Regulating Innovation of Autonomous Vehicles: Improving Liability & Privacy in Europe

Innovatieregulering van autonome voertuigen: het verbeteren van aansprakelijkheid en privacy in Europa

(met een samenvatting in het Nederlands)

Proefschrift

ter verkrijging van de graad van doctor aan de
Universiteit Utrecht
op gezag van de
rector magnificus, prof.dr. H.R.B.M. Kummeling,
ingevolge het besluit van het college voor promoties
in het openbaar te verdedigen op

vrijdag 8 april 2022 des middags te 12.15 uur

door

Roeland Wieger de Bruin

geboren op 4 maart 1984
te 's-Gravenhage

Promotoren:

Prof. dr. I. Giesen
Prof. dr. M. de Cock Buning
Prof. dr. E.R. de Jong

REGULATING INNOVATION OF AUTONOMOUS VEHICLES: IMPROVING LIABILITY & PRIVACY IN EUROPE.

Roeland Wieger de Bruin.

https://doi.org/10.33540/1078

CONTENTS

PART ONE – IDENTIFYING *FACTORS* FOR ASSESSING RELATIONSHIPS BETWEEN REGULATION AND INNOVATION

Chapter 1. INTRODUCTION

1.1 GENERAL INTRODUCTION & RESEARCH QUESTIONS

1.1.1 AUTONOMOUS INTELLIGENCE

Autonomous intelligent technology has the potential to shift traditional, human, decision making towards algorithm-based decision making by humanly created systems on a large scale in the coming years. *Autonomous intelligence* (AI)[1] forms a spectrum in which human intelligence becomes decreasingly necessary as a basis for decisions. Technological innovations endowed with AI can for instance be used to execute "dirty, dangerous and dull"[2] tasks, in order to minimise hazardous or degrading labour for human workers. AI can also be used in jobs requiring high levels of precision and delicacy.

Examples displaying actual forms of emerging AI include profiling algorithms of social networks such as Facebook, showing personalised news-feeds and advertisements, based on earlier 'likes' and contributions of the users' connections; Apple's maps-app recognising where one has parked his or her car, and how long it will take to reach one's probable next destination; and IBM's supercomputer Watson, who has won knowledge quiz show Jeopardy. Many predictions are made of the routes that these developments might take, varying from autonomous warfare (with or without human casualties);[3] to autonomous robotic surgery;[4] to autonomous intelligence judging court cases;[5] and to completely unmanned systems for the transportation of people and goods – including the object of this research: autonomous vehicles.[6]

1.1.2 POTENTIAL INFLUENCE OF AI ON LIABILITY AND PRIVACY REGULATION

AI has potential to impact the legal order in an unprecedented way. Regulation, enforcement and the administration of justice have always dealt with *human* decisions and the consequent behaviour, and did not anticipate decisions originating from a system. A prominent question is:

---

[1] Autonomous intelligence and artificial intelligence are related terms, which is elaborated in Chapter 2. Artificial intelligence is used in autonomous intelligent technology, however the latter is broader; see section 2.2.
[2] See for example Takayama, Ju & Nass 2008.
[3] Williams & Scharre (eds.) 2015, p. 4; also Scharre 2018.
[4] See Strickland 2016.
[5] See e.g. for example Bhorat 2017.
[6] See for an overview of actual developments: http://www.futureforall.org/transportation/future_of_transportation.htm (last accessed 25 August 2021).

who must account for these new types of decisions and potential damage as a consequence thereof?

> At some point in the future, autonomous vehicles will be able to drive from A to B without a human driver: passengers will eventually no longer be in the position to make any alterations to the driving task that is carried out by the system once it has commenced.[7] AI-systems in cars will be equipped to 'learn'. Operating software that these systems are endowed with, is 'fed' with their own experiences and possibly that of their peers on the road over time. Should however something go completely wrong in the autonomous-driving process, resulting for instance in a car to accelerate rather than to brake when approaching a red traffic light, this will likely have serious consequences – and immediately raise the question who can be held accountable and liable.

Accidents as a result of autonomous decisions with a comparable origin to what is described above, will lead to the question who bears the responsibility for an AI-decision and subsequently to the question who is liable and thus, who is to remunerate damages. In many cases, under current regulation – as is further elaborated in Chapter 4 – it will be necessary to establish where the cause lies of the harmful result of the learning process by a respective car, and to what extent this can be attributed to actors, such as (a multitude of) manufacturers, software-developers, or 'third parties' who were not involved in the production- or vehicle-operation processes. Such assessments will likely consume much time, effort and money, which will increase as technology gets increasingly autonomous, and may even show that it is impossible to pinpoint *precise* causes, as the learning skills of AI comprise of many different although interrelated pieces of hardware and software, of many different origins.

> The Product Liability Directive for instance entails that proving a *defect* in a product, and a *causal relationship* between a defect in a self-driving car and the origination of damage is necessary to establish product liability for manufacturers, and calculating the damages to be remunerated. These principles also apply to most (non-harmonized) national regimes regulating liability of actors involved in motor-vehicle related accidents, although the applicable regimes in Europe show significant variations. To unearth the respective root-causes of self-driving car related damage, in-depth analysis of the underlying hardware, software and data will be necessary.

[7] See below for an overview of different (expected) stages of autonomy, and the table of the SAE, which has been included and elaborated in section 2.3.

Some have even suggest that holding the respective AI-systems liable themselves, would save considerable amounts of these efforts. It is argued that AI must be seen as new, independent actors in the legal order, which pleas for the creation of a legal personhood for AI.[8] Besides matters of feasibility and desirability of that approach, significant changes would be needed in the currently applicable legal systems throughout the world in order to facilitate such new forms of legal personhood. Alternatives for the approach of creating legal personhood for AI, such as introducing or extending no-fault liability systems, and/or no-fault insurance models,[9] may also require changes in currently applicable regulatory regimes.

> Alongside – or instead of – changing laws as an answer to the questions how to establish liability in self-driving-accident cases, technology itself may also play a pivotal role, for example by equipping cars with Accident Prevention and Registration Systems (APRS, see section 2.3). Data recorded in an APRS can be used to help establishing where accident-causes could lie, and to whom liability may be attributed.

The introduction into society of AI-technology can also strongly impact rights and fundamental freedoms of citizens such as the right of privacy, especially when deployment of AI concerns big-data processing and profiling. Focussing again on autonomous vehicles, the deployment thereof will generate huge amounts of data. These data could for instance consist of information regarding the position of vehicles over time; the passengers of these vehicles and their behaviour – not unlikely including camera footage and bank-account details of the passengers; the (technical) characteristics of respective rides; the audio(visual) preferences of the passengers, et cetera. Many of these data qualify as personal data in sense of the applicable privacy-regulation including the EU General Data Protection Regulation (GDPR),[10] as these data can be traced back to natural persons.[11] Such data can *inter alia* be used for technical purposes: based on the mileage and driving characteristics, maintenance can be scheduled, and driving characteristics can be adjusted to the preferences of the respective passengers. In a less optimistic scenario, these data can also be used to help establishing causes when it came to accidents in which vehicles become involved.

---

[8] See European Parliament 2017, p. 18, cons. f), in which it had been suggested that the possibility must be explored to create a "specific legal status for robots, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons with specific rights and obligations, including that of making good any damage they may cause, and applying electronic personality to cases where robots make smart autonomous decisions or otherwise interact with third parties independently". See also Bertolini 2021. In more recent communications of the European Parliament (see for instance European Parliament 2020 and 2020a), legal personhood for AI is no longer considered.

