IOP Conf. Series: Materials Science and Engineering **448** (2018) 012030 doi:10.1088/1757-899X/448/1/012030

# Law and Economic Analysis of the Legal Environment Related to the Autonomous Vehicles – Is There a Legal Paradigm Shift?

**K Pétervári**1,3 **and K Pázmándi** 2,4

1 Lecturer of Business Law – Neumann János University, Faculty of Economics, & ELTE University, Institute of Business Economics, 6000 Kecskemét, Izsáki út 10.
2 Lecturer of Business Law – Neumann János University, Faculty of Economics, & ELTE University, Institute of Business Economics, 6000 Kecskemét, Izsáki út 10.
3 E-mail: petervari.kinga@gmail.com
4 E-mail: pazmandi.kinga@gtk.uni-neumann.hu

**Abstract**. Autonomous vehicles trigger lots of legal problems. Whether this challenge, however, adds up to a paradigm shift in legal thinking is to be analysed further. As robotics develop globally, the legal institutions need to keep pace with it, because business risk, such as liability, has to be reasonably calculable for investors. Due to the expansive applicability of robotics, the relevant legal questions are manifold. The law faces applicatory as well as regulatory challenges. What is the standard for an autonomous vehicle? What should be the safety standards in driverless cars? How many bugs are to be acceptable in a software in case of a car crash? Who should be liable for an autonomous vehicle when it follows the rule and when it does not? How to tame the regulation by design to be more like a rule of law? This paper focuses on pragmatic problems and solutions and new regulatory models, like regulation by communication. It also introduces the concept of stealthy technologies, the meaning of which is that no matter what the rule is innovative technologies are going to be overwhelmingly widespread.

## 1. Introduction

Since there is no consensual opinion on what the paradigm as such means in social sciences, including legal sciences, this paper does not serve with a direct answer to the question whether or not there is a paradigm shift in legal thinking. Yet, one thing is certain. There are many changes in our contemporary, specific world which could generate the feeling of radical difference. But do they touch upon basic legal principles too? The real debatable question is then whether profound changes or whether *many* profound changes, would cause paradigm shift. The exact answers will undoubtedly be delivered by the numerous decisions of the legislation and the law enforcement in the near future.

Having said that, however, in this paper it is going to be shown that the law, as it is today, operates with analogies and fictions. And as long as there are analogies and precedents or fictions available, one is not crossing the border of normal sciences, the territory of one paradigm. Obviously, there are, and has never been homologous cases, legislators and/or judges always apply the interpretations of the previous cases.

The paper here, therefore, relies on the use of analogies too. It analyses the various legal tools applicable to the relevant cases, such as the legal personality, the vicarious liability and the culpability as opposed to strict – objective – liability. Again, one thing is certain. All of these legal techniques were familiar in the course of the legal history, none of these are new, but perhaps their applicability of scale is different. Since law is a social construction, the conceptions of the various legal tools may change. But even the most radical recommendation of awarding a computer a legal personality, or constitutional fundamental

rights, can found its roots in the past, like legal personality to organs created by the law, such as the companies, or the standing for the trees, which provides now legal protection to the environment.

On the other hand, one might object, that the new suggested *models* of regulation could cause a paradigm shift in legal thinking. These are the *regulation by design* or the *regulation by communications*. Regulation designers, like system designers, software engineers, and so on, need to find out the language what computers speak, and be able to speak the same language, also with the law-makers and courts and the law enforcement people.

Yet, this paper would introduce a new conception: the *stealthy automatics* or *stealthy technology*. With this term this paper argues, that whatever the regulation may be the autonomous cars are going to ameliorate and widespread.

## 2. The regulatory challenge

### *2.1. Analogies in regulating: EU v. USA*

Unlike the other rivalling companies back in 2016, Uber, this innovative but fairly eccentric company, refused to apply for a permit in San Francisco when launched a test driving of its autonomous vehicles (Wired (2016/12). Although the *new* rules of California would have so required, and the authorities so enforced indeed, Uber deliberately chose to remain under the scope of the old regulations. Truly, the cars on the streets are driverless, but there is always an engineer behind the wheels, ready to intervene and so autonomous vehicles qualify as vehicles driven in a "conventional mode", Uber argued.

Unlike California, however, Pittsburgh, Pennsylvania, where Uber had its basic testing sites, did *not* have new rules on autonomous vehicles operating in the city. Since then Uber has launched there its taxi services with a driverless car fleet. Lyft followed suit quickly (Wired 2016/12).

The rivalry among manufacturing companies of autonomous vehicles is recently so tense, that one must but wonder, whether the rules matter at all.

These cases do not mean that there are no regulations whatsoever, though.

Interestingly enough, one of the first statements of the US federal authorities asserted the continuity of the existing structure of the legal institutions, namely that "the division of regulatory responsibility for motor vehicle operation between Federal and State authorities is clear… should *remain* largely unchanged for highly autonomous vehicles" (NHTSA Policy Guidance, 2016).

The Europeans in the EU have somewhat analogous experiences but with a philosophically different attitude. Whereas it is a federal competence in the USA to decide who can access the public roads, this decision belongs rather to the competence of the Member States in the EU, so far, at least. And the Member States do use their power to regulate, and they regulate fairly disparately, of course. The Hungarian version of modification, for example, deals merely with the testing of the highly automated vehicles (11/2017. (IV. 12.) NFM order), whereas the German one applies to the traffic itself, even if under strict scrutiny (Achtes Gesetz zur Anderung des Strassenverkehrsgesetzes, vom 16. Juni, 2017). In any event, due to its determinant effect on the internal market, the EU will have to act at Union level.

The EU has, however, a rather ambiguous approach to the matter. It has *shared competence* in transportation policy (Article 4.2.(g) TFEU), but transportation in its stricter sense. It means that as far as it is indispensable for the common trade policy or competition within the internal market, this area is covered by the competence of the EU. So the EU legislators are abide by the otherwise classical notion

of subsidiarity principle and proportionality principle. Under the principle of subsidiarity, "in areas which do not fall within its *exclusive competence*, the Union shall act only if and insofar as the objectives of the proposed action cannot be sufficiently achieved by the Member States,… but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level" (Article 5.3 TFEU). Further, the proportionality principle compels that the EU "shall not exceed what is necessary to achieve the objectives of the Treaties" (Article 5.4 TFEU).

On the other hand road safety does not only extend to the commercial attributes of transportation, but also to the very basic idea of the European integration. Therefore one might argue that *free movement* requirements trigger broader EU competences. Besides, the EU has again another kind of competence to act, namely "to carry out actions to support, coordinate or supplement the actions of the Member States in certain areas such as (a) the protection and improvement of human health; (b) industry or (d) tourism" (Article 6 TFEU), which all involve the very issue of the autonomous vehicles too.

These complicate structures of the EU, actually boil down to various, often soft, legal tools regarding road safety and autonomous vehicles, like declarations (Valletta Declaration on Road Safety, 2017), resolutions (Motion of the European Parliament (2015/2103(INL), guidelines but also directives (framework directive 2007/46/EC on type-approval of motor vehicles) and regulations (Regulation (EU) 2017/1154 on type-approval of motor vehicles). This structure of the legal competence in Europe is, therefore, conspicuously more complex, than that of the USA. Especially because the relevant authorities of the Member States still have further room for manoeuvre to regulate, since it is not yet preempted by the EU.

