software,or even of the vehicle at large, is defective). This might affect the actual possibility for ISPs to effectively argue that the defect stems from another (part of the) device or product (e.g. the vehicle as a whole), for which they are not responsible. While this issue now affects mostly the victim-consumer (who bears *in primis* the burden of proof), it is not excluded that the burden of proof regime be amended, further touching upon the different operators in the supply chain, who need to fairly allocate responsibilities among them (i.e. by exercising their right to redress).

Chapter 2. RECOMMENDATIONS

In light of the analysis above, some recommendations for the legislator are set forth. Recommendations aim at implementing fair rules that properly balance vehicle liability, security, and unrestricted access to in-vehicle-data, functions, and resources, and, ultimately, at guaranteeing the possibility for Mobility Clubs to offer the current and future services to their members. Each set of recommendations is contextualised and accompanied by a brief introduction.

[195] Bulgarian case no. 20942/2012.

[196] See Article 7 (f), under which the producer shall not be liable as a result of this Directive if he proves, in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.

1) Type and level of action: In general, a gap between the evolving technology and the codified rules of law persists. Legal doctrine often questions the extent to which regulatory changes are needed in response to technological progress and the risks inherent in codifying technology, as it usually changes faster than regulators. Although some industry stakeholders seem to favour accommodating new technologies and associated risks through harmonised standards representing state of the art, rather than through substantive regulatory changes, this Study diffusely remarks that current rules are not suited to accommodating new technological developments and favours instead a revision of the relevant framework. Indeed, new products and services are not to be deemed inherently less safe than traditional products, but consumers' trust and the uptake of new technologies will depend on whether they are *perceived* to be safe and on whether the legal framework is considered clear and effective to provide remedies to victims. Further critical thinking on the need for amending some established civil law rules on liability, keeping into account future needs and developments is therefore needed. Also, since practical liability implications of the chosen data sharing architecture typically depend on their exact features and concrete implementation, a clear set of rules on data sharing solution seems also necessary.

- *Citizens and business should be able to trust technology they interact with, having a **predictable legal environment** around the development and use data. Clear-cut rules on vehicle data sharing in general, and on the S-OTP functioning in particular, and addressing some liability concerns, are paramount. An **intervention at legislative level, in the form of binding acts**, is therefore preferrable over interventions in the form of soft laws or guidelines or over leaving technology unregulated.*

Different rules between Member States may hamper legal certainty and predictability, potentially leading to inconsistent legal solutions and affecting the EU-wide provision of data driven services. Furthermore, differences across national laws generate additional cost when operating across different jurisdictions.

- *A coordinated **EU approach** is the preferred option when updating the current legal framework for liability, compared to national initiatives. The role of EU legislation is also crucial to ensure that, as a matter of principle, certain essential conditions are met, in particular those identified by the C-ITS Platform (such as prior consent of the driver/owner of the vehicle in its quality of data subjects; fair and undistorted competition; data privacy and data protection; tamper-proof access and liability; data economy).*

- *The choice of intervention **in the form of regulations**, rather than directives, in compliance with subsidiarity and proportionality principles, might further reduce the scope for national discrepancies.*

2) Adapting the liability rules to digital contexts: In any case of more or less automated decision-making processes on which a technology or service relies upon, humans must always be ultimately responsible for decisions taken. Either by clarifying existing provisions or by enacting new legislation (or by a combination of the two), the goal pursued should be that from the perspective of the victim: ensuring equitable remedies, compensation and allocation of responsibility, while from the perspective of the innovators and companies operating in the EU, ensuring legal certainty and clear allocation of risks between those in control of them, key for good business development.

Accordingly, below are some considerations and consequent recommendations put forward, aiming to shape the set of requirements for the establishment of liability, regardless the specific (either already existing or new) act where the needed rules will be hosted.

It is noted that the more sophisticated and more autonomous a system, the less someone exercises actual control over the details of the operation. In some cases, defining and influencing the algorithms, for example by continuous updates, may have a greater impact than just starting the system. Control is hence a variable

concept, which varyingly affects multiple players at the same time[197]. In case of multiple operators, which could in abstract be held accountable, the NTF experts found that the risk of unexpected and unforeseeable outcomes (e.g. under a strict liability regime) is better borne by the party who (i) has more control over the risks posed by the operation and (ii) benefits more from it in terms of economic benefits which derives from the activity overall (although the benefit can often be very difficult to quantify), rather than the occasional harmed party. It also noted that emerging digital technologies are becoming more and more backend-focused, so there may be cases where continuous control over the technology remains with the backend operator rather than the frontend.

- *Liability rules should be shaped in order to provide desirable incentives to all players involved and maintaining a **consumer-friendly approach**, in line with recent EU initiatives of consumer protection in the digital context.*

- *In allocating liability among actors, causation should be seen as a key element. As a result, when determining the burden of prove, it should be considered **which party is best positioned to understand the cause of a risk, and to gather evidence on what** (e.g. the end user has a better knowledge on the damage suffered; while the producer or service provider on the service provided or product manufactured and their characteristics, functioning, absence of defects, need for updates).*

- *Systems based on **strict liability** can continue providing a good mechanism ensuring easier victim's compensation, rather than fault-based systems. In parallel, forms of **shared responsibility** instead of individual responsibility should be envisaged. The operators deemed liable in the first place should be those best positioned to ex ante (a) control, (b) minimize or reduce and (c) insure against the risks associated with the use of the technology, to grant prompt and adequate compensation ex post.*

Also, it has been highlighted that with digital devices or services the classic notions of defect and damage, which producer's or service provider's liability depends on, is controversial. Along with physical risks, connected vehicles and apps running on them can hide risks related to cybersecurity flaws, loss of connectivity, loss or corruption of data, wrong decisions taken by automatic or semi-automatic systems or by lack of needed update, etc.

- *The legal **notions of defect and damage** should be extended, thus encompassing defects such as unintended behaviour of the connected vehicle or application, cybersecurity failures, or lack of after-market needed updates, and damages related to data (e.g. loss, corruption) regardless they entail a purely economic loss in the classic meaning of the term.*

Under today's framework the *ex-ante* allocation of liability is hard to ascertain with a degree of certainty. Notably, doubts relate to which party is accountable for which damage when dealing with data-driven services because digital goods have blurred the distinction existing between products and services that permanently interact. Exclusive reliance on contractual agreements to overcome this issue is costly and not fully effective, as other rules may still come into play along with or in place of the agreed terms. Despite certain authors consider it reasonable to resolve the issue created by new technological developments by means of interpretation of the courts only, waiting for the future evolution of the new technologies, it seems that this is not enough. Conversely, the standardization of the liability rules and use of a mandatory regime, or a set of standardized regimes, would help address concerns and give ground to a healthier competition and a higher level of trust of users towards the new services. Tailored EU rules on service providers' liability might hence be needed,

[197] In this regard, the NTF Group observed that: "with emerging digital technologies, there is often more than just one person who may, in a meaningful way, be considered as 'operating' the technology. The owner/user/keeper may operate the technology on the frontend, but there is often also a central backend provider who, on a continuous basis, defines the features of the technology and provides essential backend support services. This backend operator may have a high degree of control over the operational risks others are exposed to. From an economic point of view, the backend operator also benefits from the operation, because that operator profits from data generated by the operation, or that operator's remuneration is directly calculated on the basis of the duration, continuous nature or intensity of the operation, or because a one-off payment this backend operator has received reflects the estimated overall duration, continuous nature and intensity of the operation." Ibid.

complementing the producers' liability framework and in line with the recent initiatives to adapt the EU consumer law *acquis* to the digital environment. As also noted by the NTF, the adequacy and completeness of liability regimes in the face of technological challenges are crucially important for society. The risks at stake if the system is inadequate or flawed or has shortcomings in dealing with damages caused by emerging digital technologies are very high, as '*victims may end up totally or partially uncompensated, even though an overall equitable analysis may make the case for indemnifying them*'[198].

- *Along existing rules, opportunely revised,* ***new ad hoc rules on the digital service providers' responsibility for damages*** *could be enacted, tailored on the characteristics of the AI and evolving products. As such, a new genus of responsibility would be envisioned, alongside and in addition to fault or negligence liability, consisting in the violation of rules of conduct required according to the highest standards of the industry. This seems preferable to simply extending the PLD scope.*

3) Revision of existing producers' liability framework: On balance, traditional concepts depicted and definitionw used in the product safety and liability framework are considered out-dated and not helpful in the context of new digital technologies. Both horizontal and sectorial rules, especially on extra-contractual product liability, need therefore to be reviewed to properly address liability related issues.

For instance, the framework is agnostic on how the safety of a product must be assessed, which can affect the ascertainment of which assurances a consumer is entitled to expect, and which tests a producer should be required to apply before bringing a product to the market, in case of innovative product categories.

- *The definition of 'producer', under the relevant set of rules, could be replaced by the more neutral and flexible concept of* ***'operator'****, encompassing all actors in control of the risk connected with the operation of the technology and benefiting from such operation.*

- *Acts included in the* ***Product Safety Framework*** *should be amended in line with the new PLD*

In parallel, as noted in this Study, the common rationale of the strict liability regime for products' defectiveness is the aim to increase the possibility of compensation of the victim/consumer, by relieving them from the difficult task of proving specific acts of negligence of the manufacturer, and shifting the onus on the latter, who is deemed in a better position to insure the loss and protect against a risk. Yet, as also diffusely stressed, this result is not reached under the current framework, despite the consumer-friendly approach of courts rulings. In fact, consumers end up bearing an excessive burden, being required to prove elements they do not have a real control on or knowledge of, and that the producers have no interest in disclosing. In turn, producers have a much better insight of the technical interactions of their devices, as well as possibility to access to their proprietary information which might be needed, and would therefore be at more ease if required to provide evidence of the (lack of) defect and causality. All the more, the mandatory equipment, in new vehicles – by virtue of Regulation (EU) 2019/2144 – of event data recorders that store a range of crucial anonymised vehicle data, might further facilitate producers' task of gathering the needed evidence on the actual functioning of their complex products. Such systems, recording and storing critical crash-related parameters and information shortly before, during and immediately after a collision, will indeed enable obtaining more accurate, in-depth accident data, which may help assessing the source of accidents in the precise vehicle type, variant and version identified by the recorder, and hence the defect.