[9] These concepts will be further elaborated in Chapter 8. See also Engelhard & De Bruin 2018, p. 77-92.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), *Official Journal L 119, 4.5.2016*.

[11] See 0 on personal data protection regulation.

Besides technical uses, vehicle data may as well serve commercial purposes. With these data, profiles can be built and advertisements can be tailor-made and directly targeted to the respective users.

The informational privacy of car-users may be at risk when their personal data are to be shared and used without necessary guarantees and constraints. These risks could for example include identity theft,[12] publication of information that was intended to be kept confidential and unintended secondary uses of personal data.[13] Although one of the goals of the GDPR is to ensure a high level of informational privacy of citizens, the question has already been put forward whether or not that goal is likely going to be achieved.[14] Despite the regulated measures to the contrary, high-tech developments such as in AI will be easily non-compliant with the GDPR requirements. Some of the reasons for that include: that data processing may deviate from the original goals and purposes as a result of the self-learning capacities of AI-endowed systems; that (big) data processing chains will likely consist of many actors based in many different countries; that all links in the chain can be vulnerable to *inter alia* hacking and other forms of abuse; that compliance will be costly and difficult and sometimes uncertain since there are many open norms in the GDPR; and that in practice, consumers are not likely to exercise their powers and rights the GDPR has equipped them with. Therefore, the question could be raised whether or not the actual regulatory framework on the protection of personal data would be fit do deal with the outcomes of current and forthcoming developments in AI-technology.

1.1.3 POTENTIAL INFLUENCE OF PRIVACY AND LIABILITY REGULATION ON DEVELOPMENT AND DEPLOYMENT OF AI

The regulatory frameworks mentioned above, could at the same time influence the ways AI will develop and will be deployed in society. Some argue that for example the regulatory framework that applies to matters of establishing and determining the scope and amounts of liability,[15] hinders innovation in the field of AI, when developers can be easily held responsible and liable for damage resulting from the developed AI-technology.[16] While a certain relationship between liability risks for developers and innovation is mentioned in literature, the aforementioned statement is too bold, which is elaborated in Chapter 3. Conversely, it can also be argued that when

[12] See Dimmroth & Schünemann 2017, p. 109.
[13] See R.L. Finn e.a. 2013, p. 6.
[14] See Koops 2014, and section 7.4.
[15] Hereinafter referred to as *(extra-contractual) liability regulation*; see further Chapter 4.
[16] See for example Robolaw 2014, p. 57; Blind 2012a, p. 394-395.

liability risks (were to) be attributed to users of AI-technology, rather than to developers, this could form a disincentive for the adoption thereof.[17]

Some of the liability-related issues might be partly mitigated by AV-technology itself. Accident Prevention and Registration Systems (APRS), including for instance event data recorders (black boxes), or vehicle-to-vehicle and vehicle-to-infrastructure communication may *inter alia* assist in establishing the cause of accidents, and can thus help resolving uncertainty in liability-related questions. However, APRS technology that is set to record any event in the car during its operation, and to make for instance camera-footage of the passengers, which data are simultaneously streamed to other road-users or stored for unlimited periods in cloud-servers for possible later analysis purposes could negatively impact the privacy of its users. In order to protect the privacy of EU-citizens, European rules on personal data protection, hereinafter referred to as *personal data protection regulation,* [18] stipulate strict rules for personal data processing through APRS.[19] The GDPR leaves many open norms, for instance on what precisely constitute appropriate levels of security measures to be taken, or material requirements on rightful intra-continental data processing. Making APRS- and comparable "tracing" technology comply with these rules, and accordingly adjusting practices of processing (personal) data within and across the borders of the European Economic Area, will take considerable effort. In turn, this may prove a high and expensive burden for innovators which may at the same time slow down the investments in - and therefore the pace of - technological developments.[20] Failing to comply with the regulated provisions can result in liability towards the data subjects, and hefty fines – up to €20 million, or 4% of the annual worldwide turnover.[21] Should however the compliance-bars be lowered, and should personal data be processed with less – expensive – adequate protection measures, this may have negative consequences for the privacy protection of citizens. Less protection measures could for instance lead to easy hacking or otherwise compromising these

[17] See for example Hirunyawipada & Paswan 2006, p. 188; Hosseini et al. 2016, p. 501; and furthermore section 3.4.

[18] Which is in this research taken to comprise of the written and unwritten rules stemming from both state- and non-state actors and applicable case law regarding the protection of personal data, which is further elaborated in 0. Rules on informational privacy, or personal data protection, have been laid down in directives and regulations, including the 1995 Data Protection Directive (DPD), which is succeeded and replaced by the General Data Protection Regulation of 2016 (GDPR). These instruments are derived from the broadly formulated fundamental right to 'privacy', as incorporated in article 7 an 8 of the Charter of Fundamental Rights of the European Union.

[19] See 0.

[20] When companies have to spend more resources in (privacy) compliance, they would have left less for innovation. See for a further elaboration on this topic section 3.4, 0 and Chapter 7; and for a recent report on compliance costs (which lists privacy regulation in its top 5) by Thomson Reuters: English & Hammond 2018, p. 5, 16.

[21] Liability towards those whose rights have not been obeyed and have suffered damage as a result thereof, is stipulated in article 82 of the EU General Data Protection Regulation (GDPR). The height of possible fines are regulated in article 83 GDPR.

data. Privacy protection – or the lack thereof – can be seen to be of influence to the trust in,[22] and adoption of new technology by consumers.[23] Apart from the considerable compliance efforts and costs and related fine- and liability risks for innovators, a positive outcome of safeguarding information privacy by innovators, may be that consumers' trust in this new technology increases. This could in turn have a positive impact on diffusion of innovation and the adoption thereof.[24]

In order to further highlight the questions regarding the potential influences of regulation on innovation, I will illustrate the contours of one specific form of emerging AI-technology as incorporated in *autonomous vehicles*, hereinafter: AVs, which form the objects of this study.

1.1.4 AUTONOMOUS VEHICLES

Innovations in the automotive industry are heading towards a 'driverless' future. Fully autonomous vehicles are however not yet available, and it is predicted that it will take at least some years if not decades before AVs will be commonplace on European roads. The incorporation of autonomous intelligence in cars can be observed as a spectrum. Starting from 'driver only', the next steps towards 'full autonomy', a stage in which drivers eventually become redundant, may be 'assisted driving', 'partial autonomy' and 'high autonomy'.[25]

AV-technology is promising in terms of road safety: AVs could significantly reduce the risks of car accidents, as in 93% - 95% of the traffic accidents human failure is involved, currently leading to 1.3 million deaths and 50 million serious injuries worldwide per year.[26] Besides contributing to road safety, AV-technology can lead to more efficient use of the road network, may contribute to the reduction of CO2 emissions and can assist in improving the mobility of disabled people.[27] However, not everyone is optimistic about a driverless future. It is stated that, while AVs will be beneficial to inter alia road safety, environmental and congestion problems, other risks and challenges will follow from the introduction of autonomous vehicles. As shortly introduced above, especially in the transit-period between 'partial autonomy' and 'full autonomy', when AVs remain to co-exist with non-autonomous traffic participants, there is the risk of accidents – and *inter alia* liability questions as a result. Widespread use of AVs also entails privacy risks for the users, as AVs will be generating and processing many personal data. These vehicles will be connected to the internet and to each other, implicating risks that personal data get hacked into, compromised

[22] See for example Carter & Belanger 2005, p. 9, 18-19.
[23] See for example Fagnant & Kockelman 2015, p. 178, and section 3.4.
[24] See Fagnant & Kockelman 2015, p. 178; Carter & Belanger 2005, p. 9, 18-19 and section 3.4.
[25] See SAE J3016_202104 , distinguishing six levels of automation. See more elaborately section 2.3.
[26] See Walker Smith 2013 and OECD 2013.
[27] See Wadud, MacKenzie & Leiby 2016.

or otherwise used contrary to the purposes for which these data were originally obtained.[28] These, and other issues are now appearing on regulatory agendas, since the shortly introduced phenomena are 'new' to existing legislation.[29] Regulators will be challenged to formulate durable, interoperable and transnational solutions to these AV-induced problems.