Yet, it is not preempted in the USA either. The U.S. Code, Title 49, Chapter 301-305 on motor vehicle safety, standards and compliances, which basically corresponds to the EU regulations on type-approval of motor vehicles, is not yet adjusted to the automated vehicles, therefore many states issued special regulations. Having wished to stop that regulatory wave of the States, the Obama Administration in 2016 allowed the federal supervisory regulating agency (NHTSA) to preliminarily exempt some automated vehicles from the compulsory compliance with certain requirements, until the Department of Transportation, DOT, elabourated an acceptable version of new regulations. This exemption seems to be approved in both actually, competingly, debated Senate and House Bills and even in a growing scale (Senate Bill: S.1885, House Bill HR 3388). Thus in 2020 there would be 100.000 such driverless cars in the public roads in the USA. The justification seems to be that technology becomes ever better and the driverless cars are much safer than the conventionally driven cars are.

In addition to the tiring issue of division of competences related to the topic, there are, however, other differences between the US and EU regulations: firstly the divergent structure of the EU and the USA, secondly the divergent way of approach to the regulation as such and thirdly, the divergent basic legal institutions applicable in this field.

Certainly, due to its lacking of federalism, the cross-border incidents in the EU can trigger international law further complicating the legal problems, like in the case of a cross-border accident (Kiilunen 2018, Pétervári 2017, Nagy 2010). Mostly for this reason, the EU also employs a more administrative approach towards regulation, since it lacks the real power of enforcement, so the ticking of the check box in the compliance procedures is rather convenient. But this might not serve the interest of the competing industry. The recent regulatory approach of the USA has, on the other hand, been very much innovative and competition-friendly above all. The exemption policy *puts the risk* of bad regulation, or no regulation whatsoever, on the federal regulatory agency. In the meantime not even the States may legislate on the safety requirements of a driverless car, albeit especially big cities are tempted.

Needless to point out, that the mainstream European approach is conceptually different. Already at the beginning of the 2010's various working groups in the EU suggested a "top to the bottom" approach to the legal problems of robotics (Leroux – Labruto, 2012 10). Certainly, there are rather convincing arguments supporting this attitude, like avoiding wastes by not investing in competing but failing research projects and thereby gaining time. Nevertheless there is no guarantee, that an action plan based on administrative prescriptions, no matter how deliberated it is, will serve a safer and quicker result. All such an approach can assure is, that whatever the result is, it will be expensive. This undoubtedly provides less smooth pathway for innovative manufacturers, *since the burden of risk* will be held by the industry and not the administration. Surely, however this burden of risk will ultimately be paid by the consumers, and the risk in this kind of world of innovation is generally allocated to the tax-payers. This may not be unfair but less efficient.

Not surprisingly, though, in certain fields, the stakeholders may dictate in both worlds. The driverless cars run first of all in cities all over the world and both the US and the EU concentrate the scope of regulations on automated vehicles to the lighter type of cars. Thus, for example, lorries cannot be exempted in the USA. This may seem to be counterfactual, though, since automated lorries are expected to be less dangerous rolling on the public roads (like OTTO of Uber) than the automated cars in the cities. Nevertheless due to the existing fear of employees, and the governments, the stakeholders' concerns are very strong and seemingly deserved legislative attention in this and other primarily robotics threatened industries.

The lack of the necessary skills to understand the applied technology makes the law-makers and the courts vulnerable to this controversial information asymmetry and might also have a disadvantageous impact on applying *less reasoning* and *more technical slang*. The unintended acceleration problems in car crashes in the Toyota case of 2009 are good examples to that. The jury may not be competent enough to decide on real causation, some experts claim. Whether the undeniably many bugs in a software can be proven to directly lead to fatal crashes, that is the question. In traffic accidents the driver's negligence needs to be shown to find him liable under common law. The driver can defend himself by claiming, that it was not his fault but that of the car. Then the so called proximate cause has to be evidenced, namely, that the accident is the direct causation of the existence of all those bugs in the cars' software. And then the real question is, if an expert witness explains to the jury that the standard of the numbers of the bugs allowed in "one software": is zero, or maximum 5-6, and in the "relevant software" there are 1000 of them, then if the jury can count, the software producer will definitely be found liable, no matter whether that is verified to calculate the bugs so (Cummings 2017, Parrish 2016). Although in this case Toyota finally lost generating billions of dollar damages, these sort of product liability situations do not necessarily end so. And what is more, especially in the case of driverless cars there is no "one software" or it is almost impossible to track down the "relevant software", let alone the possibility of the car to develop "own softwares" with the deep learning method.

The new challenges provoke new models and there are various possible answers for how to create an architecture of the regulation by design and how to make designers be responsible for it. Some argue for translation from the real space to the cyberspace (Lessig 1999), a commitment to moral understandings and values in technical regulations too (Urquhart – Rodden 2016), application of the rule of law considerations in the cyberspace too (Murray 2013) or language gaming, design by communications (Koops – Hildebrandt – Jaquet-Chiffelle 2010). These are all important issues so that to ascertain on whom to allocate the risk, the burden of proof, the impossibility of proving or the impossibility of foreseeability, to name but a few.

### *2.2. The regulatory challenge – are there robot-subjects or do the robots have legal personhoods/personalities*

In fact, the regulatory challenge, related to the automated vehicles, is that it encompasses obviously many more legislative areas than just that of the transportation. Safety on roads covers a lot more than just a physical well-being or simply a being on the roads without accident.

Driverless cars create new environment. It presumes swiftly communicating softwares of others and complex infrastructures. But, most importantly, it allows on the spot decision-making without human interference. Apart from the usual technological development problems, therefore, this all requires, from a legal aspect, *special cooporations of old* market actors as well as *innovative applications of old* knowledge. Thus beside the general manufacturing questions the legal institutions seem to be tested too.

If a driverless car is to make an on-the-spot, or even a predetermined but externally generated, decision, for example, it needs to rely on special networks of databases, involving the questions of ownership rights, copyright and software issues, beside personal data protection and liability considerations. A driverless car, to be able to navigate on the public roads, needs data owned by a competitor, a driverless car's data one-two-three cars of it ahead, or needs to have access to others' special databases without the necessary legal relationship between the parties, resulting in, perhaps, the lack or in the end of the privity of a contract. Yet, vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication may be rendered on a general duty of care in the traffic. But it triggers further concerns of protecting one's data, one's private data in a commission trip of the driverless car.

Obviously, the conception of property constantly changes. No one really thinks nowadays that without possession one could not have ownership, although possession used to be the bases of ownership: what I could possess, what I could grasp and protect should be regarded as mine. Hence come the tangible goods. The intangible things or assets, on the other hand, posit real headaches for lawyers even today. Intangible things, nonetheless, are vital to the business. Long before, came the *copyholders* of the land, then the *shareholders* in the company, which could be owned and thus became negotiable separately from others. Then even the "market position" as such was recognized as a unique subject matter of transactions thereby creating ownership and value. Afterwards the database was awarded legal protection, as a special asset, *sui generis* subject matter of the copyright and the civil law. And now the hottest debated issue is the ownership of the data in the clouds (Reed 2010).