- *To ensure that strict liability be a vehicle of social policy, geared toward consumers' protection,* ***the burden of proving defect and causation should be reversed*** *and borne instead by the industry operators, as they are in a better position to gather the needed information and to identify and demonstrate the source of defect. The injured party would still be required to prove the damage suffered.*

[198] 2019 NTF Report, Ibid.

Finally, while with traditional, non-connected vehicles, development is frozen at the time of launch of the vehicle, this is no longer the case with connected vehicles, which typically feature massive amounts of software code that determine the features and functions of the vehicle and evolve over the vehicle lifetime. Consequently, and how previously shown in this Study, the 'time when the product was put into circulation', in relation to which the defect shall be assessed, is a notion that triggers interpretative questions and uncertain outcomes, especially in the digital context.

- *The **time at which the product was placed on the market** should remain relevant when assessing defects only to the extent the producer actually looses control over its product after its release. If, conversely, after that point in time, the producer (or a third party acting on his behalf) still maintains a high degree of control over it and remains in charge of updating the initial product, the time of release of the initial product should not set a strict limit on the producer's liability. The time at which the product was placed on the market should therefore no longer be relevant for all kinds of defects.*

- *If all kinds of new technologies would be encompassed in a revised PLD, including so-called **evolving products**, what is key is that the party exposed to the associated liability remains in a position to control the risks. To avoid that a producer (or service provider) is held accountable for distractions or wrongful behaviours of other marker players, regardless his possibility to effectively monitor and avoid risks, the PLD revision shall not limit to broadening its scope of application, but should also carefully assess and adjust remaining rules, including exceptions and defences.*

4) Regulating access to vehicle data and resources: The mentioned reform of Type Approval Regulation, with its explicit acknowledgement of the technological progress in the sector, has shown some improvements in what concerns ISPs' access to RMI. However, this should not be seen as a final step for protecting effective competition in the automotive aftermarket. Indeed, the amendment of the previous Regulation on type approval of 2007 was driven by the urgent need to respond to issues related to the emission standards compliance, rather than to the emerging discussion about data access[199]. As a result, l unsolved problems remain regarding ISP's direct access to in-vehicle data and the IT-system of the vehicle: on the one hand, as remarked in the introduction of this Study, the OEMs seem to insist on limiting the scope of the data made available to ISPs; on the other hand, ISPs generally advocate for a far-reaching regulatory access solutions, even beyond RMI. As previously highlighted, the Extended Vehicle or Neutral Server Solution, as any choice of closed proprietary ecosystems, could hamper competition and innovation in the automotive aftermarket. Nevertheless, no comprehensive proposal for a regulatory solution on the access to in-vehicle data and resources has been advanced so far. Given the open set of R&M and other possible services offered by ISPs, competition, innovation, and consumer welfare could be protected through a regulated access not only for R&M services but also for other services that require access to data and that are complementary to the car users during connected driving, beyond R&M, and for which competition, innovation and consumer welfare issues do not differ.

The Type Approval Regulation already emphasizes that it is appropriate to develop principles for exchanges of vehicle component data between VMs and ISPs and notes the key role of standardization processes for such future exchange to be formally developed by the European Committee for Standardisation (CEN) '*reflecting the interests and needs of VMs and ISPs alike*'[200]. This implies a clear normative statement on the importance of preserving competition under the new technological frameworks.

In light of this, and of the evolution of the debate on data access and the Commission formal acknowledgement of the competition problems entailed by some proposed architectures, the time seems right for a clear step in the direction of a regulated access regime. The standardisation process for the exchange of vehicle data

[199] On this topic and view, see W. Kerber, D. Gill, 2019, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, 10 (2019) JIPITEC 244 para 1. Available at: https://www.jipitec.eu/issues/jipitec-10-2-2019/4917

[200] Recital 54 of the Type Approval Regulation.

between VMs and ISPs should not be misused for restricting competition, as also emphasised in the Type Approval Regulation programmatic statement.

- *A clear sector-specific **regulatory solution for access to in-vehicle data and resources** should be designed and developed at EU level, aiming to protect competition, innovation, and consumer choice. Notably, the far-reaching solution of a **S-OTP**, as recommended by vast literature, would lead to an open ecosystem of connected driving, in which the driver can freely choose between the providers performing services directly in the car.*

The regulatory proposal on the S-OTP solution should be designed with due account of safeguards that ensure security and safety of apps, thus reducing the risk for liability implications. These include, inter alia, a mandatory logging of data necessary to identify root cause, the strengthening of the already existing[201] obligation for VMs to provide **safe and secure environments for apps**, as well as **rules on validation processes** that avoid the need for VMs to review and accept all apps or service provider to be granted write access.

- *The S-OTP should be complemented by an **independent certifying body**, called to ensure that services making use of in-vehicle data and resources do not endanger the proper safe and secure functioning of the vehicles. This would permit liability to be passed along the chain, without the need for the VMs or ISPs to provide evidence that they had not acted negligently with respect to allowing access or acceding to the system and functions for interaction with the customer, because expected/foreseeable risks implied by their access are assessed and accepted beforehand, by a different actor or body. Each service provider should be responsible for applying for the certification, before marketing his app/service. Only this way user's consent can be deemed 'informed' and assume a real meaning.*

- *Alternatively, since what is key is that the party exposed to the associated liability is in a position to control and insure against the risks, each service provider could be tasked to **autonomously verify and validate his apps**, including their functioning on the device chocen by the consumer, taking on the responsibility to guarantee to the consumer their correct functioning.*

- *This solution could be achieved through **amendments to the Type Approval Regulation or adoption of a new act** (and consequent amendement to the Type Approval Regulation's data sharing rules). Amendement to the Type Approval Regulation should also include a clarification on whether digital apps or services running on the vehicle shall or shall not be type approved as the other parts and spare parts, systems, components, technical units, or equipments of motor vehicles.*

- *The scope of available data should be broadly defined to ensure that innovation through ISPs is not restricted, but also taking into account the legitimate interests of OEMs in terms of protection of business secrets, with a **differentiated approach depending on different types of data**.*

Finally, it is stressed again that, under any data sharing solution adopted, it is possible that VMs maintain a dominant role, as they have a role similar to mobile app store owners, to the extent they develop the car operating system where apps run. Like Apple and Google in the mobile field, VMs have indeed a dual role: (i) they distribute their own apps and services on their cars; and (ii) they manufacture the vehicle and provide the platform where ISPs may offer their services directly to the car users. This dual role, which creates both vertical and horizontal relationships, can entail competition issues, if VMs leverage their dominance in the upstream market (i.e. platform) via favoring its downstream division (i.e. apps) vis-à-vis their competitors.

- *Competiton authorities, already tuned into mobile app stores, should strive to implement classical competition rules into non-traditional digital markets, **ensuring fair competition between ISPs and VMs**.*

[201] Under Art. 13(5) of the Type Approval Regulation, as amended, manufacturers shall ensure that their vehicle or vehicle's components and parts are not designed to incorporate strategies or other means that expose them to risks, including in terms of cybersecurity.

Annex – Case studies

ITALY

1.1 Liability structure and different hypothesis

In the past, non-contractual civil liability was limited to cases of **fault-based liability** (*i.e.* the obligation to pay compensation was only triggered for those who had unlawfully caused the damage in question). The process of industrialization showed the limits of the fault-basis system, because a culprit is not always identifiable in relation to damage; and damage, according to the principle of "*neutrality*", must always be compensated for.

Therefore, a plethora of liability cases without fault have arisen (Art. 2050 et seq Italian Civil Code), and have converged into two different kind of liability, known as *"**strict liability***" and "***liability aggravated by the event***". In any case, non-contractual general liability holds a limitation period of **10 years** from the event in question and the burden of proving the damage is on the injured party.

The "*strict liability*" entails the liability of the defendant, irrespective of fault, whenever it is reasonable to assume that a given person has acted in a controlling or responsible manner. The Italian Civil Code knows a lot of cases under the umbrella of "*strict liability*". For example, Article 2049 of the Civil Code provides that the "*the supervisor of the employees is liable for damages caused by them in the course of their work*", irrespective of actual fault. This principle can be summarized in the Roman proverb "*et eius incommoda et eius commoda*", which means that if a person takes advantage of the work of others, he or she is also responsible for it. Therefore, in the case of strict liability, the liability arises automatically, regardless of fault.

On the other hand, "*liability aggravated by the event*" represents all the scenarios of strict liability in which the author can go guilt free, only providing in the court proceeding the positive proof of an external cause (*i.e.* act of natural t, intervention by third party and/or conduct from the injured party) which, due to its unpredictability, exceptionality and inevitability, is completely beyond the sphere of control of the operator of the dangerous activity and, therefore, the only cause of the damage. Therefore, in those situations, the courts require not only the absence of fault, but rather proof of a fact extraneous to their conduct capable of breaking the causal link between their conducted the harmful event suffered by the victim. This phenomenon, albeit allowing the defendant to prove his innocence, still represents strict liability given the difficulty of proving the impact of external causes (known as *probation diabolica*) on the causal link.

Therefore, giving a macro framework of the liability system in Italy there are three type of liability: fault-based liability (the general rule), strict liability and liability aggravated by the event; the last two being in practice the same given the high evidence threshold required to discharge liability.

While the Italian Civil Code has already presumptively categorized the liability a given type of damage warrants, the situation is different in the application of the European directives[202] or scenarios that are not yet regulated by the law, such as artificial intelligence and OTP. In the specific field of ISP and/or OTP in applications of AI applications, the applicable discipline is a mixture of different legal guidelines and EU directives.

[202] Regarding Directive 72/166/EEC, Directive 84/5/EEC and Directive 90/232/EEC (insurance and regulation of civil liability for damage caused by accidents arising out of the use of motor vehicles), according to case law, the directives do not aim at harmonising the laws on civil liability in Member States. In fact, the directives do not specify the type of civil liability - strict or negligent - to be covered by insurance. Therefore, the Court of Justice deduced that, in the absence of common legislation, the choice of the civil liability regime applicable to claims is a matter for the Member States.

1.2 Liability in the event of defective product and rules implementing the Product liability directive

The issue of product damage led to the formulation, at EU level, of a harmonized framework on producer liability for defective products, which was introduced by Directive 85/374 /EEC[203], known as the Product Liability Directive (the "**PLD**"), which aimed to identify a unitary model of producer liability.

