Gefördert durch:

Bundesministerium
für Verkehr und
digitale Infrastruktur

aufgrund eines Beschlusses
des Deutschen Bundestages

Technische
Universität
Berlin

Legal Framework for Automated Driving

SUMMARY

of the study “Legal Framework for Automated and Connected Transportation Systems”

Chair of Economic, Corporate, and Technology Law,
Technische Universität Berlin

Berlin, January 2019

This is a condensed version of the study “Legal Framework for Automated and Connected Transportation Systems” (AVF_RERA) with summaries from the study’s four subsections:

1. Standard-essential patents and vehicle networking

2. Permissibility and legal approval

3. Liability law

4. Data protection, data security, and data ownership

The long version of the study will be published in the spring of 2019 in the Deutscher Fachverlag’s (dfv) InTeR series.

About the Study

Acronym:	AVR_RERA
Title:	Rechtliche Rahmenbedingungen für automatisierte und vernetzte Verkehrssysteme (Legal Framework for Automated and Connected Transportation Systems)
Duration:	12 months
Grant recipient:	Technische Universität Berlin
Executing department:	Chair of Economic, Corporate, and Technology Law
	Prof. Dr. Dr. Jürgen Ensthaler
Principal investigator:	**Markus Gollrad, Ass. iur.**

Gefördert durch:

aufgrund eines Beschlusses des Deutschen Bundestages

1. STANDARD-ESSENTIAL PATENTS AND VEHICLE NETWORKING

Legal questions related to standard-essential patents (SEPs) arise because vehicle manufacturers need to use telecommunication standards in their vehicles. These technologies become especially important when automated driving functions rely on networking with infrastructure or other vehicles. When using the technologies in vehicles, the manufacturers then need licenses to use the patents on which these standards are based.

Problems include the confusing jungle of patents, a constant risk of patent infringement due to this confusion, the fact that in many cases the patents are actually invalid or are not essential to standards, unreasonable licensing fees, or the risk of injunctions with far-reaching consequences. There are also uncertainties related to the significance of the term Fair, Reasonable, and Non-Discriminatory (FRAND) and FRAND declarations. Many courts around the world and the European Commission have already dealt with these issues.

1. The European Court of Justice's (ECJ) 2015 decision on Huawei/ZTE was of key importance, as it averted the threat of serious effects posed by imminent injunctions in that the Court provided more details on the antitrust objection of compulsory licensing.

Since then, the patent proprietor must give notification of the SEPs necessary for using standards, name these SEPs, and provide a reasonable licensing offer while the user of the patent has an obligation to react. As long as no notification is given or the license negotiations are ongoing, the user of the patent may continue to use the SEP subject to retroactive license fees.

2. Based on existing case law, in particular the ECJ's, the importance of the term "FRAND" must be qualified. According to this study's findings, FRAND is not an indeterminate legal term that could be abstractly defined and interpreted. Instead, the requirements described with the term "FRAND" are already set down in relevant legal provisions in antitrust law, patent law, or general civil law. This includes, for example, the antitrust regulations in Art. 102 TFEU, which prohibit the abuse of a dominant market position. The question of what FRAND is rests not on an abstract definition of the term but on the application of the legal provisions in each individual case.

However, the term "FRAND" is important when it comes to international legal practice because its international recognition means that it is suited for use in legal harmonization.

3. In relation to the party seeking a license, the FRAND declaration on its own has only a limited legal meaning. Because the term "FRAND" cannot be set down abstractly according to what was stated above but must be derived from the legal provisions on a case-by-case basis, the FRAND declaration also does not include sufficient, specific legal obligations for those making the declaration that could constitute a contractual license claim for undetermined third

parties. Even if one assumes that the declaration confers rights to third parties, the declaration must still adhere to patent and antitrust legal principles; in each individual case, its content is determined by these principles.

But in the relationship between the patent holder and the standard organization, the FRAND declaration is important because the standard organizations may not set any norms for the respective invention outside of these declarations.