These piecemeal changes in law basically follow the demands of the business and provide guarantees to assets there, where it is so desired by the market practices. Capitalism has always been built on information capital, thus on the efficient allocation of property of information, like business secrets, copyright, patent and know-hows (Cooter and Ulen 1989).

A self-driving car, however, generates further basic regulatory questions of robotics and law today. From a delicate legal point of view, there is an intriguing suggestion in the technology and law literature to consider (Calo 2015, Santosuosso – Bottalico 2016). Accordingly, depending on the nature of its purpose, task or function, an "intelligent" machine may be regarded either as a robot-*object* or a robot-*subject*. In a somewhat rude interpretation and summary, a robot-object, despite of its ability of information-transmission, qualifies as a thing in the eye of the law, if it is not autonomous. Autonomous in this respect would mean that the robot has independence, cognitive skills and special cognitive architecture too. Cognitive architecture would further include three special elements: teleonomy (special directed purpose), adaptiveness (capacity to adjust to the environment when challenged) and teleology (capacity to interpret the environment and adjust goals and means accordingly). Therefore, a targeting system, the argument goes, is still a robot-object, because of lack of independence: the ultimate decision

is made externally, an operator pushes the "fire" button. Also, a landmine may well be independent, but lacks cognitive skills, since it explodes automatically when so programmed. A self-driving car, on the other hand, may rather be regarded as a robot-subject: (i) it is independent, it requires no external influence, (ii) makes independent decisions (iii) it has directed purpose, it understands its purpose and it is capable to adapt its actions to the environment, necessary for its goals to achieve. The final conclusion of this narrative is that the robot-subjects would be recognized differently in the legal context. Instead of calling it a thing, it would be a "non-human" agent, acting on behalf of the principal, let it be the owner or not. And in this latter case, the relevant applicable laws are different. In lieu of property and intellectual property or employment rights, products liability issues or consumer and data protection, the applicable laws or legal institutions here would rather be the agency problems, legal capacity issues, criminal law, torts, the non-contractual liability, e-personhood, intent, etc.

Consequently, driverless cars may be called also as tele-operated autonomous vehicles with cognitive skills. These cognitive skills, with special respect to the latest results in deep learning, allow better adaptivity and decision-making of own-account. Deep learning however, provokes further questions for lawyers: how to know whose software was bugged or whether it was the driverless car itself who generated the bug itself. So are these autonomous vehicles equipped also with cognitive architect, as the theory requires it from a robot-subject?

Definitely not, yet. Asserting that a robot can speak or answer the questions – even all questions – does not mean that the robot understands what it says. There are plenty of examples to that: Bina48 in the 1990s, Watson Jr. from IBM in the turn of the century/2000, or Sophia in 2018.

Driverless cars become robot-subjects, again, no matter what the rule is, when risk allocation rules for innovation so desire. The robot-objects are not at all in the visier of the law because they first need to qualify as a thing. A thing is defined by the legal literature. A general definition is that it has to be something that a man can keep under his control or power; even the wind, or the sun. As soon as the robot-object becomes more evolved, one could argue, and bursts out of this control, it becomes a robot-subject any way, even if the rules do not recognize it. Liability issues however are not at all the subject matter of pure moral and legal concerns, there can be plenty of examples to that, like the legal entity and liability or even culpability of a company.

The recent findings of neuroscience is that the free will, or the operation of a human brain maybe more pre-determined than it is generally accepted by the tort law or criminal law since at least the enlightenment (Scwaab 2014). So legal punishment might lose its ground and so it would put delicate questions to the law and robotics (Eszteri 2015).

Truly, these problems are not only legal questions but deeply rooted moral issues. The answers, therefore, more often than not, reflect one's own world view and one's tacit attitude towards legal norms as such, from a strictly legal point of view. If one accepts the view that the law is separate from any ethical concerns, than the law should be the matter of rational choice and economic interest beside the political deliberations. On the other hand, if it is not acceptable and one could not imagine a world without the moral foundations of the legal norms, then the answers to these challenges may lead to a very different path.

This paper here, focuses on only a few of the problems, namely the privacy issues, the software issues and the strict liability issues.

## 3. The applicatory challenges by analogies

### *3.1. The applicatory challenge by analogies – Privacy analogies*

The construction of privacy changes. Robotics in the driverless cars are desperately data thirsty. They need various enormous databases to be able to operate. Thus driverless cars running on the streets often induce legal problems such as invasion of privacy, illegal data collection, illicit categorization and usage of them, to name but a few. Some of these include personal data, some infringe competition rules, copyrights or property rights of database-owners.

So what data and how should be protected?

The EU is highly sensitive to the personal data protection which is conspicuously demonstrated in the new General Data Protection Regulation (GDPR 2016/679). The idea of privacy by design (PbD) advocated in this piece of legal act is not at all brand new, it has been developed by the European Commission for some time, from the Privacy Establishing Technology project. However, the regulation itself was basically, though not entirely, triggered by the, allegedly, reckless use of the European citizens' personal data in the USA or US companies (e.g. Schrems v. Data Protection Commissioner C-362/14). The regulation has effect also outside of the EU in the sense that any company wishing to make any business in the EU but settled in a non-EET country should also comply (USA, China).

No doubt that both the European Union and the United States recognize privacy as a fundamental notion. The U.S. Constitution enshrines protection against state intrusions and the Charter of Fundamental Rights of the European Union (the Charter, art. 6-8) as well as the European Convention for the Protection of Human Rights and Fundamental Freedoms (the ECHR, art. 8) each mandate that law and public authorities are not to interfere with private life. Notwithstanding, lately, the state/police surveillance demands ever more invasion of these rights and a want for more data, due the recent indispensably data-addictivity of the new technologies and their reliance on mass businesses, and so allegedly mass security.

As one of the most influential judge, Richard Posner, in the USA puts it, "privacy is mainly about trying to improve your social and business opportunities by concealing the sorts of bad activities that would cause other people not to want to deal with you" (Posner 2014).

And this is perfectly demonstrated by the ECJ decision in the case of Gomez v. Google (C-131/12). The decision is wrong for its being as overbroad and over-inclusive as it is. Vesting a right in Mr. Gomez to claim a deletion of his data from Google generates serious problems with free speech and rule of law. In this case Google Spain had digitized a local newspaper in which, from that time on, if someone looked for an attorney in the region on-line in an advertisement, could bump into Advocate Gomez's house being at auction for overdue tax-depths. Upon Mr. Gomez claims the ECJ finally read the EU Treaty in a way, that Mr. Gomez was awarded the right to claim from Google to delete its link to his personal data. Hence there is a living *right be forgotten* in the EU.

Nonetheless, the right to be let alone advocated by Brandeis and Warren in 1890 was a conceptually diverging idea from the European right to be forgotten (Brandeis – Warren 1890). The *right to be let alone* meant something else, though the leading case back then might resemble to the problem of Mr. Gomez. In this legal suit Ms. Roberson, an attractive girl had had a picture made of her at a professional photo shop and in a short while she realized that her so taken picture covered the paper package of the flour in the relevant grocery shops all over New York (Roberson v. Rochester Folding-Box Co., 71 N.Y.S. 876, 876 (N.Y. App. Div. 1901). Although the majority was in favour of the photographer, there was a powerful dissent in the decision of the New York Supreme Court, even citing the famous Brandeis-Warren article on privacy. Yet, this case emerged with the rising new technology of the smaller, portable

photo camera allowing photographers to take pictures from anyone anytime anywhere, looking at the techniques of that time with a hindsight, and watching the then still man-size photo-cameras, this fear of invisible invasion of privacy by photographers must have only been a threat. However, the impression of the invasive being of photographers must have been felt real, because the new ever smaller and better versions of cameras came into the market so rapidly, that the threat must have felt very imminent even then.