In Italy, the PLD was transposed by Presidential Decree No 224 of 24 May 1988 and, subsequently, by the Decree no. 206/2005 (known as the Consumer Code), that replaced the entire discipline[204]. Therefore, in Italy the liability of defective products is set entirely within the Consumer Code and provides for the following main aspects:

- According to Article 117, a product is '*defective*' when it does not offer the safety that can legitimately be expected, taking into account all the circumstances, including, in particular, the way in which it has been presented, its characteristics, the instructions and warnings given, the use for which the product may reasonably be intended and the behavior which, in relation to this, may reasonably be expected. The defect thus consists of an unexpected insecurity and is a relative, not an absolute, notion.[205]
- According to Article 123, death, personal injury, and property destruction or deterioration of tthings other than the defective product itself can be compensated for. In essence, the discipline covers two types of damage, personal injury (physical integrity), and damage to things other than the defective product (provided they are things intended for private use). The damage to property shall be indemnifiable only to the extent that it exceeds the sum of EUR 387.
- Potential claimants include not only the injured user, but also anyone who, although not user of the defective product, has nonetheless been damaged by the defective good because of its use by others (also known as 'spectators').
- Article 120 divides the burden of proof between the "*damaged party*" and the "*producer*" on the basis of the distinction between the facts that constitute the right of the damaged party and those that exclude the producer's liability. The injured party must prove, in addition to the damage, the existence of a defect in the product and the causal link between the defect and the damage. The object of the burden of proof *vis-à-vis* the aggrieved party is commonly understood to mean that the defect to be proved is not the defect in design or manufacture (from a technical point of view), but the product's unsafety. Thus, proof of product unsafety is achieved as soon as it appears that the damage was caused during normal and proper use of the product (*i.e.* in the presence of a product defect)[206].
- Article 125 provides that the right to compensation shall expire **three years** after the day on which the injured party knew or should have known of the damage, the defect, and the identity of the liable party. On the other hand, Article 126 provides that the right to compensation expires at the end of **ten years** from the day on which the manufacturer or importer in the European Union put the product that caused the damage into circulation.

In light of the aforementioned principles, it can be observed that the PLD liability is an example of *liability*

[203] 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; OJ L 210, 7.8.1985, p. 29–33.
[204] With reference to the general discipline, see G. ALPA, R. BIN, P. CENDON, The liability of the producer, in Tratt. dir. comm. and dir. publ. ect., directed by F. GALGANO, Padua, 1989, and spec. G. ALPA, The implementation of the directive in EEC countries; AA.VV., The damage from products, edited by S. PATTI, Padua, 1990; C. BALTHASAR, Producer liability: compensable damage, burden of proof and legal logic, in Danno e resp., 2014.
[205] Cfr. Court of Palermo, judgment n. 6589 of 17 November 2015 – "In particular, the Court of Palermo has condemned a car dealer to replace a motor vehicle purchased by a consumer on the ground that the vehicle had defects that made it not consistent with the contract of sale. In particular, the Court of Palermo ruled on the matter of a consumer's remedies in the event of the purchase of goods with serious defects making it not conform with the contract of sale".
[206] See also Court of Justice, 5 March 2015, C-503 e 504/13, Boston Scientific Medizintechnik GmbH.

aggravated by the event. In fact, according to Article 118 of the Consumer Code, the producer of the product may exclude his own liability, proving a fortuitous event and, therefore, that the defect that caused the damage did not exist when the manufacturer put the product on the market and/or the possibility that the state of scientific and technical knowledge at the time the product was put on the market did not allow it to be considered defective. In this specific case, the producer must prove that he had taken, at that time, both the control measures (to ascertain the defect) provided for by the legislative or regulatory framework and the measures known on the basis of scientific and technical knowledge at that time (even if not provided for by law as mandatory and whatever the cost and complexity). If the liability of the producer is established in court, then, according to the Consumer Code, the producer is obliged to withdraw and/or recover defective products from the market and compensate the damage suffered by consumers [207]..

1.3 Civil Liability for unlawful treatment of personal data

In Italy (as in all Member States), Regulation No. 2016/679, better known as GDPR, is directly applicable and sets forth an entire discipline to better control and/or regulate the personal data in various contexts. [208]

The GDPR affirms the right of the data subject, when harmed, to obtain compensation for the damage suffered. Thus, this right arises when a breach of one of the provisions sanctioned by the GDPR has been made through conduct of the controller, joint controller or processor, which may have been active or omissive, and will be sought, together with compensation for damage from the controllers, joint controllers, and processors of personal data[209]. Additionally, Article 82 provides that the unlawful processing of personal data furnishes the consumer with the right to compensation for damage, both pecuniary and non-pecuniary, regardless of whether a crime is established, for the sole fact of having violated the principles and rules of lawfulness of processing data.

In general, according to the GDPR, the controller shall be liable where he is involved in the processing which, by infringing the GDPR, has caused the damage, whereas the data controller shall only be liable for the damage caused by the processing if he has failed to comply properly with the obligations laid down by the GDPR for controllers, or if he has acted in a manner different from or contrary to the lawful instructions given to him by the controller in respect of the processing of his data.

In this regard, the GDPR has introduced the principle of accountability, whereby the data controller is required to demonstrate that it has taken all legal, organizational, and technical measures to ensure the protection of personal data, including through the development of specific organizational models. The data controller must also ensure the effectiveness of the measures taken and demonstrate, on request, that it has taken them

[207] Cfr. G. Ponzanelli, Responsabilità oggettiva del produttore e difetto di informazione, in Danno e resp., 2003; R. Frau, in Corr. giur., 1987, p. 99. The Court of Appeal specified that if the producer is not known, it is up to the supplier to communicate all the data in his possession (Appeal. 1° June 2010, n. 13432); in the case law of the Court of Justice, see ECJ, 10 January 2006, C-402/03, Skov Æg.
The Council Directive 85/374 / EEC of 25 July 1985 concerning liability for defective products must be interpreted as: - precluding a national rule according to which the supplier is liable, beyond the cases exhaustively listed in Article 3 (3) of that directive, for the faultless liability which the directive establishes and imputes to the producer; - not precluding a national rule according to which the supplier is obliged to bear unlimited liability for the producer's fault.

[208] 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); OJ L 119, 4.5.2016, p. 1–88.

[209] See Cass. 04 June 2018, n. 14242. On the notion of "manager" and "treatment", see Court of Just. May 13, 2014, C-131/12, Google Spain. Article 2, letters b) and d) of 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, must be interpreted as meaning that, on the one hand, the activity of a search engine consisting in finding information published or entered by third parties on the Internet, in automatically indexing it, in temporarily storing it and, finally, in putting it disposition of Internet users according to a specific order of preference, must be qualified as "processing of personal data", pursuant to the aforementioned article 2, letter b), if such information contains personal data, and that, on the other hand, the manager of said search engine must be considered as the "controller" of the aforementioned treatment, pursuant to article 2, letter d), above.

properly. This principle implies that it is up to the data controller to identify how to comply with the requirements of the provision, adapting them to the concrete case, taking responsibility not only for implementation, but also for balancing the legitimate interest in processing against the interests or the fundamental rights and freedoms of the data subject that require the protection of personal data[210]. Moreover, when claiming compensation, the data subject must prove the existence of the damage and its quantification, the existence of conduct in breach of data protection legislation and the causal relationship between the first two elements; in order to be exonerated from liability for the damage, the data controller or processor must prove that the damaging event is in any case attributable to him.

Italy, in order to transplant the GDPR, has adopted the Legislative Decree No. 101 of 10 August 2018[211]. The above-mentioned Decree does not provide for specific civil liability cases and therefore, necessarily finds application within Article 82 of the GDPR. Despite the lack of a specific liability regulation, the European provision appears to be in line with the tendency to extend the area of compensation for non-asset damage, thus allowing compensation for non-asset damage even in the absence of a crime, provided that a fundamental personal right of constitutional relevance has been harmed. Thus, it is in the contract between the ISP and the consumer that the areas of liability must be defined[212].

1.4 Liability in artificial intelligence – smart car cases

In Italy there is no specific provision regarding the liability in and/or use of AI. The lack of a regulation is due the recent application and implementation of AI and the difficulty in identifying the person responsible for the damage (on a fault-based system model) nor the person responsible for controlling/supervising the event (on a strict-liability model). Furthermore, part of the doctrine thinks that, given the complexity of the operations and the unpredictability of the outcomes, a better solution could lie in the adoption of a new approach that, going beyond the traditional conceptual model based on error and fault, is based on a criterion of risk allocation, so that what matters is not the identification of who actually commits the error, nor the error committed.

Therefore, due to the discrepancy of views in the regulation of AI, the Italian Court has adopted a particular approach to ensure – in any case – the right compensation to damages arising from AI and using the general norms set forth in the Civil Code by analogical or extensive interpretation.

With specific view of the application of AI in products, it must be underlined that the question of the identification of the liable party in the event of damage to property or persons resulting from AI applications also arises with respect to the identification of the liable party in the event of injury or damage resulting from a product incorporating AI. Where the result of the processing carried out through the use of AI cannot be controlled ex ante and is characterized by a certain degree of processing autonomy, the person responsible may be the author of the program, the producer, the vendor, or the user of the program[213].

In the White Paper on Artificial Intelligence[214], the Commission stressed that consumers must expect the same level of safety and respect for their rights, regardless of whether a product or system is based on AI. However,

[210] According to Article 24 of the GDPR, related to the principle of accountability, "The controller shall implement appropriate technical and organizational measures to ensure, and be able to demonstrate, that processing is carried out in accordance with this Regulation. Those measures shall be reviewed and updated as necessary."

[211] Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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).

[212] F. PIRAINO, Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, in Le nuove leggi civili commentate, 2017, 40, 2, pp. 369-409.

[213] In general, on the subject, v. M. BASSINI, O. POLLICINO, Artificial Intelligence Systems, liability and accountability. Towards new paradigms? in Artificial Intelligence, Personal Data Protection and Regulation, F. PIZZETTI (edited by), Milan, 2018; G. Mazzini, A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law, in A. DE FRANCESCHI - R. SCHÜTZE (eds.), Digital Revolutions - New challenge for Law, Munich, 2019, p . 4 ss.