1.1.5 RESEARCH QUESTION

The hypothesis that formed the starting point of this research, is that the currently applicable regulatory frameworks on extra-contractual liability and informational privacy, can influence innovation in the field of Autonomous Vehicles, and that these frameworks do not, in their current forms, provide for optimal conditions for innovation and acceptance. In their Robolaw-study, Palmerini et al. for instance observe a "heightened liability risk […] and the prospect of damage to the reputation" of AV-manufacturers, which could cause a too long delay of the market introduction of AVs in Europe.[30] Considering the liability system(s) in the USA, Marchant & Lindor make a similar statement as Palmerini et al. They argue that it is likely that in the initial stages of AV-development there will likely be "a significant rate of failure", for which manufacturers may be held liable, and that such "liability may be a barrier that blocks the introduction of this socially beneficial new technology".[31]

I found further indications regarding this hypothesis in regulatory steps that were prepared in recent years on a European level. The 2017 report for the European Commission on *Civil Law Rules on Robotics*,[32] recommended for instance to address robotics technology on a more general level. In that report, it was *inter alia* argued that the traditional extra-contractual liability rules are not adequate in terms of compensating victims, and would need to be reformed.[33] Since then, the European regulators proposed several concrete regulatory steps, of which to date the Proposed AI-regulation (by the European Commission)[34] and the European Parliament's Proposal

[28] Besides these issues, it must be noted that AVs might have be endowed with a framework to make ethical decisions on the road. When for instance an accident is unavoidable, AV technology may have to make the decision to either crash itself and its passenger into an inevitable road-blocking obstacle, or to dodge it and overrun for example a women pushing a pram. Such decisions can and must be for a large part be pre-programmed, or when not pre-programmed, instantly decided, based on a standard ethical framework, which does not exist to date.
[29] See for example Engelhard & De Bruin 2018; Robolaw 2014, p. 57; De Bruin 2016, p. 386; Green Paper 2012; European Parliament 2017, p. 12, and the recently proposed AI-regulation by the European Commission (European Commission 2021a, Proposed AIR); and the EP-proposal regarding a Civil liability regime for artificial intelligence (European Parliament 2020a, Proposed CLAI), as evidence of some first steps taken into this direction by the European regulator.
[30] Robolaw 2014, p. 59.
[31] Marchant & Lindor 2012, p. 1339 – 1440.
[32] See European Commission 2017.
[33] European Commission 2017, cons. AF.
[34] See European Commission 2021a; see further section 2.2 and section 3.2 ff.

on Civil Law Rules for Artificial Intelligence,[35] form the most relevant examples in terms of this study.[36] Not only liability rules would have to be altered, also privacy rules need revision,

> "whereas […] the General Data Protection Regulation […] sets out a legal framework to protect personal data; whereas further aspects of data access and the protection of personal data and privacy might still need to be addressed, given that privacy concerns might still arise from applications and appliances communicating with each other and with databases without human intervention".[37]

Relationships between liability and privacy regulation and innovation are also sketched in the Robolaw 2014 report. Palemerini et al. for instance illustrate that "there is a potential clash between the goal of ensuring fulfilment of responsibility and the notion that personal data ought to be kept private".[38] I have explored such interplays, if not trade-offs, between liability and privacy in relation to innovation in 2016. One of my findings was, that in order to mitigate liability risks, manufacturers might take measures that infringe on the right to personal data protection of consumers. In order to be allowed to take these measures, rather high compliance-bars must be met by manufacturers, which in itself might negatively implicate innovation.[39]

The aforementioned contributions in the literature, and the examples given in section 1.1.1 of damage that results from an accident involving Autonomous Vehicles, thus indicate a certain relationship between liability- and privacy-regulation: rules on (product) liability entail that it is often necessary to assess the precise causes of AV-accidents, requiring many (personal) data to be logged and analysed, which in turn has implications for the privacy of citizens that is safeguarded through personal data protection regulation. Failing to comply with rules on personal data protection could furthermore lead to liability of the respective non-compliers.

The observations above also imply that regulations may influence innovation and adoption of AV-technology. Against the backdrop of EU-policies to stimulate innovation and adoption thereof by citizens, I will investigate whether or not *factors* can be identified in European regulatory frameworks on extra-contractual liability and the protection of personal data, which may influence innovation and the consumer acceptance of Autonomous Vehicles, on a more substantial

[35] See European Parliament 2020a; further section 4.4.
[36] That is: to date, i.e. September 2021.
[37] European Parliament 2020a, cons. O.
[38] Robolaw 2014, p. 89, where they refer to Böhle, K., Coenen Chr., Decker M., & Rader M., "Biocybernetic adaptation and privacy", *Innovation: The European Journal of Social Science Research* 2013, 26 (1-2), pp. 1-10.
[39] De Bruin 2016, p. 499.

level. Such *factors* can be used to help establishing the current influences of regulation on innovation, and – where possible – to improve these.

Given the above, the central research question reads:

Which factors in regulation may influence innovation in the field of autonomous vehicles in the EU, how do the regulatory frameworks on extra-contractual liability and personal data protection encompass these factors, and how could these factors in the regulatory frameworks be optimized in order to improve the conditions for innovation and acceptance by citizens of AV-technology?

To answer this research question, it is relevant to conduct a study of the potential influence of extra-contractual liability and informational privacy regulation, viewed both in their own respects and in each other's contexts, on innovation in the field of autonomous vehicles. This relevance can be viewed from a material, legal academic perspective (looking at the contents of the respective regulatory frameworks), as well as in the light of overarching EU-policy on better regulation, [40] which aims at increasing the European Union as an innovation-friendly environment.[41] Concerning the material norms on informational privacy and extra-contractual liability regulation, it is worthwhile to evaluate the potential influences thereof on AV-innovation, including its acceptance by citizens, and to see whether or not more innovation-friendliness could be achieved, if necessary, without detriment to the underlying core values of the respective regulatory frameworks as much as possible. Should the outcome of the evaluation be that there would be room for optimisation, it is relevant to assess how that could be done from a regulatory perspective.

[40] See for example European Commission 2016.
[41] See for example: from http://ec.europa.eu/research/innovation-union/index_en.cfm (last accessed 23 February 2018); State of the Innovation Union 2014; European Innovation Scoreboard 2016.