Notwithstanding the internet, the crucial similarities in these two cases, more than a 100 years in between them, are that the actor who publishes or who decides to publish certain personal data is not the "owner" of the personal data. And this actor, thanks to the technical facilities, may act independently. It should be noted though, that in the early case of Ms. Roberson there were no copyright issues in the USA, whereas nowadays this aspect is not negligible at all. Ownership rights in Cyberspace, or the ownership in information is quite an important topic, since several of the basic elements of the term ownership are missing, namely the classical "thingness" of the object of the ownership and the exclusivity, or the exclusive use, of the owned "thing" (Reed 2010). On the other hand these cases show the huge difference in scale, in huge public access, which may matter the most.

Truly, the term privacy has problems and there is a discrepancy between the EU and the USA (Reidenberg 2014). Europe supports privacy even at the expense of free speech, and commercial speech too, which is the language of the business communication, the freedom of advertising and marketing. The USA does just the opposite. And indeed, legal privacy has many ramifications (Gormley 1992) and the construction of those may not always match between the American and the European one. Firstly, there should be the right to have secrets from the State even (laws against unwarranted searches), secondly, the right to have own opinion and to let it be public (free speech), thirdly, the right to be let alone (tort laws, damages by delicts), and fourthly, the right to have fundamental decisions (rule of law principles, fair hearing, fair trial). In addition, the new kind of business-models enabled by the new technologies provide further privacy issues, like the cross-border jurisdictional legitimacy problems. Whereas Brandeis and Warren dealt with basically the right to be let alone, the legal problems generated by the new technologies nowadays embrace all privacy elements.

Now, when a driverless car wishes to travel through several cities or countries in Europe, it needs to have access to a lot of databases. It uses for example, official public databases when gathers information about the street facilities. Then it uses private databases for meteorological data or pictures of the artificial world in the human environment, or outside. It may have access to personal data too when reaches out to the clouds and collects information about the exact location of a person, depending on the driverless car's mission. And again, it uses information which is owned by someone else(s). In these instances the smart things full of personal data being used and stored in one's home might become a useful, but illicit?, resource to the driverless cars.

The prescribed 'privacy by design' in the GDPR may not necessarily be safe unless privacy is legally clarified, precisely described and expressed to the designers and the design is specified in due course and in due terms. First of all however, the GDPR is a general regulation and even if it is directly applicable, certain technicalities require further elaborations. Besides, these specificities needs to be provided by the relevant authorities of the relevant Member States according to the applicable EU directives, such as the e-Privacy directive. Encoding privacy requirements into software is obviously, not at all self-evident in the EU.

Koorps and Leenes criticize therefore that the entering into force of the GDPR and thereby the privacy by design, would not solve even the problems of the personal data owners (Koorps-Leenes 2014).

According to their opinion this new regulation would not change the existing mode of operation and would not stop the pattern in which the industry tries "to achieve rule compliance by techno-regulation". The claim is, that what may be intelligible for a human, may not be as such for the machine, the driverless car.

The Turing test fails here. Even if this test can help to decide whether the other speaking party is a computer or a human, it cannot have any prediction whether this other party thinks or understands his doing as well. Searle has his relevant, even rethought, criticism with the Chinese room, in which a sole non-Chinese speaking human could answer Chinese questions with a dictionary and a grammar book without understanding the questions let alone the answers (Searle 1980). Should that now mean that the autonomous vehicle cannot be liable, and that the data collected by the driverless car on the street can be freely downloadable because it has no rights either?

A question, what data could be collected and under what purposes on the public roads, could therefore be very important. It could include to decide whether special human mental diseases may contribute to traffic accidents in the streets. Is it allowed that manufacturers collect data therefore on sensitive health issues for safety reasons or health preservation on the public roads? What is more, the transfer of such data may further create sensitive personal data infringement. In order to facilitate the designer to "translate" these kind of purposes and requirements into codes there are other possibilities. Instead of regulation by design Koorps and Leenes offer the *regulation through communication* (Koorps-Leenes 2014 9). IoTs and autonomous vehicles should use data for profiling as well, since they in fact support one's routine activities, which, again, on the other hand, is a sensitive issue in the GDPR. This to be done needs prior and clear understanding and consent and in case of circumstantial changing, the approval needs a renewal too. To translate these changes in time more thorough interpretation and understanding is suggested.

This structure of data protection does not sort out the question, though, citing Posner above, whether it would be such a problem, if certain personal data were less protected and more public, as it used to be prior to the capitalism.

Despite of its newer regulatory model of the GDPR, the very existence of the GDPR is an evidence of how the top bottom law making works in law and robotics. Advocates of the GDPR claim that this regulation is needed, because the bad practices should no longer be tolerated and thus the social conventions must be changed by the law, ultimately by legal sanctions. However, the GDPR could well create a rather administrative, check-the-box answers with a send-the-declarations or disclaimers-always-everywhere attitude.

On the other hand, designers come to the market with products, with carefully prepared regulatory design, fit in the legal framework of the laboratory times. With the shift in time, however and when they really hit the market, the law changes and so should the regulation by design again, which again, is not so trivial. Koorps and Leenes demonstrate it by referring to the simple and surely predictable problem of aging: a minor needs the approval of the parents in order to have consent to data collection, but how to monitor its changes?

Surely, laws on robotics require from lawyers the understanding of technological details. And this is the challenge the law faces and which may be described by the stealthy technologies which again would trigger a necessary interdisciplinary pragmatism (Calo 2015, Urquhart – Rodden 2017, Somkutas – Kőhidi 2017).).

### *3.2. The applicatory challenge by analogies – legal entity*

Although it is a (statistical) fact that autonomous vehicles create safer public roads, still no one needs an extraordinarily vivid imagination to fancy how much damages an autonomous vehicle may cause, if something goes wrong, without any human interference. Certainly, as long as the machine follows the rule, the encrypted orders, it may not be held legally liable. But let's suppose that there is a fleet of driverless cars operated by a network of these cars. Is that sort of business enough for holding this network of autonomous vehicle responsible, even liable? If this business makes money, should the driverless cars also be able to make money?

Common sense, that to qualify as a legal subject, one does not need to be a natural person or a human being. And this is true the other way round, not all human beings are/were legal subjects. Good examples for the first are companies with or without legal personality, the state or its agency, like the authorities, ministries. And examples for the latter are slaves. Currently, "everyone has the right to recognition everywhere as a person before the law" (according to the UN Charter, Art. 6). Also as *ius cogens*, it is found in the Hungarian Civil Code as well (HuCC Articles 2:1, 2:4 on the legal capacity of a human person and Art 3:1 on the legal capacity, and the scope, of a legal person). Though "everyone" needs not necessarily be a human being, the preamble of the charter might be construed that way. A thing may be owned, a person acts and has self-consciousness about his doing it, about his doing it rightly or wrongly. Nonetheless not only (human) persons can cause changes to the environment, or damages for that matter. Frequent examples are animals, but plants or volcanos too, in fact.