[214] COM (2020) 65 final.

determining the characteristics of AI can make it difficult to enforce existing legislation (e.g. uncertainties surrounding the application of the liability regime in the face of possible accidents caused by self-driving cars). In this case, it may be difficult to prove that the product is defective, the damage caused, and the causal link between the two. Furthermore, in its resolution of 20 October 2020 – "*Recommendations to the Commission on a liability regime for artificial intelligence - the European Parliament*", the European Parliament notes that physical or virtual activities, devices or processes that are driven by AI systems may technically be the direct or indirect cause of damage or harm, but are almost always the result of someone's creation, deployment or interference with the systems and notes that there is no need to give AI systems legal personality.

It is therefore proposed that a regulation be adopted covering any virtual or physical activity, device or process driven by an AI system that has caused damage or harm to the life, health, or physical integrity of a natural person, to the property of a natural or legal person, or that has caused significant non-pecuniary damage resulting in verifiable economic loss, as well as any contract between the operator of an AI system and a natural or legal person who is the victim of damage or harm because of an AI system that circumvents or limits the rights and obligations set out in the regulation. Moreover, the concept of "*product*" in the PLD should also be amended, since it currently covers the mere material component, whereas for the artificial intelligence component it is a question of analysing whether and to what extent the intangible and autonomous element prevails over the activity for which the product is intended. In fact, a device equipped with AI hardly falls within the notion of product under the PLD.

1.5 Conclusion/ practical applications

Although there is no case law on either defective automatic automobiles and related liability or OTP, the existing discipline is capable of ensuring innovative options in ensuring liability for the producers and distributors of "smart" cars, (*i.e.* in terms of allocation, forecasting and rationalisation of production and product liability, as well as of co-responsibility extended to the "*producer*" of the "*artificial intelligence*" component; or, better, extended to the multiple "producers" of components of that component: think of the creators of the algorithm governing the self-learning car).

Therefore, the applicable discipline is the result of a plethora of elements, including the judicial approach. In some cases, it is also possible to invoke an "*algorithm liability*", and therefore the potential extension of the liability for defective and harmful products also to the person who "*supplies"* the "*algorithm*" component to the manufacturer of the "*smart*" car. The result achieves a balance of, on the one hand, ensuring direct exposure to product labiility for co-producers of (''immaterial'') component of the final good; whilst, on the other, granting said producers with rights of redress against mediated agents and other intermediaries in the supply chain in relation to such product liability claims.

Therefore, considering that no specific provisions are applicable for AI, the smart car can be regulated by the plethora of norms set forth in the Civil Code. Thus, specifically, in the context of self-driving cars, the driver is liable both as ***''driver''*** (specifically under Article 2054 of the Civil Code), as "***the person in control of the artificial intelligence that drives the vehicle***" (specifically ex art. 2054 of the Civil Code); and as "***the subject in charge of managing the artificial intelligence that governs the automated traction of the vehicle***".

SPAIN

2.1 Liability structure and different hypothesis

The liability arising from an unlawful/extra-contractual act in Spain is governed by Article 1902 of the Código Civil

which sets forth that "a person who, as a result of an act or omission, causes damage to another person through fault or negligence is obliged to repair the damage caused". Overall, Spain has a typical European liability system, but what characterizes it most is the short limitation period for the right to compensation: one year from the damage or knowledge of the damage.

Going forward, Spain has a duplex liability system: the general rule set forth in Article 1902 represents an implication of a fault basis system, complemented by an exceptional *ad hoc* strict liability regime connected to the specific allocation of risks[215]. Behind this imposition of strict liability through special rules lies the idea that these cases are exceptions to the general rule of fault-based liability. Inevitably, this approach leads to the exclusion of analogical application of strict liability by the courts and, in some cases, also to the exclusion of extensive interpretation of already established cases.

Consequently, these gaps risk being filled by fault-based liability 'palliatives', with results that negatively affect the coherence of the legal system. In Spain this problem has been highlighted by part of the doctrine, pointing out how these complex and artificial procedures can alter the meaning and scope of liability for fault. Moreover, this model requires the legislator to be constantly active in adapting the laws to progressive technical and scientific development. Among all the positive aspects, the possibility for the legislator to assess all the interests at stake is often mentioned, giving him the possibility to apply strict liability on a case-by-case basis. Despite all the advantages, the model also has several shortcomings. As mentioned above, the enactment of several special laws is a common practice in many legal systems, yet over time this practice has become the target of severe criticism as a means of treating similar cases differently. To this end, it has been pointed out, on the one hand, that the enumeration of special cases of strict liability does not follow specific criteria; whilst on the other, that it seems impossible to exhaustively list all risks that may be subject to the principle of strict liability and regulate them entirely.

2.2 Liability in the event of defective product and rules implementing the Product Liability Directive

Civil liability for defective products in Spain is regulated by European Union law, specifically the (Directive 85/374), which was implemented into Spanish Law Law 22/1992 of 6 July 1992 and has become an integral part of the Spanish Consumer Code, known as *Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios* (also called "TRLGDCU").

According to the specific regulation of product liability (included in Chapter I, Title II, Book Three of the Consolidated Text of the General Law for the Defence of Consumers and Users) Art. 135: *"... manufacturers shall be liable for damage caused by defects in the products they manufacture or import*". The general principle of Article 135 TRLGDCU is to be read together with Articles 128 - 149 TRLGDCU stating that "Every injured party has the right to be compensated under the terms established in this Book for the damages caused by the goods or services...", noting that the actions for such damages do not affect "...other rights that the injured may have to be compensated for damages, including moral damages, as a consequence of contractual liability, based on the lack of conformity of the goods or services or any other cause of non-compliance or defective performance of the contract, or liability extra-contractual to that place". Although the TRLGDCU makes no explicit reference to the strict character of the liability of the manufacturer, importer or supplier, this condition cannot be denied to the liability regime enshrined in the above-mentioned regulations.

Regarding the burden of proof, although Art. 139 TRLGDCU exempts the injured party from having to prove the fault of the producer, it does not exempt them from proving the damage, the defective condition of the product nor the causal link between the two. These requirements s are in accordance with the general rules of the

[215] Those provisions are set forth both in the Spanish civil Code (Código Civil, arts. 1905, 1908 c.2 and 3, 1910) and in some special legislations, like the one enacted to adopt the PLD.

distribution of the onus probandi. Moreover, with respect to causation, Art. 137(2) TRLGDCU specifies that it is sufficient to prove that the product which caused the harm did not offer the safety normally provided by other products of the same series[216].

Article 140 TRLGDCU lists the grounds for exemption from liability for defective products. According to the prevailing doctrine, this is a mandatory provision, intended to attenuate the strict character of liability. In this respect, the doctrine has argued that it would no longer be a strict liability but a "*quasi-strict*"[217], "*qualified*"[218], "*relative*"[219] or "*attenuated*"[220] liability.

In particular, strict product liability would be justified in light of two reasons: (i) the producer is responsible for the risks generated by his goods, in light of the connection between profit and risk; and (ii) the producer is best placed to minimise the risk of damage caused by the distribution of the product and can do so through the application of precautionary measures in the design and during production.

2.3 Civil Liability for unlawful treatment of personal data

Spain is a country where the culture of data protection is deeply rooted. In the circumstance that a person suffers damage as a result of the processing of their personal data, they may exercise, according to the characteristics of each case, various actions for compensation.

In particular, the affected party may have recourse to the action provided for in Article 9.3 of *Ley Orgánica* 1/1982 on compensation for unlawful interference with the rights to honor, privacy and self-image, as well as to the general civil liability for negligence of Article 1902 of the *Código Civil.*

In addition to these actions, it finds applications within the regulation set forth in Article 82 of GDPR, aimed at obtaining compensation for damages suffered against the data controller or data processor who has breached data protection rules. This new uniform and directly applicable civil liability regime for damages resulting from a breach of data protection rules clarifies some uncertainties that were generated by the previous system and also includes some regulatory innovations. It should be noted that Article 82 of the GDPR, which entered into force, like the rest of the Regulation, on 25 May 2018, contains a liability regime that is directly applicable in all EU countries, replacing the application of the various national legal rules which, in implementation of Directive 95/46/EC, had recognized a right to compensation for damages arising from breaches of data protection law.

With a specific view to Spanish regulation, the most frequent claims are for compensation of non-pecuniary damage[221]. This type of compensation can be found in cases of improper inclusion in debtors' registers; violation

[216] M. PASQUAU LIAÑO, El defecto de seguridad como criterio de imputación de responsabilidad al empresario de servicios, in Responsabilidad civil por daños casusados por servicios defectuosos. Daños a la salud y seguridad de las personas, A. ORTÍ VALLEJO (dir.) and M. C. GARCÍA GARNICA (coord.), Aranzadi, Pamplona, 2006, p. 71. In giurisprudenza, v. SSAP de Almería del 17.05. 2004 (JUR 2004, 193357), of Cordoba of 11.01.2007 (JUR 2008, 140551), of La Coruña of 29.07.2004 (JUR 2005, 32723), of Pontevedra of 08.05.2008 (JUR 2008, 287766), of Santa Cruz de Tenerife of 15.03.2006 (JUR 2006, 153965).

[217] C. LÓPEZ SÁNCHEZ, El menor, sus juguetes y la responsabilidad civil, in Perfiles de la responsabilidad en el nuevo milenio, J. A. MORENO MARTÍNEZ (coord.), Dykinson, Madrid, 2000, p. 668; J. M. SOTOMAYOR GIPPINI, La nueva Ley sobre responsabilidad civil por los daños causados por productos defectuosos", in RES, n. 79, 1994, p. 73.

[218] R. JIMÉNEZ DE PARGA CABRERA, La Ley reguladora de la responsabilidad civil por daños causados por productos defectuosos en el marco del moderno derecho de la responsabilidad de acuerdo con las normas comunitarias europeas y de derecho comparado, in Estudios jurídicos en homenaje al Profesor Aurelio Menéndez, J. L. IGLESIAS PRADA (coord.), vol. III, Civitas, Madrid, 1996, p. 2898.

[219] L. GAZQUEZ SERRANO, La responsabilidad civil por productos defectuosos en el ámbito de la Unión Europea: Derecho Comunitario y de los Estados Miembros", in Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro, n. 32, 2002.

[220] J. SANTOS BRIZ, La responsabilidad civil. Temas actuales, Montecorvo, Madrid, 2001, p. 429.