4. The requirements for a patent being considered essential to a standard must also be clarified. If the patent holder declares to the Standard Setting Organisation (SSO) that the patent is standard-essential, then the patent is considered essential. However, it is still necessary to interpret the term under consideration of antitrust law. What is decisive in determining whether a patent is essential for a standard is whether the patent is actually unavoidable for the standard user, so that it can be assumed that the patent holder has a dominant market position. In this context, there are different types of cases. There are areas in which the patent is obligatory for the standard, that is, there is no other technology that is just as applicable. Essentiality can arise in many other cases, however. In particular, a patent is essential if a newly developed, alternative technology cannot be used due to lengthy, ongoing regulatory approval processes.

This understanding of essentiality also affects the importance of the FRAND declaration. If a patent is actually essential for a standard in one of the ways described above, then antitrust principles prohibiting the abuse of a dominant position can be applied, leading to a compulsory licensing claim under reasonable conditions. If the patent is not standard-essential according to this description, then the FRAND declaration would also not be relevant.

5. When licensing SEPs, in the practice it is increasingly the case that comprehensive portfolios are being offered by patent utilizers. These blanket licenses are generally welcomed by the licensees in the automotive industry because it is not easily possible to identify the exact patents needed in each specific case, and license gaps are to be avoided. The price of the portfolio license is calculated as a lump sum per vehicle according to the expected added value and the intensity with which the standard will be used in the vehicle. This practice seems to be advantageous for everyone involved.

There are disputes between the license providers and vehicle manufacturers, however, about whether the vehicle manufacturer can be the sole licensee for the entire value chain. Instead, the vehicle manufacturers also want to refer the licensers to their respective suppliers, that is, the suppliers who produce the parts for using the standard (chipsets, modems, telecommunications modules) and who are familiar with the corresponding technologies.

In these cases, the exhaustion doctrine must be observed as it applies to product patents. A significant portion of the standard-essential product patents are used as intended by patent

law in earlier stages of the supply chain by the vehicle manufacturer's suppliers, and exhaustion could therefore be asserted. Exhaustion means that the patent owner can no longer influence the use of these products. The vehicle manufacturers could then freely use the respective components and thus also the standard.

From this, it follows that there must be differentiated licensing processes for standard-essential process and product patents. The licensor must usually license the product patents to the respective suppliers. That is not the case with process patents; for these, the vehicle manufacturer must typically also be a licensee.

However, currently licensors primarily restrict themselves to the vehicle manufacturers as contractual partners, apparently for economic reasons. This practice, in which the suppliers are not considered in the licensing process, likely violates patent and antitrust law and is therefore also not FRAND.

6. According to the ECJ's principles, the patent owner's injunctive rights are only enforceable if the patent user is not willing to carry out any serious negotiations about the licensing fee. The ECJ's guidelines are therefore intended to balance interests. Any additional proportionality assessments for enforcing the injunctive rights are then superfluous.

7. One problematic situation that can arise is that the patent user will try to defend himself with a nullity action to the German Federal Patent Court against the infringement claims. However, it is not possible to stay the infringement proceedings until the nullity action has been decided as long as the nullity is not clearly evident. SEPs, especially software-related SEPs, are statistically speaking often null, but their nullity usually does not result from obvious circumstances. As long as it is not clearly evident that the patent is null, the judge on the infringement case must assume that the patent is valid.

8. In contrast, the calculation of FRAND licensing fees can only be abstractly defined within narrow limits. From a legal perspective, the call will be focused on determining the price in a way that is understandable and based on concrete, actual criteria. Otherwise, establishing a reasonable price is left to the parties or the market.

2. PERMISSIBILITY AND LEGAL APPROVAL

The focus of this section is on whether and under which conditions automated driving functions are permissible on public roads and which technical requirements apply for approving (homologating) automated driving functions.

1. The automated driving levels 0-5 determine the areas of responsibility and tasks assigned to the driving functions and the driver. They are of technical import because they form the basis for determining the technical requirements for the driving functions. On the other hand, they are also important in a legal context. This is the case because the driver's rights and obligations vary depending on the level.