It is a commonplace too that law is a social construction and as such, granting non-humans legal personhood (legal personality or legal entity) may be a matter of rational choice, depending upon the world view of the regulators though. For a historical analogy, companies acquired the title of legal entity geographically sporadically but almost always driven by necessity motivated by business considerations (Hansman – Kraakman 2000). Without a reliable, transparent registry, the creditors were finally awarded with the separation of the assets. In order to create a trustworthy business environment the assets needed to be separated, so that to enable the creditors to have access to the company assets without competing with other private creditors of the company owners. So the legal entity of a company was a good move, even so because soon the limited liability of the company indeed insulated the assets of the company not only from other creditors too but also from the owners and the private creditors of the owners. Credit became cheaper.

Legal personality therefore is not necessarily a moral issue. Legal personality or legal entity allows one then to be recognized by the law, so that any act of this entity be legally challengeable, have legal consequences. On the other hand this legal entity may have also access to the courts in case of its grievances. Under classical European continental law legal capacity to have rights and duties is to be distinguished from the legal capacity to act which may be denied from non-human legal entities constructed merely by the law (Smith 1928).

And so it is in the case of the companies. So is the legal capacity of a company limited, it cannot act on its own behalf. Needs an agent. Notwithstanding the limited liability of certain companies, the liability of the companies are recently extended to certain criminal activities. It means that the acts of certain employees, usually that of the management, can be attributed to the corporate entity, if this activity benefitted the company and the employee committed it as the manager of the company.

In any event this sort of development in legal thinking has ever been based on the economic interest, on property allocations. And so, even if it seems now to be a shift in the legal thinking, it is not. Such application of a fiction is not at all new and conceptually the ultimate sanction is an analogy. The

termination of the existence of the legal entity may be parallel to the execution of the human person. The reason of attributing this (criminal) deed to the company is therefore a moral and a business concern rather than a legal one. Why should the company be able to get away with a tax fraud, for example, when the company had the benefit of the crime and also the collateral, perhaps, for the remedies.

The idea is that the borderlines in the fields of liability have become blurred, and there are no longer clear distinctions among the territories of the criminal and the civil law or the administrative law liability. But this is not that big a change under common law, even if it creates debates under the German civil law tradition (Bérces, 2015, Ligeti, 2002, Eszteri 2015).

The *objective liability, the liability without negligence* or intent is not at all a new legal institute. The idea, that it is not only the human that can cause harm is again not a new notion. These legal tools of interpretation, however, were designed to be applicable in environmental protection cases or anti-corruption cases and not for machines having impacts on humans' life.

And in this sense, there is a distinction. In the case of the AI, IoT or autonomous vehicle it is ultimately *not the human* whose action is being under scrutiny and then judged. Therefore, none of these cases raised as seriously the question of legal personhood as it is being discussed in relation with the IoTs nowadays.

The technological phases of the artificial intelligence (AI) obscure the borderlines of the development and so the level of capacity too. The legal capacity of these machines may be hard to fix. According to a widespread notion of conditions an AI needs to be conscious about itself in order to gain legal personhood. No doubt, it all leads us to the interpretation of the other minds problem and the predictions of others acting and doing. But neuroscience does use predictions very often even at courts, at criminal trials. And so does the judge at the court, the prosecutor and the police too (Garland ed 2004 116). Clearly, the widespread use of such technique may not qualify the method as good but certainly as something practical which cannot be replaced with something better, so far.

The breaking point in questioning of the legal capacity of an AI was provided by Lawrence Solum's highly intriguing and illuminating article in 1992 (Solum 1992). He wrote that, with due regard to the complexity of the issue, the answer needs to be a *pragmatic* one. So he put the question, whether an AI may be a trustee. Solum distinguished three different levels of an AI. Firstly, the AI absolutely routinely follows the rules/orders and serves basically as a huge library for the owner who actually makes the transaction with the AI's assistance. Secondly, the AI practically sorts out the business on its own and enters the contracts but needs the signature of the owner. And thirdly, the AI does everything alone. Solum's conclusion was that although the time was not ripe, there might come a turning point where the AI will claim for own perhaps constitutional rights: what would stop an AI to open up a Law Directory on line and commission a lawyer to represent him at the court. Nick Bostrom would certainly object, alleging that it is due to the construction, the architect of the machine, which disables a machine to "think" as a human (Bostrom 2003). Solum further argues that multiculturalism prevents us from denying this possibilities for non-humans and he predicts the necessary change in legal concept of the legal personhood.

Twenty years later, Koops, Hildebrandt and Jaquet-Chiffelle relying heavily on this article and on its findings concluded still that at the time being, a proper construction of the *existing laws would suffice* (Koops – Hildebrandt – Jaquet-Chiffelle 2010). After having screened and summarized the relevant new European (legal) literature, they argue that the laws are flexible enough and allows the interpretation of the *laws on agency* – however divergently in the USA and in the EU – to be applicable to the machines

being built. On the other hand, they emphasize, that sooner or later, all of the researchers suggest modifications to the law and perhaps to the legal concept as well (e.g. Matthias 2008).

According to their model, which recommends also a three-step approach, in the short-term, at the starting point, the interpretation and extension of the existing law suffices (Koops – Hildebrandt – Jaquet-Chiffelle 2010 554.). At this level, in case of a legal transaction, the acts of the computer may be attributed to the owner/user as his general intent. In case of invalidity problems, if the computer buys more shares than should have the court would have no difficulty to decide on the intent of the owner as the intent of the human and not that of the "electronic agent", since agency rules may not yet be applicable. As a middle term, they argue for a limited personhood with strict liability. At this level agency rules could already apply, so the agents need to be registered as such in a public registry which could allow the contracting parties to find the identity of the agent's principal (555). Besides, they recommend the cautious introduction of a limited type of personhood for the e-Agent with a strict liability, so that the owner/user of the electronic agent may be found and be liable in its stead without questioning the intent. A further suggestion is that these electronic agents may receive a modest provision for their activities which may be a bases for an insurance fund in case damages occurred and they themselves may be found liable (in civil law only), mostly because the owner/user may not be located or they deny that they gave reason to the transaction be in their names. And finally or thirdly, when technology evolves further, the long term solution is a full personhood with "post-human" rights. Post-human rights would refer then also to that that this is not the "classical human rights" anymore. This should be the time though, when self-consciousness emerge. As a criticism to that smart future, it is argued too, that this sort of consciousness is rather facilitated by interconnectedness, thus not individual or "real". On the other hand, cognitive sciences pile up evidences to make us believe that "human identity itself emerges from distributed brain processes" (559.).

To translate it all to the autonomous vehicles, it is for sure, that so far we are at the threshold of level two and three. To attribute intent or *mens rea* to the driverless cars and let them prosecute or be prosecuted in criminal law, should have a long way to come so far. That would surely require a certain non-predictability or an intentional deviation from the rule, with purpose. That is not very likely yet. It is unlikely that a driverless car on mission to the airport to pick up a friend of the principal would go to the theatre instead to pick up the most celebrated actor in the region; and thereby causing a car crash in front of the entrance in the overcrowded street. However, strict liability in car accidents may be attributed to the driverless cars, since it does not demand the reasonable acting or the questioning of the reasonable care. Here there is no investigation into the proximate cause and thus the classical conditions like intent or fault, negligence or recklessness are not considered.