[221] Cfr. C. GÓMEZ LIGÜERRE, Concepto de daño moral, in F. GÓMEZ POMAR, I. MARÍN GARCÍA, Ignacio (Dirs.), El daño moral y su cuantificación.

of the digital right to be forgotten[222]; non-consensual disclosure of data on work dismissals; illegal access to computerized medical records; and the improper inclusion of personal data in police records.

In cases where personal data security measures are insufficient, it is possible for a person to illegally access and obtain a copy but not use it immediately to the detriment of the owner. However, Spanish courts are reluctant to allow compensation for uncertain damages. The increased risk of a future harmful use of personal data does not meet the requirement of certainty of the damage in its existence and amount. Moreover, although Spanish courts have adopted a broad conception of non-pecuniary damage, only states of anxiety or distress caused by a possible future event of which there is medical certainty should be compensated.

2.4 Conclusion/ practical applications

In lack of a specific regulation on Spanish ISPs and/or OTP, it is possible to derive some indications from the product liability regulation in force in that jurisdiction. It is therefore possible to foresee different types of liability, specifically:

- *Strict Liability*: the producer shall be liable for damage caused by the product's defect unless they proves the concurrence of those causes of exemption provided for in Article 140 of the TRLGDCU. Article 140 of the TRLGCU provides some grounds for the exclusion of liability, among these the exclusive fault of the victim. In these cases, the causal link between the vehicle defect and the damage would be broken, given the negligence of the injured party.[223]

- *Joint Liability:* the supplier of the raw materials and the producers of the byproducts incorporated into the final product, the distributors and the retailers to the final consumer will be liable. This is a system that promotes the special protection of the victim, as it allows the victim to turn against any possible liable party in order to have the damage suffered repaired.

Therefore, it can be affirmed that, according to the general rules and the ad hoc rules for service providers, whenever the existence of a defect in the autonomous vehicle and its causal link with the damage suffered is established, the imprudent or negligent behavior of the user with respect to their vehicle must be assessed in order to proportionally reduce the manufacturer's liability. Therefore, if only and exclusively the user is at fault, there will be no liability attributable to the manufacturer and no legal consequences of the protection provided can be demanded from him. Otherwise, the service provider shall be liable for the damage caused, and the relevant legal action shall be time-barred within **one year** of the damage being suffered.

FRANCE

3.1 Liability structure and different hypothesis

France, like other countries with a Romano-Germanic legal tradition, has built a general regime of non-contractual civil liability on the notion of **fault** and the right to damages is prescribed in **10 years**.

The huge number of accidents caused by the onset of industrial and technological progress, as well as the impossibility of identifying liability under the cover of fault, warned jurists against a generalised application of fault-based liability. Thus, there has gradually been a phenomenon of 'erosion' or even 'inevitable decline' of fault-based liability.

[222] STS, 1ª Pleno, n. 210/2016, del 5 aprile (MP: Rafael Sarazá Jimena).
[223] The Supreme Court ruled in a similar case, exonerating a manufacturer by observing that the damage was caused exclusively by the person who had purchased the product and used it in total disregard of the indications contained in its labelling.

The liability of Service Providers has developed primarily through the common law of fault, but the needs of special provisions are pending. In particular, in French legal system, the civil offense is essentially atypical, 'open' and without an established reference to illegality[224]. In particular, it is based on three elements:

(i) *la faute*, that according to the majority doctrine, is represented by the non-observance of a duty of behavior knowable by the author of the damage and, in turn, divided into *faute délictuelle* and *faute quasi-délictuelle;*

(ii) *le dommage*, initially referring only to absolute subjective rights, but subsequently extended to the area of mere factual interests with the affirmation of the *intérêt légitime juridiquement protégé* (called *moral dommage*);

(iii) *le lien de causalité* between the conduct of the damaging party and the injury suffered by the victim: pursuant to Article 1151 of the Civil Code, the damaging party is only liable for the injury suffered by the victim which is *une suite immédiate et directe* of his conduct.

3.2 Liability in the event of defective product and rules implementing the Product liability directive

As is well known, Directive 85/374 /EEC, also known as the PLD, establishes a strict liability regime for defective products and seeks to eliminate obstacles to the unity of the common market resulting from the simultaneous existence of all the different national legislative regimes. Furthermore, a uniform regime aimed at eliminating distortions of competition resulting from differences in national laws.

In France, the Directive was transposed into national law, albeit approximately 10 years late, through Law No 98-389. Because of this delay, France was officially condemned and censured by the Court of Justice. In this regard, it should be noted that producer liability in French law had already been built up since the 1960s thanks to the intensive work by doctrine and case law that had highlighted the coexistence of two regimes:

- The contractual liability for damage resulting from the defect of goods; and
- The non-contractual liability for illicit acts committed against the victim.

The 1998 law introduced in France a regime of unlimited strict liability without a ceiling. Based on this law, some provisions on product liability have been included in the French Civil Code.

Article 1386-1 states that the producer is liable for damage caused by a defective product and under the umbrella of the development of risk clause, France decide to set a mechanism for which the provider shall be liable even if he proves that the state of scientific and technical knowledge at the time of putting the product into circulation was not such as to enable the existence of a defect to be discovered. Therefore, this is a hypothesis of a strict liability.

The distinction of contractual and quasi-contractual liability is abolished, the subsequent article sclassifying the new liability regime introduced by the Directive as covering damage caused by the product and not suffered by it. Moreover, according to Art. 1386-11, to prove the producer's liability, the victim must prove the damage, the defect of the product and the causal link between defect and damage, but not the producer's fault. According to the principle of risk-sharing between the victim and the producer, the latter is exempt from any liability if they can prove the facts. Finally, it must be stressed out that the producer must withdraw the good from the market if, after having put it on sale, they discover that it has a defect[225].

[224] P.H. LE TOURNEAU - L. CADIET, Droit de la responsabilité, Paris, 1998, pp. 1198 ss.

[225] An interesting case is provided by the case brought against French Volvo following an accident on 17 June 1999 due to a malfunction of the braking system. www.jurisques.com , cabinet d'avocats, Jean-François Carlot, "Responsabilité du fait des produits defectueux", 1/2/2002.

3.3 Civil Liability for unlawful treatment of personal data

In France, since 6 January 1978, there has been the "*Loi informatique et libertés*", which establishes the principle that anyone intending to process personal data (i.e. names) must first notify the *Commission Nationale Informatique et Libertés* ("CNIL"). In 2019, this law was revised in order to incorporate the provisions of the GDPR.

However, with reference to Article 82 of the GDPR, no specific provision has been introduced in France. As is well known, Article 82 of the GDPR confirms the principle of the right to compensation arising from Directive 95/46/EC, which has not been transposed into French law, thus not establishing the guiding principles governing compensation for damage suffered by any person as a result of a breach of the Regulation. Furthermore, it should be noted that in Recital 85 of the GDPR, there are examples of compensable damages, such as loss of control over personal data, financial loss, discrimination, theft, identity theft or damage to reputation, but there is no definition or criteria for defining the notion of damage and/or injury. Indeed, in French positive law, there is no legal definition of this notion.

On 7 October 2016 in France, the Parliament adopted the 'Law for a digital republic', which encroaches on the areas addressed by the GDPR, in particular by establishing public data default, net neutrality, a duty of loyalty for online platforms, as well as greater protection for the personal data of network users.

3.4 Liability in artificial intelligence

On 15 January 2020, proposed constitutional law no. 2585 on the "*Charte de l'intelligence artificielle et des algorithms*" was presented to the French Parliament. This represents the first initiative that aims to constitutionalise the legal implications of Artificial Intelligence. In particular, the bill formalises the constitutional basis of the general nucleus of principles applicable to Artificial Intelligence, as a regulatory intervention to adapt the current regulatory framework of technological evolution to guarantee the protection of the fundamental freedoms of individuals with the development of increasingly sophisticated algorithms capable of exercising massive forms of control over the generality of users.

After outlining the notion of Artificial Intelligence in order to identify any type of robot and evolutionary algorithm capable of making decisions, the document provides, in the event of damage caused to individuals, the attributability of obligations and liability directly to the natural or legal person who, as legal representative, creates and deploys AI systems, excluding that the latter has legal personality in the ownership of subjective legal situations.

The aforementioned draft constitutional law, which represents an unprecedented initiative in the national landscape of the Member States, seems to be in close connection with the "*European Ethical Charter on the use of artificial intelligence in the judiciary and their environment*", adopted in December 2018 within the Council of Europe by the European Commission for the Efficiency of Justice (CEPEJ), in order to ensure the compatibility of artificial intelligence tools with the protection of fundamental rights.

As in other EU Member States, the national debate in Italy, Spain, and France concerns not only the aforementioned Charter, but also the development process of the Regulation and in particular the White Paper on Artificial Intelligence[226].

[226] A European approach to excellence and trust and the resolution of the EP, of 20 October 2020, containing recommendations to the Commission on a civil liability regime for artificial intelligence, in order to propose the adoption of a regulation that covers any virtual or physical activity, device or process driven by a system of AI that has caused damage or harm to the life, health, physical integrity of a natural person, to the assets of a natural or legal person or has caused significant non-pecuniary damage resulting in a verifiable economic loss, as well as any contract between the operator of an AI system and a natural or legal person who is the victim of harm or prejudice due to an AI system that circumvents or limits rights and obligations enshrined in the regulation itself.

3.5 Conclusion/ practical applications

The French interest regarding the consequences of using technology in vehicles is shown by the aforementioned proposed Constitutional Law No 2585 on the *"Charte de l'intelligence artificielle et des algorithms"* of 15 January 2020.

The debate on liability has focused mainly on autonomous or semi-autonomous vehicles:

- In the case of *semi-autonomous vehicles*, it seems that current legislation should apply.
  Autonomous driving devices are much more similar to driver assistance devices, where the driver has to remain alert to the actions of the automaton and regain control in the event of an inappropriate response;
- Regarding autonomous and connected vehicle, the risk is independent of the users, whether they are present in the vehicle or not.

In this regard, according to the majority of sector specialists, the civil liability insurance of the manufacturer of the mechanics or the sensors, but also the civil liability of the software designer must be assessed according to the component that will be held responsible for the caused damage. The black box installation seems to be a satisfactory solution to ensure the evidence needed to understand the course of an accident or the behavior of the autonomous vehicle. For some companies, assuming full responsibility for an autonomous car accident poses no problem, even though the legislation has not yet been fully defined.