The German Road Transport Act (*Straßenverkehrsgesetz*, StVG) intentionally does not differentiate according to automated driving levels. This is problematic because it means the provisions in Secs. 1a(2) and 1b StVG are inconsistent. Both for the StVG and for legal disputes in general, it makes sense to refer to internationally established definitions of automated driving levels as a standard.

2. The question of permissibility is regulated internationally for road traffic law by the Vienna Convention on Road Traffic from 1968, revised in 2014, and the 1949 Geneva Convention on Road Traffic. According to the Vienna Convention, automated driving functions are considered permissible if they correspond to the technical requirements of the Geneva Convention from 1958 (UN/ECE regulations) or can be overridden and deactivated.

This means that the levels 3 and 4 are permissible according to the 1968 Vienna Convention and the 1949 Geneva Convention if a driver is present in or around the vehicle and can deactivate the driving functions at any time. Even after the UN/ECE group WP.1's resolution on October 3, 2018, the parties to the conventions have differing views on the permissibility of levels 4 and 5.

Coordinated and institutionalized cooperation of the UN/ECE groups WP.1 (for the 1968 Vienna Convention and the 1949 Geneva Convention) and WP.29 (for the 1958 Geneva Convention) is of key importance for the further development of automated driving. When it comes to technical aspects (UN/ECE regulations), the laws that have previously been tailored to the behavior of human drivers must be translated into technical requirements. For this, a consistent legal framework with clear legal terms must be created.

3. At the national level, permissibility is regulated in the new Sec. 1a StVG, which implements the requirements in the revised 1968 Vienna Convention. These regulations positively determine that automated driving is compatible with other road transport law, especially the German Road Traffic Act (*Straßenverkehrsordnung*, StVO). Ensuring this compatibility in detail is shifted to the level of technical requirements, Sec. 1a(2) no. 2 StVG.

4. The area of applicability for Sec. 1a(1) StVG only relates to driving functions for the levels 3 and 4 if a human driver is present in or directly near the vehicle. Higher levels are generally not permissible.

Permissibility is also restricted by Sec. 1a(3) StVG, which states that Sec. 1a StVG only includes those driving functions that are approved according to the technical requirements listed there (UN/ECE regulations or deviating requirements according to Art. 20 Directive 2007/46/EC).

Driving functions that are approved according to other technical requirements (e.g. Sec. 70 German Road Traffic Licensing Act (Straßenverkehrszulassungsordnung, StVZO)) are therefore generally not included in Sec. 1a StVG, meaning that their use must be impermissible. The use of this kind of automated driving function does not become permissible even if the driver fulfills his due diligence obligation and uses the function like an assistance system. Sec. 1a StVG must finally settle the question of the use of automated driving functions. The autonomy level should be determined during the approval process and made binding.

Test vehicles with accompanying or test drivers generally do not fall under the purview of Sec. 1a StVG, however. They are to be treated and licensed as vehicles of the level 2.

5. Using the driving functions as they were intended, as stated in Sec. 1a(1) StVG, is the central criterion for permissibility.

The term “intended use” according to Sec. 1a(1) StVG is controversial. Criticism has arisen that it enables the manufacturers to independently determine the conditions of permissibility and thus also the limits of their liability when using automated driving functions.

The intended use, however, is largely determined by the technical requirements of the driving function as stated in Sec. 1a(3) StVG, upon which the approval procedure is based. It is therefore still the law-makers’ task to determine which requirements must be fulfilled so that the intended use is also a legally permissible use. The manufacturer is bound to these requirements and thus does not have any leeway for individually determining the intended use.

The intended use of a driving function is made up of a binding assignment to an automated driving level, the necessary conditions of the Operational Design Domain (ODD), the necessary conditions in the vehicle, the interaction with the vehicle during use, and individual manufacturers’ information on the use and maintenance of the driving function.

Using the driving function for a purpose other than the intended use is generally impermissible. A separate finable offense should therefore be considered. Otherwise, each driver can test out the limits of the system on his own outside of the intended use.

Technical measures are to prevent functions from being used for something other than their intended use. Only when these measures have been exhausted can instructions be used, e.g. system notifications (Sec. 1a(2) no. 6 StVG).