On the other hand due to the damages a driverless car may cause, the risk must be assessed and allocated efficiently in advance. The autonomous vehicles' liability therefore may be paralleled with the strict or objective liability of the companies (product liability) in private law and be based on a simple risk allocation mechanism and not on intent. It is not the punishment or the retribution which should count, but the desire for restitution, the restoration of the assets status quo. The restoration of the wealth distribution to the pre-accident status quo is a private law principle as opposed to the criminal law ones. So the question is to which model one reaches out. If this could cause a paradigm shift, then it seems, that the insurance lobby might object that, since with such a shift all could incalculably change.

### *3.3. The applicatory challenge by analogies – Software warrants and strict liability*

In the case of an autonomous vehicle therefore liability issues may become somewhat complicated. Based on the three-step model of awarding legal entity to an AI an autonomous vehicle should linger somewhere between the second and the third phase, at best. That would mean that the driverless car could have a limited legal entity should be registered in a public registry and should be vested also with strict liability from the owner/user part. Driverless cars therefore should act as agents and their actions should create rights and obligations directly to the principal. Further capacities will definitely be awarded if liability on its own account will be more innovation-friendly.

In case of a car crash, the principal or the owner does not drive. This is not a big difference in most Member States in the EU, where strict liability laws apply in these cases, and, more often than not, the owner/operator of the car is liable, who might happen to be the driver but not necessarily. It can be so, since strict liability has no causal condition as in a negligent or intentional tort. Simply by operating a highly hazardous equipment triggers the stricter, non-subjective, liability. In other words in these accidents the driver/owner/operator/principal can hardly be exempted from liability if damage occurred.

On the other hand where negligent tort rules apply, like mostly in the common law, the driver himself is liable only if negligent and therefore the proximate cause of the accident has to be cleared and proven by the plaintiff in order to be able to collect. The defendant in these cases can be released if he shows that the car was defected. In the event however, that the car is autonomous, the driver is the car itself, so the manufacturer would be highly motivated to grant certain legal personhood to the driverless cars. Then the autonomous vehicle, as an electronic agent will be held liable. Should it be strict liability applied directly or should it remain a negligent tort?

In any event, the liability issues need to be determined on a case by case basis, regarding also the fact that with the driverless cars the software problems may override the hardware ones. And software failures are often harder to allocate but even harder to find the causal link with the necessary evidentiary standards. Like in the case of unintended acceleration software problems in certain Toyota types in the 2009, in which the victims of accidents managed to prove that the software of the breaking system had bugs. The case remained controversial until years later the management of the Toyota Company confessed lying. The criticism pointed out that the causal link between the admitted bugs in the software and the direct cause of the accident was not proven at the court and the jury was wrong. (Cummings 2017). "It is well known that nearly all non-trivial software has bugs. Furthermore, because there are virtually an infinite number of different ways of solving a non-trivial problem using software, one can often find many opportunities for criticizing software quality, sometimes using criteria that are highly subjective. As a result, the plaintiffs in a software trial can be expected to attack the defendant's software by looking for bugs and criticizing the software's quality. If they can find bugs, and show that more likely than not those bugs caused the accident, then they can establish causation. They can also use purported measures of software quality, which may be subjective, to argue that the defendant failed to fulfill their duty to provide software of sufficient quality" (Cummings 2017 1.).

Surely, the running of the driverless cars on the streets will trigger these sort of liabilities through the warranty problems of others' softwares, like the use of the free softwares and open source softwares. In these cases the risk and thus the liability questions need to be ascertained on a case by case basis and in case of doubts, the damages should be borne by those in whose interest the driverless cars were operated. The present rules on car crashes could well apply in the non-common-law countries, as said, where in such cases the strict liability is the rule.

Safety standards are a starting point in these cases, since consumer protection and product liability derives from the assumption that the product needs to be safe. But how safe? Obviously a driverless car

is regarded as to be safer than a car without or nearly autonomous driving. So under common law jurisdiction the question is, if notwithstanding, there is an accident, then the manufacturer is liable if the driver is not at fault. Product liability consists of three elements: defect in the product, defect in the design and lack of warning or lack of instructions. To translate these into the software case, bugs should certainly qualify as defects in the software. In those autonomous vehicles though, in which the deep learning is a standard, a bug may not necessarily be programmed from the start but might have been learnt by the machine. In all these cases the state of the art defence may help out the manufacturer from liability. Since most of the car companies rely on many suppliers, the driverless cars contain various softwares from different manufacturers, embedded even. This makes even harder the proving of contributory negligence or the percentage of interaction in the operation of the hazardous equipment, the car, in the accident.

Additionally, the autonomous cars need data. These data, for cybersecurity reasons, are provided via separate, very quick Wi-Fi like facilities, like the DSRC (Dedicated Short Range Communication) in the USA, and, probably, 5G in Europe, especially in Germany. The data flow needs to be free from misunderstanding, misinformation and hacking. In case of misunderstanding the question is whether there is an interoperability problem, or the rival systems fail. In any event, the node needs to be found and decided where the faulty data came from. In-built cautious messages, designs, such as use 'break, if…', could release liability. There probably is a duty of care on the public roads among the actors, therefore, if there is a misinformation, then the sender of the information may be liable for negligence or fraudulent misrepresentation if he knew or should have known that the information was false. Besides, the receiver of the information needs to show reasonable care to rely on the information received and does not react if other information contradict, like an obvious change in the traffic order. Cybersecurity protocols require special verifications of messages and other protection but hacking remains an evergreen issue, the softwares have to be able to manage it. In the end special investigation is needed to find the very legal entity, the manufacturer, supplier, seller, repairer, owner or operator to be liable. Bugs existence needs to be accepted and the software so designed so that to react reasonably cautiously.

Despite of the Toyota case, software liabilities are generally privileged in the legal systems. In case of contractual breach, the damages are limited even above the standard of the foreseeability doctrine and in torts cases the rule of economic loss applies. These all serve the same purpose that purely economic damages cannot be recovered and that the costs of innovation be widespread. Softwares in Cyberspace are extremely intertwined and since robotics are often facilitated by/on the internet, the security of the softwares is a crucial point in driverless cars. It is because robotics, and especially the driverless cars, unlike the softwares on the internet, are designed to be active in the real space, thereby much easier and more possibly causing more physical harms.

The application of strict liability of either the driver, which can certainly be the driverless car itself according to the level two-three above, or the producer or the owner, is justified first of all because of the acceptance that there is no bug-free software and because the very existence of the bug in the software may be discovered only by use. Thus the real question boils down to the procedure or to the protocol to be followed by design in situations of emergency. It is important since strict liability might provide for exemption in cases where the accident is due to an unavoidable interference of an action from the outside of the scope of the operation of the hazardous equipment, the car.

## 4. Conclusions - The smart future

”Well, Senator, my position is not that there should be no regulation” said Mark Zuckerberg, the CEO of Facebook at the Senate hearing, in a dialogue with Senator Lindsey Graham (R-South Carolina) (CNET Joint Commerce and Judiciary Committee SH-216, April 2018).