Some other countries such as the United States have circumvented legal obstacles by considering that an on-board computer can be similar to a driver, which would mean being able to use existing laws. France would like to define a legal personality for robots and thus for autonomous vehicles. This new legislation would allow users to define a person responsible who happens to be the manufacturer of the defective part of the vehicle, once the expert mission has designated the cause of the accident.

GERMANY

4.1 Liability structure and different hypothesis

Germany's model of non-contractual liability is governed by the Civil Code ("Bürgerliches Gesetzbuch" – "**BGB**"), which entered into force on 1 January 1900. Prior to the BGB, Germany, being a system of Romanesque tradition, had developed a whole series of non-contractual liability hypotheses, based on the *actiones in rem* of the Roman law.

Faced with this varied panorama, there was much discussion as to whether a general case (covering all types of non-contractual liability) should be included or whether specific cases should be envisaged. At the end of a long debate, the thesis of single hypotheses of torts prevailed, to the contrary of a general clause. A general clause, in fact, was considered to be dangerous of abuse of interpretation by the Courts.

Accordingly, the BGB does not formally provide for a general rule conferring a general obligation to pay damages on any person who unlawfully and negligently causes damage to others. In addition to the general elements of unlawfulness and culpability, the German legislature requires that there must have been an injury to one of the legal goods, expressly provided for by law. Alongside those provisions are set forth some strict liability provisions for specific cases, closely to the "liability aggravated by the event" regulated by the Italian Civil Code.

Thus, the main cases of tort set out in the BGB are contained in the § 832(I) and (II) and § 826 BGB and, specifically, are the following:

- The first case of non-contractual liability is set in Para. (1) of § 832 BGB that deals with cases where "*a person has unlawfully and negligently damaged certain legal assets of others*", such as, for example, life, person, health, liberty, property, or a "*different right to which others are entitled*". According to the German doctrine, this would constitute unlawful conduct and thus, *contra ius*, conduct of intrusion and violation of the aforementioned goods, in the absence of a cause justifying the intrusion (*i.e.* the conduct must be *contra ius* and *not iure*). It should be emphasised that even if German doctrine had tried not to take refuge behind an all-encompassing clause, elaborating different hypotheses of

unlawful acts, providing for a general clause of "every other right to which others are entitled", in fact, made the hypotheses of unlawfulness in the German legal system undefinable a priori. This general clause, contained in § 832, takes on particular importance in the light of this Study, since it makes it possible to include many different cases of 'injury' that were not foreseeable at the time the BGB was drafted[227].

- The second case of non-contractual liability in § 832(2) BGB "*protects the interest of a person that is worthy of protection at the level of the individual*". This is a category in which the so-called protective rules come together.
- The third case of non-contractual liability is set in § 826 BGB. According to this provision, a person who "*by acting in a manner inconsistent with good customs causes damage to others*" is liable to pay damages. The concept of "morality" is obviously an open concept: case law has therefore developed a series of typical cases that have as their common denominator the fact that the damage is caused by unfair behavior, *i.e.* behavior that conflicts with the sense of fairness commonly felt and accepted by society.

Thus, in light of the abovementioned principles, it can be said that non-contractual liability in Germany is based on a fault-based model and is articulated in specific provisions, potentially covering all emerging forms of liability. In addition, it should be noted at the outset that the limitation period in Germany for asserting one's rights is very long, up to 30 years after the event.

4.2 Liability in the event of defective product and rules implementing the Product liability directive

German product liability is therefore based on two main statutes: (i) the Civil Code, known as *Bürgerliches Gesetzbuch* or BGB, and (ii) the Product Liability Act ("*Produkthaftungsgesetz*"). Specifically, the Product Liability Act is based on the European Product Liability Directive of 1985 and provides for strict liability in case of liability arising products.

Until 1989, before the Product Liability Act, the basis of German product liability law was embodied in the general provision of Sec. 823(1) of the BGB, which essentially provides that anyone *"who, intentionally or negligently, unlawfully injures the life, body, health, freedom, property or another right of another person is liable*" in damages, as set forth specifically in the paragraph above.

After the transposition of the Product Liability Directive, product liability in Germany is regulated by the Product Liability Act (PLA). According to the PLA, this discipline finds application whenever "product" and "producer" are involved and the consumer claims damage caused by a "product's defect". These concepts are quite generally drafted and therefore need particular definition to ensure a clear application in the German legislation. Specifically, the Product Liability Act defines:

- "*Product*" as any movable object, even if it is part of another movable or immovable object, as well as electricity;
- "*Producer*" as manufacturer, manufacturer's suppliers, "*quasi-manufacturers*" and also importers into the EU. For clarity, a "*quasi-manufacturer*" is a company that attaches its name, trademark or other designation to a product, its packaging or instructions. Therefore, it should be emphasized, that the Product Liability Act treats a "*quasi-manufacturer*" as a producer. Similarly, it treats the importer of a product into the EU for the commercial purposes of selling, hiring, leasing or any form of distribution in the course of business is considered a producer.
- *"Product's defect"* as any defect that precludes the safety which a person is entitled to expect, taking all

[227] By way of example, it should be noted that the German courts have granted protection to new rights arising in the light of the general clause contained in § 832 BGB, such as the right to a name, image, possession, patents or other industrial property.

circumstances into account, including, the presentation of the product, the use to which it could reasonably be expected, and the time when the product was put into circulation.

The burden of proof for the injured person differs depending on the legal basis for the claim.

Under the Product Liability Act the onus is upon the injured party to prove that a product was defective and that it caused injury; whilst the manufacturer must prove any defense it puts forward. Unless the product has been modified after being put into circulation it is presumed that the defect resulted from the manufacturer's negligence and thus results in the manufacturer's liability for the defect.

In contrast, under the German Civil Code the injured party must demonstrate that there was a product defect, an injury, and a causal link between the two and, inter alia, the negligence of the manufacturer.

The reversed burden of proof, provided by the Product Liability Act, is intended to support the injured party in its claim, as it would otherwise be difficult for the injured party to prove the cause of the apparent defect. The manufacturer, however, can be expected to be able to prove, if true, that the defect cannot be attributed to its negligence.

Lastly, concerning damages, according to the German Civil Code's principle of restitution in kind ("*Naturalrestitution*"), an injured party may claim compensation for the material damages incurred and require restoring to the position it would have been in if the defect would have not occurred. Apart from physical damage to individuals or property, intangible damage, such as mental distress, can also be claimed under the Product Liability Act and the German Civil Code. Furthermore, according to the Product Liability Act, if more than one manufacturer is liable, then both will be jointly and severally liable.

Of paramount importance that must hereto be underlined is that the Product Liability Act, as transposed in the German law, imposes a cap of €85 million in damages for each single product, or several products, with the same defect, even if more than one individual is injured. This cap under the Product Liability Act does not apply to section 823 of the German Civil Code and therefore, consumers could decide to proceed with the normal discipline set in the Civil Code and not with the specific Product Liability Act whenever it's more convenient. Furthermore, it must be underlined that mere financial losses are non-recoverable under German law, nor can the claimant ask for punitive, exemplary, moral or other non-compensatory damages.

4.3 Civil Liability for unlawful treatment of personal data

In Germany, as in other EU countries, the Data Protection Regulation, commonly known as GDPR, is in force. Therefore, the violation of unlawful treatment of personal data, are regulated both by this specific provision and by the general discipline set forth in the national data protection laws.

Under Article 82 GDPR, data subjects may claim compensation for any material and/or immaterial damage suffered due to a data protection violation. Before the GDPR, became binding in May 2018, data subjects could not readily obtain substantial immaterial damage under German data protection laws. And, even after May 2018, German civil courts have been reluctant to grant significant compensation for immaterial damage under the GDPR. In particular, the courts have historically demanded proof of a specific and substantial immaterial damage before issuing an award.

Recently, the German courts have been increasingly following the US model of awarding damages in actions and this court-trend have had a substantial consequence for companies involved in the digital economy, including the risk of mass data litigation. In fact, according to the discipline today in force, consumer, after an unlawful treatment, are allowed to proceed both to the data protection authority, according to GDPR, and to the German Court.

In fact, under the GDPR, companies can face substantial fines of €20 million or up to 4% of the annual global turnover of the company's relevant group, whichever is higher. And, on the same time, data protection breaches also give rise to potential claims for damages. Since data protection breaches often affect a large number of data subjects, the financial risks can be considerable - particularly in the case of data breaches such as cybersecurity incidents.

Indeed, data subjects under the GDPR can directly claim damages if they believe their data protection rights have been violated, either compensation for immaterial damages under Article 82 GDPR or, in parallel, with the competent authority. In addition, it should be noted that on the basis of this complaint, data subjects may file a

request for access to the respective file in an attempt to strengthen their legal position in court. In such circumstances, companies may face terminations of business contracts and/or claims for contractual compensation payments in addition to damages claims under Article 82 GDPR.

In conclusion, German courts are increasingly deviating from the restrictive approach they have traditionally taken in relation to immaterial damages for data protection violations. In fact, recent decisions have showed an overruling on immaterial damages under Article 82 of GDPR. Nonetheless, the decisions demonstrate the willingness of German civil and labor courts to grant plaintiffs immaterial damages to compensate GDPR violations.[228]

4.4 Liability in artificial intelligence

Germany for the application of AI is known in the European landscape as synonymous with modern, secure and technology: it is an international brand. This is the result of the German Federal Government's Artificial Intelligence Strategy that was launched in November 2018. The German Government recognizes Artificial Intelligence as a key driver of productivity and as generator for economic growth. Although Germany is already extremely well positioned in many areas of AI, the Federal Government aims to transfer the existing strengths to areas where no or little use has been made of the potential of Artificial Intelligence.

Despite the German Federal Government's Artificial Intelligence Strategy, today, there is no specific law that regulates the AI, big data or machine learning. Instead, AI is regulated through a variety of applicable regulations, like for example, the German Copyright Act (amended in 2018), that now provides for provisions allowing text and data mining and the automated analysis of a large number of works for the purpose of scientific research or the abovementioned Art. 22 GDPR. Furthermore, in 2017, Germany passed a law allowing cars to drive highly or semi-automated vehicles. Although the car is driving partly autonomously, the law requires the driver to stay receptive while handing over control to the car. According to this law, the car still needs a driver, a person to closely monitor the car and can at any time retake control of the car. Therefore, under this law, the driver (and the owner) will be liable if the car crashes during the execution of its automated functions. This Act has already led to substantial discussions about how autonomous driving should be regulated in Germany: those in favour have argued that autonomous driving will make the roads safer and reduce the number of car crashes and persons injured or killed in traffic. Critics point out that it is irresponsible to allow drivers to use the automated functions because substantial questions relating to autonomous driving have not still been solved.