6. The technical requirements referred to in Sec. 1a(3) StVG are decisive firstly for the content of the intended use and secondly as a basis for the approval process.

The technical requirements are developed in close cooperation with the manufacturers. They define the possibilities and limitations of the driving functions. The legislators (German Federal Motor Transport Authority or WP.29) or the technical agencies are then responsible for determining whether and under which conditions the function may be used.

The technical requirements must adhere to the guidelines in Sec. 1a(2) StVG or the corresponding guidelines of WP.1. In particular, the requirements must ensure that the driving function follows traffic laws, although it only needs to have mastered those that are relevant for its intended use – not all traffic laws. Intentionally ambiguous legal terms in behavior laws are problematic in this context, and the legislators and agencies must therefore be sure to follow the doctrine of legal certainty. In general, the goal is to minimize risk while at the same time assisting the flow of traffic.

If constructive measures have been exhausted, the technical requirements can also include guidelines for the manufacturers' operating instructions, Art. 37 Directive 2007/46/EC.

A list of permitted or prohibited secondary activities is not to be given. Instead, depending on the level, the driver must be given transparent and binding information about the signs and circumstances of which he must remain aware. The driver then decides himself which other activities are possible, as has previously also been the case.

7. A core element of the intended use is the Operation Design Domain (ODD), that is, the requirements for using the driving function that are related to factors outside of the vehicle.

It does not make sense for each manufacturer to individually determine the ODD, however, as otherwise there will be significant legal uncertainty for the users. The result would be a fragmentation of the requirements for use that would also make approval processes more difficult.

The ODDs are therefore to be defined abstractly for all manufacturers for certain types of driving functions. This must be included in the technical requirements.

When setting the driving functions' ODD, the state of technology must be reconciled with the StVO's provisions. Problems with the driving functions can be compensated for by stricter requirements for the environmental conditions under which they may be used.

With standardized ODDs, licensing processes for driving functions (such as Art. 20 Directive 2007/46/EC) could be made considerably easier. In addition, it would be possible for cities to

adapt their infrastructure to these conditions in certain areas in order to promote the introduction of the driving functions on the market.

3. LIABILITY LAW

This section discusses the consequences for legal liability arising from the use of automated driving functions.

1. Sections 1a and 1b StVG integrated the use of automated driving functions into the StVG's existing and proven liability system. This means that the vehicle owner still has strict liability while the driver has fault-based liability with mandatory insurance coverage. Claims against the manufacturer remain unchanged. There is therefore no basis for concepts of a new liability for the manufacturer or even the vehicle itself.

2. There are no special issues that arise based on owner liability according to Sec. 7 StVG. The general operational risk of vehicles with automated driving functions is not higher or lower than with traditional vehicles.

3. According to Sec. 18 StVG, the driver is liable even if the vehicle was steered with an automated driving function, Sec. 1a(4) StVG. However, the due diligence standard is modified in this case by Sec. 1b StVG.

The requirement for the modified due diligence obligation in Sec. 1b StVG is the intended use of the driving function at the time the damaging event occurs. To prove whether the system was active, Sec. 63a StVG applies.

If the system was used in a manner for which it was not intended, then the driver's typical due diligence obligation applies. To exonerate the driver, it must be shown that the damaging event would have occurred even if the driver had been driving without the automated functions and had been following traffic laws. For more on the content and determination of the intended use and the impermissibility of using the functions for something other than their intended use, see Section 2 on Permissibility and Legal Approval.

The criterion of "obvious circumstances" according to Sec. 1b(2) no. 2 StVG relating to function-specific requirements of previously unknown technologies must be criticized because as yet, the average user does not have a general understanding of the technologies' limits.

Obvious circumstances must therefore be limited to rare individual cases that could also be common for drivers of traditional vehicles. This could include tangible abnormalities in driving behavior as well as errors or damage that negatively affect the drivability of the vehicle as a whole. The disappearance of function-specific requirements cannot be included in this; the driver must be able to rely on notifications from the system.