Entering a search request into the search engine of the Google Scholar, one receives more than 2.660.000 findings for the technical term ‘legal paradigm’, even if there are only about 1% out of these, which really match the request. And this is so despite the fact, that the notion of paradigm, is not at all evidentially applicable in the social sciences or humanities, thus in the legal context. Thomas Kuhn used the expression of paradigm, without the adjective, primarily to describe and to understand the truthfulness of the various and sometimes contradictory scientific assessments of natural sciences. His point of view was definitely historical and argued that certain statements may well qualify as scientific in one paradigm and not at all as such in another paradigm. Paradigm, summarized rudimentarily, would mean a complex world in which scientific development is achieved with putting the tiny little verified puzzles of the whole picture together. A paradigm shift would be brought about, put it again very unsophisticatedly, when certain puzzles could not fit in and so they challenge the truthfulness of the entire picture.

But these sort of paradigms were meant to measure/commeasure sciences pure, which were computable or verifiable in its strict sense. Social sciences and humanities, on the other hand, are not based on calculations merely, even though economics, sociology, demography, statistics would so claim. In any event law, or legal studies, is evidence-based, uses interpretation, argumentation and reasoning, and it relies much much less on calculations.

But paradigm shifts, for their being a social construction too, sociologically may also be biased. Accordingly, the paradigm shift may be delayed or accelerated depending on the social embeddedness of the very advocates of the different puzzles fit or unfit into the relevant dogmatic picture of the existing paradigm.

Paradigm, nevertheless, may translate into a context: a context of rules and language, to simplify again. And if so, it may apply to the legal environment as well, since, in a way, law relies on reading and interpreting texts by using the rules of the language.

This paper discussed the problem of paradigm shifts in legal thinking through the technique of analogies. It concluded that as long as the same interpreting tools, such as fictions, analogy, distinctions, etc., are applicable in the various incidents and the court cases, there is no paradigm shift in the normal science. The answer is upto the courts.

## References

[1] Aarnio A 1984 Paradigms in Legal Dogmatics *Theory of Legal Science* Springer Dordrecht Peczenik A, Lindahl L and Roermund B eds **176**
[2] Aarnio A 2011 *Essays on the Doctrinal Study of Law* Springer p 237
[3] Bérces V 2010 A magyar büntetési rendszer reformjával kapcsolatos jogalkotási kérdések *IAS* pp 83-99
[4] Bostrom N 2003 Are we living in a computer simulation? *The Philosophical Quarterly* **53** 211 pp 243-255
[5] Calo R 2015 Robotics and the Lessons of Cyberlaw *Cal. L. Rev* **103** p 513

[6] Cooter R and Ulen T 1988 *Law and Economics* HarperCollins pp 645
[7] Cox I and Wilfong G eds 1990 *Autonomous Robot Vehicles* Springer New York pp 477
[8] Cummings D 2017 Was the Jury Wrong about Toyota's Software? How Questionable Testimony on Embedded Software Tipped the Scales *IEEE Consumer Electronics Magazine* pp 103-107 [DOI: 10.1109/MCE.2017.2684939]
[9] Daithí M 2016 My Favourite Things: The Promise of Regulation by Design, JOTWELL
[10] Deibert R et al 2010 *Access Controlled - The Shaping of Power, Rights, and Rule in Cyberspace* The MIT Press
[11] de Vries U 2013 Kuhn and Legal Research. A Reflexive Paradigmatic View on Legal Research*: *Recht en Methode in onderzoek en onderwijs* **3** 1 pp 7-25
[12] Eszteri D 2015 A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései *IJ* pp 47-57
[13] Fuglinszky Á 2015 *Kártérítési jog* HVG-Orac
[14] Garland B 2004 ed *Neuroscience and the Law*. Brain, mind, and the scales of justice. Dana Press New York | Washington, DC
[15] Gelén K ed 2017 *Jog, innováció, versenyképesség.* Wolters Kluwer Budapest p 172
[16] Gillespie N 2014 Richard Posner: Privacy is "Mainly" About Concealing Guilty Behavior. *Reason. Free Minds and Free Markets*
[17] Glancy D 1979 The Invention of the Right to Privacy *Arizona Law Rev* **21**
[18] Gookins E 2012 *Achieving a Safe and Reliable Product. A Guide to Liability Prevention*. ASQ Quality Press Milwaukee, Wisconsin p 145
[19] Gormley K 1992 One Hundred Years of Privacy *Wisconsin Law Review*. WILR 1335
[20] Graziano T 2016 Cross-border traffic accidents in the EU – the potential impact of driverless cars ipol studies
[21] Hansmann H and Kraakman R 2000 The Essential Role of Organizational Law. *Yale Law Journal* **110** No 3 390-440
[22] Hildebrandt M and Rouvroy A eds 2011 *Law, human agency, and autonomic computing: the philosophy of law meets the philosophy of technology* Routledge
[23] Hildebrandt M 2015 Ambient Law, Smart Technologies and the Rule of Law 27 octobre 2015 Cycle de conférences octobre-décembre 2015 Le futur du droit : big data, algorithmes et robotisation
[24] Homicskó Á ed 2018 Egyes modern technológiák etikai, jogi és szabályozási kihívásai. *Acta Caroliensia Conventorum Scientiarum Iuridico-Politicarum* **XXII**. Budapest p 223
[25] Johnson D and Post D 1996 Law and Borders – The Rise of Law in Cyberspace. *Stan LR* **48** 1367
[26] Jürgen R 2013 *Autonomous Vehicles for Safer Driving*. SAE International p 142
[27] Kiilunen V 2018 Autonomous Vehicles, Competence and Liability in the EU –Answering the Call of the European Parliament DOI: 10.13140/RG.2.2.10863.74403
[28] Klein T ed 2018 Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről. *Médiatudományi Könyvtár*. **30**. p 166
[29] Koops B – Hildebrandt M and Jaquet-Chiffelle D 2010 Bridging the Accountability Gap: Rights for New Entities in the Information Society? *Minn. J.L. Sci. & Tech* **497**
[30] Koops B and Leenes R 2014 Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law *International Review of Law Computers & Technology* **28** pp 159-171 preprint version
[31] Leroux C and Labruto R 2012 Suggestion For A Green Paper On Legal Issues In Robotics – *ELS issues in robotics*. Researchgate