1.2 RESEARCH GOAL, PLAN AND METHODS

1.2.1 INTRODUCTION

The goal of this research is to provide recommendations to improve the respective frameworks to better facilitate innovation and acceptance of AVs in Europe, by answering the research question stated above. This research consists of three elements. In the first place, I will investigate whether or not a set of factors can be identified from existing literature, that can be used to map the possible influences of regulatory frameworks on innovation and acceptance thereof. My hypothesis is that such factors can be identified, which is shortly explained in section 1.2.2 hereunder. Secondly, I will evaluate possible influences of the current regulatory frameworks on extra-contractual liability and personal data protection that are applicable in the European Union, on innovation in the field of Autonomous Vehicles, using the factors identified in the first part. To the extent that the outcomes of the evaluation indicate that there is room for improvement of the studied regulatory frameworks with regard to innovation, the third part provides recommendations to improve the respective frameworks to better facilitate innovation and acceptance of AVs in Europe.[42]

1.2.2 FIRST ELEMENT: IDENTIFYING FACTORS

1.2.2.1 Goal

The first goal is to investigate whether or not a set of factors can be identified in academic literature that can be used to assess the possible influences of regulation on innovation and consumer acceptance thereof in general (which is done in Chapter 3), which in turn can be applied to the frameworks on extra-contractual liability and informational privacy (which is done in Chapter 6). Whereas the terminology is further elaborated in Chapter 2, I introduce here that the concept of *innovation* incorporates two components that I have identified from the literature, which are relevant in the context of this research. Firstly, innovation can be seen as the capacity, opportunity and willingness of organisations to innovate, [43] which I understand as the development and market introduction of new products or services, which will hereinafter be referred to as the *innovators perspective*. Secondly, I also identify a *consumers perspective*: in order to be successful, innovation requires acceptance of the newly developed products or services by consumers which is necessary for the adoption of such products or services.

1.2.2.2 Plan and methods

Regarding the *innovators perspective*, there is a rather large body of academic literature stemming from economic disciplines, on the effects of regulation on innovation. In their 2014 research

[42] This study was executed between 2016 and 1 September 2021, which is the closing date of my studies.
[43] Pelkmans & Renda 2014, p. 5.

report titled "Does EU regulation hinder or stimulate innovation", Pelkmans & Renda assessed in a qualitative way, relevant contributions in (international) economic empirical literature, mostly based on quantitative analyses, and literature on regulation (and innovation) from a regulatory and policy-making perspective. As a second important source in the first part, I will use the dissertation of Sofia Ranchordás: "Sunset clauses and experimental legislation: Blessing or curse for innovation", which has been published in 2014.[44] I will take these sources and the conceptual frameworks developed therein as a point of departure in the first part of this research. Both approaches will be compared with each other and, based on that comparison, I then seek to identify an overarching set of factors that are relevant for this research to review the potential influences of extra-contractual liability and informational privacy regulation on innovation, from an *innovators perspective*.

In order to study the *consumers perspective*, I will use theoretical concepts that have been developed in social and economic sciences literature as starting point for my research. These include *inter alia* the 'Diffusion of Innovation-model by Rogers,[45] including the 'Perceived Risk' model coined by Ostlund,[46] and the theory on 'Trustworthiness' which has been studied by Carter & Bélanger.[47] From these sources, I endeavour to distil factors that can be tested from a legal academic perspective, as there seems to be no widely available body of literature yet which bridges the gap between the said social- and economic literature, and legal and regulatory theory.

1.2.3 SECOND ELEMENT: ASSESSING THE FACTORS IN THE REGULATORY FRAMEWORKS

1.2.3.1 Goal

The second goal is to assess to what extent the regulatory frameworks on 1) extra-contractual liability (Chapter 4) and 2) personal data protection (0) that are applicable in the European Union, may influence innovation in the field of Autonomous Vehicles in the EU, according to the factors that have been identified in the first part. Also here, innovation is to viewed from both the *innovators perspective* and the *consumers perspective*.

1.2.3.2 Plan and methods

Both regulatory frameworks will be evaluated: the existence of each innovation-influencing factor described in Chapter 3 is assessed in the second part of the research. That is done through one main case study per regulatory framework (extra-contractual liability and personal data protection), and per perspective (innovators and consumers). Where the nature of the respective

[44] Ranchordás 2014. Published also as follows: S. Ranchordas, *Constitutional Sunsets and Experimental Legislation*, Cheltenham: Edward Elgar Publishing 2014.
[45] Rogers 2003.
[46] Ostlund 1974, described *inter alia* in Hosseini et al. 2016, p. 499 – 500.
[47] Carter & Bélanger 2005, p. 9-10.

parts of the regulatory frameworks or the respective factor(s) require so, this main case study may be slightly adjusted. The main case study is further introduced and explained in section 3.5.

The answers to the legal questions formulated in the case study, are used to evaluate the possible relationships between the studied rules and innovation. This will be done per factor, and per perspective. The factors, and the perspectives as well, are also cross-examined: I will try to illustrate how factors can interrelate. When for instance factor A can be considered innovation-enhancing and factor B could encompass a hurdle, it is relevant to assess the possible 'net results'. Furthermore, I address relationships among factors among the *innovators perspective* and the *consumers perspective*, in order to make assumptions on possible (im)balances between these two. The question is addressed whether or not positive factors from an *innovators perspective* entail negative factors from a *consumers perspective* and vice versa. Would it, in other words, be true that shaping better conditions for innovators automatically leads to worse conditions for consumers, or would it be possible to create an equilibrium between these two, which could benefit innovation in general?

1.2.3.3 Reviewed regulatory frameworks: extra-contractual liability

As it is impossible to assess all respective components of the applicable regulatory frameworks, within the boundaries of this research, some choices had to be made regarding the scope of this study, [48] which include the following. With regard to the regulatory framework on extra-contractual liability, I chose to study the 1985 EU Product Liability Directive (hereinafter referred to as: PLD),[49] and relevant case law of the Court of Justice of the European Union. Where necessary (for example where the PLD provides minimum harmonization, or leaves other norms to be filled in by the Member States), I will primarily look into the respective implementations in The Netherlands, France and England (and Wales),[50] and corresponding case law. These jurisdictions are not arbitrarily chosen – as I will explain below.

Choices also had to be made on the second tier of the extra-contractual liability framework: liability for accidents in which motor vehicles are involved. Despite some attempts of the EU

[48] This is further explicated in Chapter 4.
[49] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *OJ* L 210, 7.8.1985, p. 29–33
[50] In 2016, when this research started, there was no concrete indication that Brexit would eventually take place. Therefore, I included England as a part of my research into (implemented) EU regulation. As to date the respective rules have not significantly changed (yet), there is still relevance to include the respective English regulatory frameworks in this study.

regulator, the material norms remain national law to date. Also here, I chose to review the applicable rules and case law in The Netherlands, England (now ex-EU-member), and France.

The primary reason for choosing to review the applicable extra-contractual liability rules of England vis-à-vis The Netherlands and France, is of a systematic nature: it is relevant to take a closer look into both a common-law system and civil-law systems (of the Netherlands and France). This relevance shows *inter alia* in the different approaches between the rules to determine liability in case of traffic accidents. Whilst in France, the *Loi Badinter,*[51] introduced a strict no-fault liability for keepers of motor vehicles towards other traffic members, to which very limited exceptions might apply,[52] liability questions in England are (regarding AVs: until recently, were)[53] to be determined by assessing who was at fault.[54] The systematics of the *Wegenverkeerswet,*[55] and corresponding case law of the Netherlands are positioned somewhat in between the applicable rules in the UK and France: at least 50% of the damages of a non-motorized victim have (when force majeure cannot be proved, and there was no intent or gross negligence at the side of the victim) to be compensated by the owner or the keeper of a motorized vehicle, whilst for the other 50% *inter alia* the 'own fault' of the victim plays a role.[56] When, however, the victim was younger than 14 years of age, 100% of the damages have to be remunerated in principle.