4. Sec. 1b StVG states that the driver has the right to avert his attention but also the obligation to remain aware, which opens up new possibilities for drivers' activities while driving. As before, it remains the drivers' responsibility to judge which activities can be done while still fulfilling their obligations. However, it must be ensured that the signs and circumstances of which the

driver must remain aware when using the driving functions are made transparent and binding for the driver.

5. There are no special issues that arise based on Sec. 17 StVG. An increase or reduction of the vehicles' operational risk in relation to other parties involved in the damaging event follow the standard principles.

6. The manufacturer continues to be liable according to product and manufacturer liability.

In the context of product liability, liability can be excluded based on Sec. 1(2) no. 4 of the German Product Liability Act (*Produkthaftungsgesetz*, ProdHaftG) because the technical requirements are considered binding legal regulations according to Sec. 1a(3) StVG.

The specialized construction, production, instruction, and production monitoring obligations apply to manufacturer liability. In this, the technical requirements according to Sec. 1a(3) StVG in conjunction with Sec. 1a(2) StVG are considered the minimum standard. They can also include requirements for instructions.

As part of the proper construction obligation, it must be ensured that all measures are taken to exclude unintended use.

The instruction obligation is especially important if the intended use cannot be ensured using technical measures. The obligation also includes providing information about uses of the driving functions that are unintended but suggest themselves from the nature of the function. For this, the driver must be given transparent and clear information about the indications for which and circumstances in which the function should not be activated or should be deactivated.

The product monitoring obligation includes continual optimization of the algorithms to monitor traffic and vehicle controlling (as with Object and Event Detection and Response (OEDR)). For this purpose, the manufacturer must be able to evaluate and process camera and sensor data even retroactively when necessary; the product monitoring obligation can therefore represent a justification for encroaching on the rights of third parties.

7. In the case of traffic violations despite using the driving function as intended, the driver can typically not be considered at fault due to negligence according to Sec. 24 StVG. However, it might be possible for the driver to be considered responsible for ongoing or repeated violations.

8. If the driving function is dependent on networking with digital infrastructure, e.g. roadside units, then the road construction authorities could also be liable for damage that can be traced back to breakdowns and malfunctions of these systems.

4. DATA PROTECTION, DATA SECURITY, AND DATA OWNERSHIP

In this section, the legal data protection and data security aspects of automated and connected driving will be examined. The extent to which the question of legal attribution of data also arises with automated and connected driving will also be reviewed.

I. To determine whether data processing by automated vehicles conforms to data protection laws, several aspects unique to automated vehicles must be considered.

1. In individual cases, a differentiation between characteristics data and identifying data is suggested. Characteristics data could be divided into behavior-related and condition-related data. If the data gathered by the vehicle is linked to the vehicle's license plate or the vehicle identification number (VIN), then one can typically assume this is personal data.

2. The requirements for anonymization according to recital 26 of the EU GDPR are to be understood such that additional knowledge and other technical methods for direct or indirect identification used when assessing whether data references individuals are only to be considered to the extent to which they are "reasonably likely to be used". To determine whether the means are reasonably likely to be used, objective criteria such as costs and time required for identification and available technologies at the time of processing are to be considered.

3. To legally process personal data, the affected person's consent (Art. 6(1) letter a EU GDPR) or another form of legal permission (Art. 6(1) letters b to f EU GDPR) must be obtained.

4. Various actors can be considered to be the controller according to data protection laws. If personal data is processed, then for each processing step, the legal responsibility for data protection must be separately determined.

Certain particularities apply to the manufacturers in this regard. The manufacturer is considered the controller even during the manufacturing process as described by Art. 4 no. 7 EU GDPR. A lack of data processing at this point does not contradict the objective applicability of the EU GDPR.

5. Controllers are subject to the legal data security obligations arising from Art. 24, 25, and 32 EU GDPR. Especially the obligations in Art. 25 EU GDPR, that is, *privacy by design* and *privacy by default* must be upheld at the start of the vehicle manufacturing process. What "appropriate technical and organisational measures" include must be judged based on the state of the art. The judgment must also consider risks of varying likelihood as well as the severity of risks for personal rights and freedoms of natural persons.