[32] Lessig L 1999 Commentaries. The Law of the Horse: What Cyberlaw might Teach Us *Harv Law Rev* **113** pp 501-547
[33] Ligeti K 2002 Az Európai Unió büntetőpolitikája *ÁJT* pp 73-97
[34] Lunders C and Tarpley P 2017 Autonomous Vehicles, USA. in: *Autonomous Vehicles, The Legal landscape of DSRC in the US, UK and Germany. NortonRoseFulbright* p 7-11
[35] Matthias A 2008 *Automaten als Träger von Rechten. Plädoyer für eine Gesetzesänderung* Logos Berlin Verlag
[36] Murray A 2013 Looking back at the Law of the Horse: Why Cyberlaw and the Rule of Law are Important *Journal of Law, Technology & Society* Scripted 310
[37] Murray A 2007 *The Regulation of Cyberspace: Control in the Online Environment* Routledge
[38] Nagy Cs 2010 The Rome II Regulation and Traffic Accidents: Uniform Conflict Rules with Some Room for Forum Shopping – How So? *Journal of Private International Law* **6** 1 pp 93-108
[39] Parrish M 2016 The 2009 Toyota Accelerator Scandal That Wasn't What It Seemed
[40] Patterson D and Moratti S eds 2016 *Legal Insanity and the Brain Science, Law and European Courts Law and Neuroscience: revising the Legal Standard of Insanity* Hart Publishing p 336
[41] Pétervári K 2017 Autonóm járművek és jogi felelősség - a "Tesla" baleset; avagy ki vezet(het)i az autót *Gazdaság és Jog* **25**. pp 31-34
[42] Post R 1991 Rereading Warren and Brandeis: Privacy, Property and Appropriation. *Faculty Scholarship Series.Paper* 206
[43] Reed C 2010 Information 'Ownership' in the Cloud *Queen Mary School of Law Legal Studies Research Paper* 45
[44] Reidenberg J 2014 The Data Surveillance State in Europe and the United States, *Wake Forest L. Rev*. **49** 583-608
[45] Rudgard S 2011 Origins and Historical Context of Data Protection Law *European Privacy* IAPP publication
[46] Russen Spears V 2008 The Case That Started It All: Roberson v. The Rochester Folding Box Company *Privacy & Data Security Law Journal* pp 1043-1050.
[47] Sanitt A 2017 Autonomous Vehicles – The Legal Landscape of DSRC in the UK. in: *Autonomous Vehicles, The Legal landscape of DSRC in the US, UK and Germany. NortonRoseFulbright* p 35-40
[48] Santosuosso A, Goodenough O and Tomasi M eds 2015 *The Challenge of Innovation in Law. The Impact of Technology and Science on Legal Studies and Practise* Pavia University Press
[49] Santosuosso A and Bottalico B 2016 Robotics and the Law: A European Perspective *Autonomous Systems: Why Intelligence matters. Conference Lecture,* München, Automatik Industrie 4.0
[50] Sárközy T 2002 Büntetőjogi intézkedések a jogi személyekkel szemben? *MJ* pp 449-456
[51] Searle J 1980 Minds, Brains and Programs. *Behavioral and Brain Sciences*, 3: 417–57
[52] Smith B 1928 Legal Personality **37** *Yale L.J*. 3. pp 283-299
[53] Solove D 2004 *The Digital Pperson. Technology and Privacy in the lnformation Age* NYU Press p 296
[54] Solove D, Rotenberg M and Schwartz P ed 2006 *Privacy, Information, and Technology*, Aspen Publishers p 322
[55] Solum L 1992 Legal Personhood for Artificial Intelligences, *N.C. L. Rev*. **70** pp 1231
[56] Somkutas P and Kőhidi Á 2017 Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó. *In Medias Res* **2** p 232–269
[57] Stallman R 2002 *Free Software, Free Society*. Selected Essays, GNU Press. Free Software Foundation Boston, MA USA pp 230

[58] Sundquist M 2012 Oonline Privacy Protection: Protecting Privacy, The Social Contract, and the Rule of Law in the Virtual World *Regent Univ Law Rev* **25** p 153-184
[59] Swaab D 2014 *We Are Our Brains. From the Womb to Alzheimer's*. Penguin Books Ltd p 432
[60] Tóth A ed 2016 *Technológia jog - Új globális technológiák jogi kihívásai.* Budapest p 294
[61] Urquhart L and Rodden T 2017 Towards User Centric Regulation
[62] Urquhart L and Rodden T 2016 Working Title: A Legal Turn in Human Computer Interaction? Towards 'Regulation by Design' for the Internet of Things *Working_Paper_March*
[63] Van Egmond Van P, Nijkamp P and Vindigni G 2003 A comparative analysis of the performance of urban public transport systems in Europe. *Int'l Social Science Journal* **55** Issue 176, p 235-247
[64] Wadhwa I and Salkever A 2017 *The Driver in the Driverless Car How our Technology Choice will Create the Future* Berrett-Koehler Publishers
[65] Warren S and Brandeis L 1890 The Right to Privacy. *Harvard Law Rev*, **4**, No. 5 pp 193-220
[66] WIRED (2016/12).
[67] Zittrain J 2006 The Generative Internet, *Harv L Rev* **119** p 1974
[68] Ződi Zs 2017 Az információs társadalom legújabb kihívásai a jog számára - Horizontális platformok. *Gazdaság és Jog* **25**. pp 27-30

**Regulations**

The USA
i. NHTSA: Policy (Guidance) of best practices for the safe design, development and testing of automated vehicles prior to commercial sale or operation on public roads, 2017.
ii. USA House Bill HR 3388 on "Safely Ensuring Lives Future Development and Research in Vehicle Evolution or SELF-DRIVE." 2017
iii. USA Senate Bill: S.1885 — 115th Congress (2017-2018) [Report No. 115–187]: "American Vision for Safer Transportation through Advancement of Revolutionary Technologies Act" AV START Act, 2017
iv. Autonomous Vehicles / Self-Driving Vehicles Enacted Legislation. (05.18.2018) NCSL, National Conference of State Legislatures, USA
v. California regulation 2014
vi. California regulation 2018
vii. US Department of Transportation: Fact Sheet: AV Policy Section I: Vehicle Performance Guidance for Automated Vehicles 2016 12687g2-091916-v1
viii. Federal Guidance on Autonomous Vehicles, Washington State, October 18, 2016
The EU – The European Parliament
ix. Motion for a European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))
x. Resolution of 1 June 2017 on digitalising European industry 2016/2271(INI)
xi. Resolution of 18 May 2017 on road transport in the European Union; 2017/2545(RSP)
xii. Automated vehicles in the EU, EPRS briefing, January 2016
xiii. EU strategy on cooperative intelligent transport systems, EPRS briefing, September 2017
xiv. 5G network technology - Putting Europe at the leading edge, EPRS briefing, January 2016
The European Council
xv. Discussing the Commission Communication - Digitising European Industry Reaping the full benefits of a Digital Single Market COM(2016) 180 final, 20 April 2016, 8100/16

xvi. Valetta declaration by Ministers of Transport at the High-level Conference on Road Safety(Malta 28–29 March 2017) - Way forward /Valletta Declaration on Road Safety

The European Commission

xvii. Europe on the move: An agenda for a socially fair transition towards clean, competitive and connected mobility for all, COM(2017) 283 final, 31 May 2017

xviii. European Commission/European Urban Mobility: Policy Context. 2017

xix. Final Report Summary - ROBOLAW (Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics), CORDIS, 2015

Member States of the EU

xx. Guidance, (UK) The key principles of vehicle cyber security for connected and automated vehicles. Published 6 August 2017

xxi. UK: Automated and Electric Vehicles Bill 2017-19, dealing notably with the issue of insurance for automated vehicles, House of Commons Library, 2017

xxii. Directive on security of network and information systems 2016 –, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf UK version

xxiii. DE: Achtes Gesetz zur Anderung des Straßenverkehrsgesetzes vom 16. Juni 2017. Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 38, ausgegaben zu Bonn am 20. Juni 2017

OECD – International Transport Forum

xxiv. Automation of the Driving Task: Some possible consequences and governance challenges 20 July 2017

xxv. Human Factors, User Requirements, and User Acceptance of Ride-Sharing in Automated Vehicles 20 July, 2017.