1.2.3.4 Reviewed regulatory frameworks: personal data protection

With the introduction of the GDPR, most of the differences between the EU Member States, which resulted from its predecessor the Data Protection Directive have been eliminated. Therefore, the primary focus in the review of the regulatory framework on personal data protection will be on the GDPR, rather than on the (former) implementations within the Member States. Where there still exists 'margin of interpretation' for national regulators, and insofar as no "European" answers are provided by for instance the European Data Protection Board, of the Court of Justice of the European Union, I will primarily review these margins within the jurisdictions of The Netherlands, France and England – where available and relevant for answering the research questions, if only for the sake of consistency with the review of the extra-contractual liability framework. I will occasionally include other jurisdictions where opportune, and highlight some of the effects, or

[51] Loi de 5. Julliet 1985 "tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation."
[52] See section 4.3.3, and Engelhard & De Bruin 2018, p. 36-37.
[53] As the Automated and Electric Vehicles Act (AEVA) 2018 entered into force in April 2021. See sections 4.2.5.7 and 4.3.4.4.
[54] See on the new *Automated and Electric Vehicles Act*, (which entered into force on 21 April 2021 https://www.legislation.gov.uk/uksi/2021/396/regulation/3/made) is discussed further in section 4.3.4.4.
[55] Wegenverkeerswet 1994 (Road Traffic Act).
[56] See also section 4.3.2.

results of these jurisdictions, although without elaborating the entire framework(s), in order to illustrate for example the underlying argumentations.[57] That may for instance be the case when self- or co-regulation initiatives – which are actively stimulated by the GDPR – have been taken outside the jurisdictions of the countries under primary review. In that sense, I foresee to include the German initiative on "Data Protection Principles for Connected Vehicles" of the Verband der Automobilindustrie,[58] and the initiative of the European Automobile Manufacturers Association: "ACEA Principles of Data Protection in Relation to Connected Vehicles and Services".[59]

1.2.4 THIRD ELEMENT: RECOMMENDATIONS FOR IMPROVING THE FACTORS

1.2.4.1 Goal

To the extent that the outcomes of the second part indicate that there is at some points room for improvement (Chapter 7), the third and ultimate goal is to formulate durable recommendations in order to create better conditions for innovation (regarding both the *innovators*- and the *consumers* aspects) in view of the ambitions of the European Union on better regulation of innovative technology (Chapter 8 & Chapter 9). Again, both the regulatory framework on extra-contractual liability and on personal data protection will be addressed, also viewed in relation to each other. I will investigate the options to improve conditions within the regulatory frameworks themselves, i.e. how the respective *substance* (the rules) could be improved, as well as the *regulatory methods* (including self- and co-regulation) that would be most suitable.

1.2.4.2 Plan and methods

The recommendations will take two aspects into account. Firstly, suggestions are made relating to the improvement of the *substance* of the regulatory frameworks. The analysis resulting from the second part will be used as 'input' here. It will be borne in mind that these material suggestions need to be as independent as possible from the actual or predicted forms of AV-technology, in order to be 'fit' for the future.[60] In order to do so, I will try to abstract from the forms and specifications of the respective future technology, and relate to the functions thereof in view of the *factors*. Also, I will refer where possible to the fundamental principles underlying the studied regulatory frameworks. These include, *inter alia*,[61] the democratic right to privacy of citizens, the

[57] This concept of 'argumentative legal comparison' (argumentatieve rechtsvergelijking) has been developed in Giesen 2005, p. 18-19.
[58] See for the most recent version: https://www.vda.de/dam/vda/Medien/EN/Themen/Innovation-und-Technik/Vernetzung/Datenschutz-Prinzipien/vda-data-protection-principles.pdf.
[59] See for the most recent version: https://www.acea.be/uploads/publications/ACEA_Principles_of_Data_Protection.pdf.
[60] See also Chapter 3.4.2.2.2 and De Cock Buning 1998 on 'technology neutrality' and the importance thereof for sustainable regulation.
[61] See section 4.1.2 (extra-contractual liability), and sections 5.1.2, 5.1.3 (privacy and personal data protection.

right to receive fair compensation of damage suffered by victims and the – corresponding – duty to prevent damage, and if it damage nevertheless occurred: to remunerate damages caused by tortfeasors. Secondly, suggestions are made relating to the *forms and ways* of regulating.

1.3 CONCLUSION

In this first Chapter, a brief overview was given of the technological developments that can be expected in the field of autonomous vehicles. It was introduced that the current regulatory frameworks on extra-contractual liability and personal data protection may contain elements, or *factors*, that could influence the course of innovation, and the acceptance thereof by consumers. The central research question revolves around the relationship between these factors and innovation, and ultimately seeks to provide answers to the question how these factors could be optimized in order to make the regulatory frameworks on extra-contractual liability and personal data protection better, in terms of stimulating innovation and the societal acceptance of the results thereof. The answers are sought in the next chapters.

An elaboration of technological concepts including *autonomous intelligence* and *autonomous vehicles* is provided in Chapter 2. Chapter 3 further introduces the theoretical concepts of *innovation* and *regulation*, and identifies the aforementioned *factors in regulation that may influence innovation*, which is done from two perspectives: a *consumers perspective* and an *innovators perspective*. In section 3.5, the case study is sketched that is used in the second part to illustrate the potential influences of regulation on innovation. The first part is concluded in section 3.6. In the second part, the *factors* are 'tested' on the two regulatory frameworks that form the central elements of this study, as far as necessary to indicate assess the *factors* therein. Chapter 4 introduces the extra-contractual liability framework, limited for the purposes of this study to *product liability* and *traffic liability*. In Chapter 5, an overview is given of the regulatory framework on *personal data protection*. In Chapter 6, it is analysed if, and to what extent, the studied regulatory frameworks contain the *factors* identified in Chapter 3. The second part is concluded in Chapter 7. The third part focusses on the potential room for improvement of the studied regulatory frameworks. Based on the findings in the first two parts, suggestions are made in Chapter 8 for making these frameworks more innovation-friendly. Chapter 9 illustrates three routes towards the regulatory embedding of the factor-improvements that are recommended in Chapter 8. To conclude, the Summary provides the answers to the research questions and provides an overview of the key findings.

Chapter 2. TECHNOLOGICAL CONCEPTS: AUTONOMOUS INTELLIGENCE AND AUTONOMOUS VEHICLES

2.1 INTRODUCTION

Autonomous Vehicles (AVs) form the object of this study. AVs can be distinguished from "traditional vehicles" in the sense that specific driving tasks can be performed without human intervention, which were traditionally performed by human operators. Vehicles that are equipped with properties enabling them to drive autonomously, to varying extents, present an example of systems that are increasingly equipped with technology that I indicate as "autonomous intelligence". This concept, which was introduced in section 1.1.1, will be further elaborated in section 2.2. Section 2.3 more specifically focusses on AVs (as introduced in section 1.1.4), and specifies the definitions that will be used in the rest of this study.

2.2 AUTONOMOUS INTELLIGENCE

In essence, computer processes operate conform the input-processing-output model.[62] Where for instance one requires the calculation of the rather concrete dilemma "1+1" and feeds this into a computer algorithm (i.e. the *input*), it will *process* this input, and (likely) return "2" as its *output*. In the past decades, technology has developed in such ways that increasingly abstract *inputs* can be processed through computer systems. Entering for instance the phrase "what will be the weather in Culemborg today" in my favourite search engine delivers the meaningful and usable *output* that it will be 24 degrees Celsius as a maximum, with a 0% chance of rain, where the humidity shall be 64%, with wind speeds of 11 km/h. Nowadays, it is not even always necessary to concretely "feed" the desired input into a computer process: just switching on my phone and swiping right provides me with the actual weather forecast, my upcoming appointments and travel-instructions on when to leave and how to drive in order to make my appointments in due time. On the basis of my agenda – which I keep on my phone – and my regular phone-use (i.e. *input*), my phone has guessed what I might want to know (i.e. *processing*), and provided me with the relevant information (*output*). Can this phone-behaviour, which abstracts from direct input by me as its operator, and puts out what I would likely want to know, be qualified as Autonomous Intelligence?