4.5 Conclusion/ practical applications

In light of what has been said above, it is clear that an easy and transparent legal framework doesn't exist right now, either in Germany nor in Europe.

In Germany, towards the end of 2018, the Minister for Traffic announced that legislation allowing fully autonomous driving (*i.e.* the car drives entirely without a driver) would be passed in 2019. This was mainly a result of pressure from the automotive industry that felt inhibited by the fact that legislation was lagging behind the advances in technology. So far, no such law has entered into force.

Consequently, it continues to be unclear who should be liable if the artificial intelligence causes harm to another person. At the moment, the majority of commentators suggest that the manufacturer should be liable. Recently, however, the big car manufacturers have curbed the enthusiasm regarding autonomous driving and announced

[228] Ex multis, Düsseldorf Labor Court, 5 March 2020, case no. 9 Ca 6557/18; Darmstadt Regional Court 26 May 2020, case no. 13 O 244/19, Neumünster Labor Court 11 August 2020, case no. 1 Ca 247 c/20; Cologne Regional Labor Court 14 September 2020, case no. 2 Sa 358/20; Cologne Labor Court, 12 March 2020, case no. 5 Ca 4806/19: € 300 immaterial damage granted.

that it might well take another 10 years before a self-driving car might be ready for the road. Presumably the main reason being that the technology is currently too expensive for large-scale production. Nevertheless, the topic remains far up on the agenda.

REFERENCES

LEGISLATION

EU Regulations

- Regulation (EC) No 715/ 2007 of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information. Available at: http://data.europa.eu/eli/reg/2007/715/oj
- Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (*Rome II*). Available at: http://data.europa.eu/eli/reg/2007/864/oj
- Regulation (EU) No 461/2010 of 27 May 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices in the motor vehicle sector. Available at: http://data.europa.eu/eli/reg/2010/461/oj
- Regulation (EU) no 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Available at: http://data.europa.eu/eli/reg/2012/1215/oj
- Regulation (EU) No 758/2015 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC. Available at: http://data.europa.eu/eli/reg/2015/758/oj
- Regulation (EU) No 679/2016 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). Available at: http://data.europa.eu/eli/reg/2016/679/oj
- Regulation (EU) No 858/2018 of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC. Available at: http://data.europa.eu/eli/reg/2018/858/oj
- Regulation (EU) No 881/2019 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available at: http://data.europa.eu/eli/reg/2019/881/oj
- Regulation (EU) No 2144/2019 of 27 November 2019 on type approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users. Available at: http://data.europa.eu/eli/reg/2019/2144/oj

EU Directives

- Council Directive 72/166/EEC of 24 April 1972 on the approximation of the laws of Member States relating to insurance against civil liability in respect of the use of motor vehicles, and to the enforcement of the obligation to insure against such liability. Available at: http://data.europa.eu/eli/dir/1972/166/oj
- 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. Available at: http://data.europa.eu/eli/dir/1985/374/oj
- Second Council Directive 84/5/EEC of 30 December 1983 on the approximation of the laws of the Member States relating to insurance against civil liability in respect of the use of motor vehicles. Available at: http://data.europa.eu/eli/dir/1984/5/oj
- Third Council Directive 90/232/EEC of 14 May 1990 on the approximation of the laws of the Member States relating to insurance against civil liability in respect of the use of motor vehicles. Available at: http://data.europa.eu/eli/dir/1990/232/oj
- Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. Available at: http://data.europa.eu/eli/dir/1993/13/oj
- Directive 95/46 / EC 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. Available at: http://data.europa.eu/eli/dir/1995/46/oj
- Directive 96/9/EC of 11 March 1996 on the legal protection of databases (Database Directive). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01996L0009-20190606&from=IT

- Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at: http://data.europa.eu/eli/dir/2000/31/oj
- Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. Available at: http://data.europa.eu/eli/dir/2001/29/oj
- Directive 2001/95/EC of 3 December 2001 on general product safety. Available at: http://data.europa.eu/eli/dir/2001/95/oj
- Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available at: http://data.europa.eu/eli/dir/2002/58/oj
- Directive 2002/19/EC of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive). Available at: http://data.europa.eu/eli/dir/2002/19/oj
- Directive 2002/20/EC of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive). Available at: http://data.europa.eu/eli/dir/2002/20/oj
- Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=RO
- Directive 2002/22/EC of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). Available at: http://data.europa.eu/eli/dir/2002/22/oj
- Directive 2002/65/EC of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC. Available from: http://data.europa.eu/eli/dir/2002/65/oj
- Directive 2006/42/EC of 17 May 2006 on machinery and amending Directive 95/16/EC (recast). Available at: http://data.europa.eu/eli/dir/2006/42/oj
- Directive 2006/123/EC of 12 December 2006 on services in the internal market. Available at: http://data.europa.eu/eli/dir/2006/123/oj
- Commission Directive 2008/63/CE of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version). Available at: http://data.europa.eu/eli/dir/2008/63/oj
- Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. Available at: http://data.europa.eu/eli/dir/2009/24/oj
- Directive 2009/103/EC of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability. Available at: http://data.europa.eu/eli/dir/2009/103/oj
- Directive 2010/40/EU of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Available at: http://data.europa.eu/eli/dir/2010/40/oj
- Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. Available at: http://data.europa.eu/eli/dir/2011/83/oj
- Directive 2011/24/EU of 9 March 2011 on the application of patients' rights in cross-border healthcare. Available at: http://data.europa.eu/eli/dir/2011/24/oj
- Directive 2013/55/EU of 20 November 2013 on the recognition of professional qualifications and Regulation (EU) No 1024/2012 on administrative cooperation through the Internal Market Information System (IMI Regulation). Available at: http://data.europa.eu/eli/dir/2013/55/oj
- Directive 2014/35/EU of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits. Available at: http://data.europa.eu/eli/dir/2014/35/oj
- Directive 2014/104 of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union. Available at: http://data.europa.eu/eli/dir/2014/104/oj
- Directive 2015/1535/EU of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. Available at: http://data.europa.eu/eli/dir/2015/1535/oj
- Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and

disclosure. Available at: http://data.europa.eu/eli/dir/2016/943/oj

- Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: http://data.europa.eu/eli/dir/2016/1148/oj
- Directive 2018/958 of 28 June 2018 on a proportionality test before adoption of new regulation of professions. Available at: http://data.europa.eu/eli/dir/2018/958/oj
- Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (Recast). Available at: http://data.europa.eu/eli/dir/2018/1972/oj
- Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. Available at: http://data.europa.eu/eli/dir/2014/104/oj
- Directive 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods. Available at: http://data.europa.eu/eli/dir/2019/771/oj

Communications, Proposals and Resolutions

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Single Market Strategy for Europe. COM/2015/192 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions on the road to automated mobility: An EU strategy for mobility of the future. COM/2018/283 final. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0283:FIN.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe. COM/2018/237 final. Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF.
- Commission Staff Working Document - Evaluation of 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. SWD (2018) 157 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0157&rid=2.
- Commission Staff Working Document - Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe - Commission Staff Working Document. SWD/2018/137 final. Available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137.
- European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103/INL). Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bTA%2bP8-TA-2017-0051%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.
- European Parliament Resolution of 12 February 2020 on Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP)). Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0032_EN.pdf.
- Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN/2017/450 final. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450.
- Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; JOIN/2013/01 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001.
- Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. COM/2015/0634 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015PC0634.
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final - 2017/03 (COD). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.
- Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (*Digital Services Act*) and amending Directive 2000/31/EC. COM/2020/825 final. Available at: https://eur-

lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN.

- Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=EN.

National legislation

- (FR) French Law No 98-389 of 1998
- (FR) French Decree No 211/2018 on experimentation with automated vehicles on public roads
- (FR) French Law Badinter No 85-677 of 1985
- (GE) German Road Traffic Act (*Straßenverkehrsgesetz*). Available at: https://www.gesetze-im-internet.de/englisch_stvg/index.html
- (GE) German Civil Code, BGB. Available at: https://www.gesetze-im-internet.de/englisch_bgb/
- (ES) Spanish Royal Legislative Decree No 1 of 16 November 2007
- (ES) Spanish civil Code - Código Civil of 1910
- (UK) UK Automated and Electric Vehicles Act of 2018. Available at: http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted).

CASE LAW

Court of Justice of the European Union

- ECJ, Judgement of 5 July 2007, C-327/05, *Commission v Denmark*, ECLI:EU:C:2007:409
- ECJ, Judgment of 24 April 2002, Case C-52/00, *Commission v France*, ECLI:EU:C:2002:252
- ECJ, Judgment of 29 May 1997, Case C-300/95, *Commission v UK*, ECLI:EU:C:1997:255
- ECJ, Judgment of 21 December 2011, Case C-495/10, *Dutrueux,* ECLI:EU:C:2011:869
- ECJ, Judgement of 5 March 2015, Joint Cases C-503/13 and C-504/13, *Boston Scientific Medizintechnik*, ECLI:EU:C:2015:148
- ECJ, Judgment of 16 January 2014, Case C-45/13, *Kainz,* ECLI:EU:C:2014:7
- ECJ, Judgment of 4 June 2009, Case C-285/08, *Moteurs Leroy Somer*, ECLI:EU:C:2009:351.
- ECJ, Judgement of 20 November 2014, Case C-310/13, *Novo Nordick Pharma,* ECLI:EU:C:2014:2385
- ECJ, Judgment of 9 February 2006, Case C-127/04, *O' Byrne*, ECLI:EU:C:2006:93
- ECJ, Judgment of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, ECLI:EU:C:2016:779
- ECJ, Judgment of 25 April 2002, Case C-183/00, *Gonzalez Sanchez*, ECLI:EU:C:2002:255
- ECJ, Judgment of 7 December 2017, *Snitem and Philips France*, ECLI:EU:C:2017:947
- ECJ, Judgment of 3 July 2012, *UsedSoft,* Case C-128/11, ECLI:EU:C:2012:407
- ECJ, Judgment of 10 May 2001, Case C-203/99, *Veedfald*, ECLI:EU:C:2001:258