6. The data storage device prescribed by Sec. 63a StVG combined with the legally required retention periods in Sec. 63a(4) StVG is problematic if the system does not recognize an accident as such and relevant data is then deleted from the data storage device after six months instead of three years. Once the damaging event is made known, the retention period

should be extended to three years regardless of whether the system recognized the event as an accident or not.

II. Vehicle networking (Car2X communication) creates many other issues related to data protection and data security. Car2X communication is divided into Car2Backend, Car2Infrastructure, and Car2Car communication.

1. Car2Backend communication transmits vehicle data to backend systems. Because the data is regularly linked to individual persons based on the VIN, a justification for transferring the data to the backend system is required according to Art. 6 EU GDPR. If pseudonymization in the backend system is not technically possible, then any additional processing also requires justification. For Car2Backend communication, the manufacturer must adhere to legal data protection obligations in Art. 24, 25, and 32 EU GDPR in order to prevent loss and manipulation of data, among other reasons.

If the manufacturer only processes the data to debug the system as part of their product monitoring obligations, then the data processing could be justified using Art. 6(1) e) or f) EU GDPR, as fulfilling the product monitoring obligations is in the legitimate interest of the manufacturer and public road safety outweighs the privacy interests of those affected.

2. For Car2Infrastructure communication, data is received and transmitted by central points such as infrastructure providers. Because the transmitted data is regularly linked to individual persons, the involved actors are responsible as described in Art. 4 no. 7 EU GDPR. Besides the EU GDPR's legal data security obligations, the requirements set by the German Telecommunications Act (*Telekommunikationsgesetz*) and the German Telemedia Act (*Telemediengesetz*) must also be observed.

3. To enable Car2X communication, the European Telecommunications Standards Institute (ETSI) determined that two standard messaging protocols would be used: Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM). For transmitting data, a Public Key Infrastructure (PKI) with a Certification Authority (CA) is foreseen to ensure the authenticity and integrity of the messages and that the vehicles are connected securely.

4. The NIS Directive was implemented by and large by the German IT Security Act. The obligations arising from the German Act on the Federal Office for Information Technology (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, BSIG) are only relevant if the actors are to be categorized as operators of critical infrastructure. Connected vehicles and other elements of intelligent traffic systems are currently not treated as critical infrastructure under Sec. 2 BSIG in conjunction with the Ordinance on Determining Critical Infrastructure (*Verordnung zur Bestimmung Kritischer Infrastruktur, KRITIS-Verordnung*). One could, however, imagine that this infrastructure might also be categorized as critical infrastructure in the future. The information technology and telecommunications that play a

significant role in networking are already considered critical infrastructure and therefore fall under the purview of the BSIG.

III. The importance of data ownership in automated driving and the legal basis for this ownership are controversial.

1. Even the relationship between data protection and data ownership is problematic, although the relationship can be resolved by giving data protection priority. More specifically, this means that the person whose personal rights are protected by the EU GDPR can object to the entity who may have ownership, that is, the exclusive authorization to use the data.

2. The question of data ownership becomes key to automated and connected driving when there is no reference to an individual person or the reference no longer exists after anonymization. How the data is to be attributed in these cases is in dispute. Besides a purely contractual solution, there are those who would use the assessment based on Sec. 950 of the German Civil Code (*Bürgerliches Gesetzbuch*, BGB) for the attribution and assign data ownership to the manufacturer due to their contribution to transmitting the data. This is not to be done without some sort of compensation, however. There are others, though, who believe that data obtained by the use of a machine are products of the machine and belong to the machine's owner. Another recommendation is to introduce a new, ancillary intellectual property right.

IV. Regardless of how the data is attributed as part of data ownership or data protection, the question arises who should have access to the data generated by the vehicle. The German Automotive Industry Association (VDA) created the NEVADA concept proposing neutral servers that act independently of the automotive industry for the benefit of fair competition. However, this concept envisages the manufacturers retaining exclusive access to the vehicle for security reasons and serving as a transmission channel to the neutral server. This would mean that the manufacturers would always have a key role in the data economy, although this does not appear to be mandatory. One possible option is whether the driver should be given a free choice about which provider will transmit the data to the neutral server.