---

[62] See for instance Braunschweig, D. "Input-Process-Output Model", the Rebus Community, via https://press.rebus.community/programmingfundamentals/chapter/input-process-output-model/ (last accessed 11 August 2021), for an introduction. See also Wikipedia, "IPO Model", via https://en.wikipedia.org/wiki/IPO_model#cite_note-5 (accessed 11 August 2021); and Grady, J.O., *System Engineering Planning and Enterprise Identity*, Boca Raton: CRC Press 1995, p. 143-146.

The concept Autonomous Intelligence consists of two elements: *autonomy* and *intelligence*. Etymologically, the word *autonomy* is derived from ancient Greek. The two parts of the word "αύτόνομος" are αύτός, which translates as "self";[63] and νόμος, which translates (*inter alia*) as "law".[64] Taken together, "αύτόνομος" indicates "living under one's own laws, independent, of persons and states",[65] according to the Liddell-Scott-Jones Greek-English Lexicon. It is stated, that humans as well as systems (i.e. non-human entities) can be – to varying extents – autonomous. Further to the theories of Kant and Mill for instance – and put very shortly – people are autonomous in the sense that they have the capacity to be their own person, to make their own choices, and to live their life independently, i.e. according to the choices that fit them best, without external manipulative influences.[66] Human autonomy is a debated concept,[67] as is autonomy of systems.[68] However, for instance Chopra & White indicate that (artificially created) agents can be autonomous, in the sense that they act according to predefined goals, which they can achieve on the basis of their own decisions, as they can

> "autonomously decide how to carry out the task given [their] resources and features of the environment [… they …] can select among the various choices available […] along several dimensions of preference".[69]

Autonomy in machines, which is per definition *artificial*, i.e. created by humans,[70] can be viewed as a "spectrum", rather than as a binary concept.[71] As Chopra & White present it, this spectrum varies from systems containing a minimum amount of autonomy, such as internet browsers or word processors at the one end, to systems which operate "without intervention and can adaptively modify [themselves] in response to user and environmental inputs", such as learning systems with sensors,[72] at the other end. Rather than focussing on the techniques underlying

---

[63] The Online Liddell-Scott-Jones Greek-English Lexicon (LSJ), accessed on 6 August 2021, via http://stephanus.tlg.uci.edu.proxy.library.uu.nl/lsj/#eid=18328.
[64] LSJ, accessed on 6 August 2021, via http://stephanus.tlg.uci.edu.proxy.library.uu.nl/lsj/#eid=73326.
[65] LSJ, accessed on 6 August 2021, via http://stephanus.tlg.uci.edu.proxy.library.uu.nl/lsj/#eid=18252.
[66] See the Stanford Encyclopaedia of Philosophy, lemma "Autonomy in Moral and Political Philosophy", via https://plato.stanford.edu/entries/autonomy-moral/ (accessed 7 August 2021), published on 28 July 2003, revised on 29 June 2020.
[67] Ibidem.
[68] See for an overview of different definitions for instance , p. 29-35. Wiliams, A.P., "Defining Autonomy in Systems: Challenges and Solutions", in Williams, A.P., & Scharre, P.D., *Autonomous Systems – issues for Defence Policymakers*, Den Haag: NATO Communications and Information Agency, via https://bit.ly/3iq01wI (Accessed 6 August 2021); see also Bertolini 2020, p. 88;
[69] Chopra & White 2014, p. 9.
[70] In literature, AI is often referred to as *artificial intelligence*. As this does not necessarily indicate *autonomy*, which I consider to be relevant in this study (illustrated above), I prefer to include *autonomy* when referring to AI, which thus presupposes that this is *artificially* created.
[71] Chopra & White 2014, p. 9.
[72] Ibidem. The ends of the spectrum should however not be seen to resemble "weak" and "strong" AI in sense of the concepts coined by Searle in 1980, who holds that "strong" AI would resemble an actual

autonomy in machines and how they would resemble human autonomy (or not), the following observation can be made regarding the (outcomes of) modes of operation of autonomous systems. From a functional perspective, systems can be categorised as increasingly autonomous, when the necessity for human intervention in the system's behaviour decreases,[73] in order to achieve certain goals. Referring back to my "smart" phone, it can be noted its algorithms observed my behaviour and derived my preferences, and subsequently presented me with the information that may likely be relevant to me without my direct input. Therefore, the phone can be stated to have a certain level of *autonomy*. Cars form another example (which is further elaborated in the following section) of objects that are increasingly autonomous. For instance, a vehicle that needs less human intervention to drive itself from A to B, can be qualified as comprising a higher level of autonomy than a car that needs more human intervention to pursue the same route.

Autonomous systems furthermore characterise as *intelligent* – also to varying extents. Intelligence can be perceived as "the ability to adapt one's behaviour to fit new circumstances [which] encompasses […] the ability to learn, to reason, of problem solving, perception and language understanding".[74] Albeit it is very difficult to precisely determine when one can speak of "perception" and "language understanding" by a system, one can argue that systems can be observed – again from a functional perspective – to have certain "learning", "reasoning" and "problem solving" capacities, using for instance "language" in their processes.[75] *Machine learning* forms one of the core components of system's *intelligence*. This concept describes the ways in which systems are enabled to process *input*-data into more meaningful information (or even knowledge),[76] which can be achieved through for instance knowledge-based,[77] (and/)or data-

human mind (Searle, J., "Minds, brains and programs", *Behavioural and Brain Sciences* 1980, vol 3, p. 417-457 (specifically p. 419-420); and Flowers J.C., "Strong and Weak AI: Deweyan Considerations", contribution to the AAAI Spring Symposium 2019: *Towards Conscious AI*, via http://ceur-ws.org/Vol-2287/paper34.pdf (last accessed 9 August 2021).

[73] See De Cock Buning, Belder & De Bruin 2012, p. 198; Breemen & Wouters 2020, p. 71.

[74] Davies, C.R., "An Evolutionary Step in Intellectual Property Rights – Artificial Intelligence and Intellectual Property", *Computer Law & Cybersecurity Review* 2011, vol. 27, p. 603, who paraphrases Copeland, J., 2000, via the Turing Archive, as cited in De Cock Buning, Belder & De Bruin 2012, p. 198. See also Devillé, Sergeyssels & Middag 2021, p. 2. Their perception of "intelligence" is comparable to the definition above, although it compares more to human capabilities, as they define intelligence as "the ability/capacity of a machine to act purposefully, think rationally and deal effectively with its environment, like humans are ideally supposed to do" (p. 2).

[75] See also Chopra & White 2014, p. 9.

[76] See for the dichotomy data-information-knowledge-wisdom which is used in information sciences further Ackoff, R.L. "From Data to Wisdom", *Journal of Applied Systems*, 1989, no. 16, p. 3-9.

[77] In which human experts model their own expertise into rules that are to be used by a system, see Devillé, Sergeyssels & Middag, 2021, p. 4.

based,[78] learning methods.[79] Thus, machine learning enables a system to *process* input-data in such a way that more meaningful information (for instance in the forms of patterns or rules) forms the *output* of such a system. In turn, that information can for instance be used to solve problems which are presented to the intelligent system. The smartphone referred to above contains some *intelligence* as well: it's algorithms derived from my phone-use and appointments in my calendar (*input*) for instance that I would likely want to know when I should leave in order to be in time for my upcoming meetings (*processing*), and notifies me (*output*) when it is time to get in the car. A car in turn, may comprise *intelligence* when it has for instance "learned" what my driving preferences are, and how to drive me most efficiently and safely to my destination.