National courts

- (BG) Case no. 20942 of 2012
- (IT) Tribunale di of Palermo, Case no. 6589 of 2015
- (IT) Corte di Appello, Case no. 13432 of 2010
- (UK) Jurisdiction of England and Wales, Case of 28 April 2008, *Ide v ATB Sales Ltd*, EWCA Civ 424
- (GE) Düsseldorf Labor Court, Case no. 9 Ca 6557/18 of 2020
- (GE) Darmstadt Regional Court, Case no. 13 O 244/19 of 2020
- (GE) Neumünster Labor Court, Case no. 1 Ca 247 c/20 of 2020
- (GE) Cologne Regional Labor Court, Case no. 2 Sa 358/20 of 2020
- (GE) Cologne Labor Court, Case no. 5 Ca 4806/19 of 2020
- (ES) Tribunal Supremo, Sala de lo Civil, JUR 2016, STS 1280
- (ES) SAP Almeria of 17.05. 2004, JUR 2004, 193357
- (ES) SAP Cordoba, 11.01.2007, JUR 2008, 140551
- (ES) SAP La Coruña of 29.07.2004, JUR 2005, 32723
- (ES) SAP Pontevedra of 08.05.2008, JUR 2008, 287766

- (ES) SAP Santa Cruz de Tenerife of 15.03.2006, JUR 2006, 153965

LITERATURE

- AA.VV. (1990) The damage from products, S. PATTI, Padua.
- ACEA (2016) Strategy Paper on Connectivity. Available at: https://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf.
- ACEA (2016) Position Paper on Access to vehicle data for third-party services. Available at: https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf.
- Alpa G., Bin R., Cendon P. (1989), The liability of the producer, Tratt. dir. comm. and dir. publ. ect., F. GALGANO, Padua.
- Balthasar C. (2014) Producer liability: compensable damage, burden of proof and legal logic - Danno e responsabilità
- Bassini M., Pollicino O., (2018) Artificial Intelligence Systems, liability and accountability. Towards new paradigms? in Artificial Intelligence, Personal Data Protection and Regulation, Pizzetti F., Milan.
- Battaglia F., Nida-Rümelin J., and Mukerji N. (2014) Rethinking Responsibility in Science and Technology, Pisa University Press.
- Bertolini A. (2014) Robots and liability - Justifying a change in perspective. Pisa University Press.
- Bertolini A., Palmerini E. (2016) Liability and Risk Management in Robotics. Nomos.
- BEUC (2020). Product Liability 2.0 - How to make EU rules fit for consumers in the digital age. Available at: https://www.beuc.eu/publications/product-liability-20-how-make-eu-rules-fit-consumers-digital-age/html
- Brown D. (2016) Responsibility for Vehicle Security and Driver Privacy in the Age of the Connected Car (IDC). Available at: https://www.veracode.com/sites/default/files/Resources/Whitepapers/idc-veracode-connected-car-research-whitepaper.pdf
- Byrne R. E. (1974) Strict Liability and the Scientifically Unknowable Risk, 57 Marquette L. Rev. 660. Available at: http://scholarship.law.marquette.edu/mulr/vol57/iss4/6.
- Chatzipanagiotis M. P. (2020) Product Liability Directive and Software Updates of Automated Vehicles, Department of Law University of Cyprus Nicosia. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3759910.
- Osborne Clarke LLP (2016) Legal study on Ownership and Access to Data. European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1.
- Osborne Clarke LLP (2017) What EU legislation say about car data. FIA Region I. Available at: fiaregion1.com/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf
- CNIL (2017) Connected Vehicles and Personal data. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf)
- Deloitte (2018) Study on emerging issues of data ownership, interoperability, (re-)usability and access to data and liability. European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en.
- Drexl J. (2017) Designing competitive markets for industrial data – between Propertisation and Access. Available at: https://www.jipitec.eu/issues/jipitec-8-4-2017/4636/JIPITEC_8_4_2017_257_Drexl.
- EP, Directorate General for Internal Policies (2016) Study on Cross-border traffic accidents in the EU - the potential impact of driverless cars. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU(2016)571362_EN.pdf.
- European Commission, C-ITS (2016) C-ITS Platform - Final report. Available at: https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf.
- European Commission (2019) Minutes of Meeting of the Expert Group on "Liability and New Technologies – Product Liability Formation. Available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=31014.
- European Court of Auditors (2019) Briefing paper: challenges to effective cybersecurity policy. Available at:https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.
- European Data Protection Board (2019) Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf
- European Data Protection Board (2019) Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Available at: https://edpb.europa.eu/our-work-tools/our-documents/styrelsens-yttrande-art-64/opinion-52019-interplay-

between-eprivacy_en

- European Data Protection Board (2019) Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en
- European Parliament (2018) EPRS Study on A common EU approach to liability rules and insurance for connected and autonomous vehicles, European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf;
- European Data Protection Board (2020) Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
- European Data Protection Board (2021) Guidelines on processing personal data in the context of connected vehicles and mobility related applications.
- European Parliament, EPRS (2018) A common EU approach to liability rules and insurance for connected and autonomous vehicles. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf.
- EY, Technopolis Group, and VVA (2018) Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products. European Commission. Available at: http://publications.europa.eu/resource/cellar/d4e3e1f5-526c-11e8-be1d-01aa75ed71a1.0001.01/DOC_1.
- Expert Group on Liability and New Technologies - New Technologies Formation (2019) Liability for Artificial Intelligence and other Emerging Digital Technologies. Available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.
- Fairgrieve D., and Goldberg R. (2020) Product Liability, 3rd ed., Oxford University Press, Oxford.
- Felwick M., Kenyon V., Martin E. (2019) The product liability in the EU, European Union, Global, Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=ab1e2137-df8d-42f2-8b5b-3849f32726b1.
- FIA Region I (2016) Policy Position on Car Connectivity. Available at: https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf
- FIA Region I and others (2021) Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach. Available at: https://www.fiaregion1.com/wp-content/uploads/2021/03/2021-02-S-OTP-Paper-vFin.pdf.
- FIGIEFA (2016) Memorandum presented as input during the preparation of the Commission Communication on Building a European data economy.
- Gallage-Alwis S. (2020) Updating The EU Product Liability Directive For The Digital Era, Signature, Available at: https://www.signaturelitigation.com/updating-the-eu-product-liability-directive-for-the-digital-era-sylvie-gallage-alwis.
- Gazquez Serrano L. (2002) La responsabilidad civil por productos defectuosos en el ámbito de la Unión Europea: Derecho Comunitario y de los Estados Miembros, in Asociación Española de Abogados Especializados en Responsabilidad Civil y Seguro, n. 32.
- German Federal and State Data Protection Authorities and the German Association of the Automotive Industry (VDA) (2016) Joint statement on Data protection aspects of using connected and non-connected vehicles. Available at: https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
- Gómez Ligüerre C., (2017) Concepto de daño moral, in El daño moral y su cuantificación.
- Jiménez de Parga y Cabrera M., (1996) La Ley reguladora de la responsabilidad civil por daños causados por productos defectuosos en el marco del moderno derecho de la responsabilidad de acuerdo con las normas comunitarias europeas y de derecho comparado, in Estudios jurídicos en homenaje al Profesor Aurelio Menéndez, vol. III, Civitas, Madrid.
- Kerber W. (2018) Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data. Available at: https://www.jipitec.eu/issues/jipitec-9-3-2018/4807.
- Kerber W., Gill D., (2019) Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation. Available at: https://www.jipitec.eu/issues/jipitec-10-2-2019/4917 .
- Knobloch and Gröhn Gbr (2018) FIGIEFA Study - OEM 3rd Party Telematics - General Analysis. Available at: https://www.figiefa.eu/wp-content/uploads/Knobloch-Gr%C3%B6hn-OEM-3rd-Party-Telematics-General-Analysis-Report.pdf.
- KPMG (2019) Autonomous Vehicles Readiness Index. Available at: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/kpmg-2019-autonomous-vehicles-readiness-index.PDF.
- Le Tourneau P.H., (1998) Cadiet L., Droit de la responsabilité, Paris.

- López Sánchez C. (2000) El menor, sus juguetes y la responsabilidad civil, in Perfiles de la responsabilidad en el nuevo milenio, J. A. MORENO MARTÍNEZ (coord.), Dykinson, Madrid.
- Mazzini G., (2019) A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law, in A. DE FRANCESCHI - R. SCHÜTZE (eds.), Digital Revolutions - New challenge for Law, Munich.
- McCarthy M., Seidl M., Mohan S., Hopkin J., Stevens A., and Ognissanto F. - TRL (2017) Access to In-vehicle Data and Resources. European Commission. Available at: https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf.
- Pasquau Liano M., (2006) El defecto de seguridad como criterio de imputación de responsabilidad al empresario de servicios, in Responsabilidad civil por daños casusados por servicios defectuosos. Daños a la salud y seguridad de las personas, Pamplona.
- Piraino F., (2017) Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, in Le nuove leggi civili commentate.
- Ponzanelli G., (2003) Responsabilità oggettiva del produttore e difetto di informazione, in Danno e resp; R. Frau, in Corr. giur., 1987, p. 99.
- Santos Briz J., (2001) La responsabilidad civil. Temas actuales, Montecorvo, Madrid.
- Schulze R., and Staudenmayer D. (2016) Digital Revolution: Challenges for Contract Law in Practice. Nomos.
- SMMT (2017) Connected and Autonomous Vehicles – Position Paper. Available at: www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf.
- Sotomayor Gippini L. M., (1994) La nueva Ley sobre responsabilidad civil por los daños causados por productos defectuosos.
- TNO (2014) Study on the operation of the system of access to vehicle repair and maintenance information – Final report. Available at: https://op.europa.eu/en/publication-detail/-/publication/c2c172a5-3f49-4644-b5bb-c508d7532e4a.
- TNO (2019) Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems - Final Study Report regarding CAD/CCAM and Industrial Robots ("2019 TNO Study"). Available at: http://publications.europa.eu/resource/cellar/aad6a287-5523-11e9-a8ed-01aa75ed71a1.0001.01/DOC_1.
- TUVIT – Bartsch M., Bobel A., Dr. Niehöfer B., Wagner M., Wahner M. (2020) On-Board Telematics Platform Security. FIA Region I. Available at: https://www.fiaregion1.com/wp-content/uploads/2020/06/20200615_FIA_vehicle_security_report.pdf.