From a regulatory perspective, autonomous intelligent technology is relevant, as their deployment may have legal consequences.[80] Where, as relevant in this study, for instance machine learning (*input*) requires the analysis (*processing*) of large amounts of data, or when the activities of a deployed system are logged in a database (*output*), this can constitute "personal data processing" as regulated by the General Data Protection Regulation. [81] When autonomous intelligent algorithms are deployed in vehicles, and these vehicles nonetheless cause accidents, this could lead to damage compensation obligations under the applicable product-[82] and/or traffic liability frameworks.[83]

.Recently, European Union regulators acknowledged the relevance of autonomous intelligent technology. The European Commission and the European Parliament recommended *inter alia* a Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Proposed AIR),[84] and the European Parliament proposed to create a Civil Liability Regime for Artificial Intelligence (Proposed CLRAI).[85] In the Proposed AIR, AI systems[86] are defined as:

> "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content,

[78] In which the system seeks rules, patterns or other logic itself in large amounts of ("Big", see) data – thus without being "fed" with such logic by a human expert, see Devillé, Sergeyssels & Middag 2021, p. 4-5.
[79] Further distinctions can be made – but with limited relevance in terms of this study. See for instance on "supervised" versus "unsupervised" machine learning, and the use of neural networks and deep learning: Devillé, Sergeyssels and Middag 2021, p. 6-11.
[80] As introduced in section 1.1.2.
[81] See further 0.
[82] See further section 4.2.
[83] See further section 4.3.
[84] European Commission 2021a. See further section 3.2 ff.
[85] European Parliament 2020a. See further section 4.4.
[86] Note that with AI, the European Commission refers to *artificial intelligence*. See footnote 70, in which it is illustrated that in terms of this study, I prefer to refer to *autonomous intelligence* instead, which is more-encompassing, and includes artificiality.

predictions, recommendations or decisions influencing the environments they interact with".[87]

Annex I refers *inter alia* to what is described above as technology that sees to the creation of *intelligence*, including machine learning.[88] This definition contains similar elements as those indicated above: systems can be qualified as comprising AI, when they can create certain forms of output, including decisions, using some form of intelligence, within the boundaries of pre-set (human-defined) objectives. However, the definition does not relate to the diversity in the potential levels of autonomy that can be the result of the deployment of AI-systems as for instance Chopra & White do.

In their Proposed CLRAI, the European Parliament more explicitly addresses autonomy. AI-systems are defined as software (which may or may not be embedded in hardware) which displays simulated "intelligent behaviour".[89] This may consist of collecting, processing (analysing and interpreting) and outputting data, including data that a system collects from its environment itself – and by "taking action" with some degree of autonomy, in order to achieve "specific goals". Autonomy refers to the potential of a system to "interpreting certain input" on the basis of "pre-determined instructions", although *without* being limited to these instructions – within a certain pre-programmed framework, for pre-programmed goals.[90]

Based on the definitions in literature and the proposed regulations, and viewed from a functional perspective, I understand *autonomous intelligence* in the light of this study as humanly created systems which have the ability to perceive information from their environment as *input* and to *process* that information in such a way that it can be used to achieve pre-defined goals as *output*, whereas those systems are increasingly autonomous as less human intervention is necessary in order to achieve certain (increasingly abstract) goals.

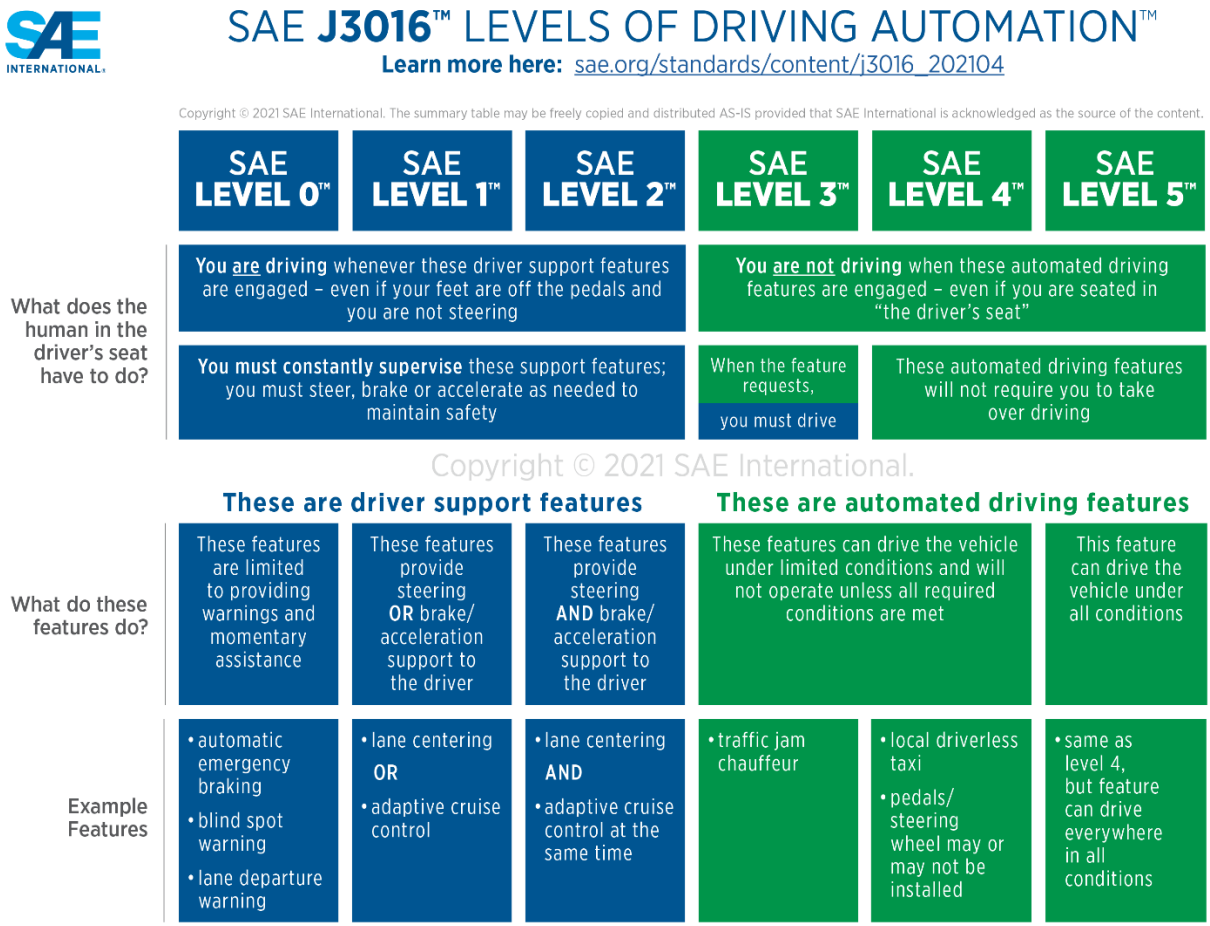
[87] Article 3(1) Proposed AIR.
[88] However, it contains much more than just *intelligence,* and encompasses also "logic- and knowledge-based approaches, including knowledge representation […] knowledge bases […] statistical approaches, Bayesian estimation, search and optimization methods" (Annex, subs b-c). Therefore, the definition in the Proposed AIR is criticized to be over-encompassing – see for instance Dufour, R., Koehof, J., Van der Linden, T & Smits, J., "AI or more? A risk-based approach to a technology based society", *IT&R* 10 August 2021, via https://www.itenrecht.nl/artikelen/ai-or-more-a-risk-based-approach-to-a-technology-based-society (last accessed on 11 August 2021).
[89] European Parliament 2020a, Article 3(a).
[90] Ibidem, article 3(b).

2.3 AUTONOMOUS VEHICLES

Road vehicles will be equipped with technology enabling them to (partially) drive themselves, with, as technology develops, decreasing needs for human interception in completing a driving task. Machine learning plays an important role in the development of this technology,[91] and regards for instance the identification of objects on the road,[92] and to adapt driving behaviour accordingly.[93] Thus, vehicles are (being) equipped with *autonomous intelligence*, which make them less dependent on human driving in the near future. The development and potential deployment of increasingly *autonomous vehicles* (AVs), and more specifically the different stages in the spectrum of autonomation that can be expected, have been mapped by the Society of Automotive Engineers (SAE) in collaboration with the International Organisation on Standardisation (ISO).[94]

[intended white space]

[91] See for instance Wyffels 2021, p. 35-38; Vellinga 2020, p. 139-140; Rao, Q., & Frtunikj, J., "Deep Learning for Self-Driving Cars: Chances and Challenges", conference paper to the 2018 ACM/IEEE 1st International Workshop on Software Engineering for AI in Autonomous Systems, via https://dl-acm-org.proxy.library.uu.nl/doi/pdf/10.1145/3194085.3194087 (last accessed 11 August 2021).
[92] Ibidem Wyffels, p. 35.
[93] See Vellinga 2020, p. 140.
[94] See https://www.sae.org/news/press-room/2021/05/sae-international-and-iso-collaborate-to-update-and-refine-industry-recognized-sae-levels-of-driving-automation (accessed on 11 August 2021) Their standard J3016_202104 is available through https://www.sae.org/standards/content/j3016_202104/.



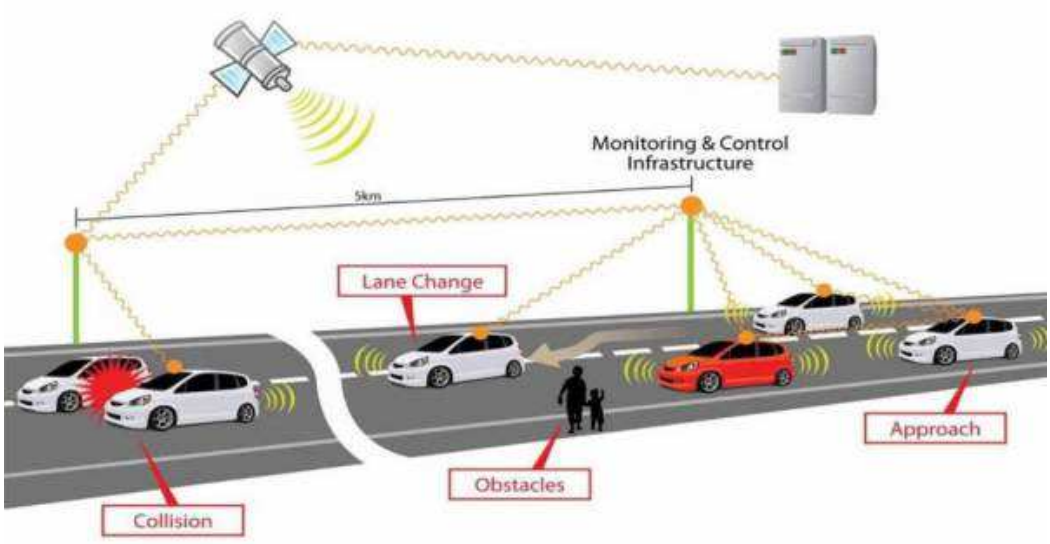
SAE distinguishes 6 stages of driving automation (see the image above).[95] The first stage, "Level 0" does not contain any automation; a human driver needs to perform all the aspects of what is called the "Dynamic Driving Task" (DDT). Automatic emergency braking, blind spot warning and lane departure warning may however be expected within a vehicle with Level 0-automation. Level 1, "Driver Assistance" still requires the human driver to be at the steering wheel, but the vehicle may be able to perform "part of the DDT by executing either the longitudinal or the lateral vehicle motion control subtask".[96] Level 2, which still refers a human to drive at all times, refers to "Partial Driving Automation". At this stage, longitudinal *and* lateral vehicle motion control subtasks can be deployed at the same time by the car itself. This means that adaptive cruise control and lane centering can operate at the same time. From the third level onwards, automation of the DDT increases such that a human operator can no longer be considered the driver when the automated driving features are engaged. At Level 3 however, the human driver is required to take back control on request of the vehicle. Within this third level, "Conditional Driving Automation", the

[95] SAE J3106, illustrated by SAE, available via https://www.sae.org/blog/sae-j3016-update (accessed 11 August 2021).
[96] SAE J3106_202104, p. 28. This comprises for instance lane-keep assistance or adaptive cruise control

Dynamic Driving Task may partially be executed by the vehicle itself, under limited conditions, and might operate as a "traffic jam chauffeur". A Level 4 "High Driving Automation" – car does not require a human driver for most of the driving tasks, and even the pedals and steering wheel are not considered necessary. Level 5 is the highest level, and refers to fully autonomous vehicles, which can drive themselves everywhere, under all conditions.

Where in this study I refer to AVs, or autonomous vehicles, SAE Level 5, fully autonomous-vehicles are indicated, unless stated otherwise. Fully autonomous vehicles are to date (September 2021) not deployed on the European roads.

It is likely that road- and communication infrastructure will contribute to the successful deployment of AVs. [97] This might include for example mechanisms allowing vehicles to communicate with one another (so called vehicle-to-vehicle, V2V, communication)[98] and/or with other elements on or alongside the road (vehicle-to-infrastructure, V2I, communication), in order to verify that those vehicles are driving properly, and that accidents are prevented as much as possible. The picture below illustrates how V2V and V2I communication may operate in order to warn upcoming traffic of a collision further down the road, and to instruct the upcoming traffic to change lanes, or to slow down.[99]



[97] See European Commission 2018d, p. 25-27.
[98] See Dey et al. 2016, *inter alia* where they observe that "[r]eliable and seamless vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communication is the critical component of Connected Vehicle Technology (CVT) applications (p. 169).
[99] This illustration was taken from the Technical Report "M2M enablement in Intelligent Transport Systems" by the M2M Automotive Working Group, Telecommunication Engineering Centre, Department of Tekecimmunications, Ministry of Communications & Information Technology, Government of India, November 2015 (release 2.0), p. 16, available via https://www.tec.gov.in/pdf/M2M/V2V%20%20V2I%20Radio%20communication%20and%20Embedded%20SIM.pdf (last accessed 11 August 2021).

Furthermore, as is currently often the case, it is likely that AVs will contain, or be connected to, event data recorders.[100] Albeit it is not sure in what form V2V, V2I and event data recorders will be operating, I assume within this study that, with the deployment of AVs, there will also be a role to play for what I indicate as "Accident Prevention and Registration Systems" (APRS), which might combine the V2V/V2I with the event data recording functions.

2.4 CONCLUSION

Above, I illustrated that *autonomous intelligence* describes the (growing) capacity of systems to behave increasingly independent of human intervention. In that, their capacity to learn plays an important role. For the purposes of this study, I defined *autonomous intelligence* as humanly created systems which have the ability to perceive information from their environment as *input* and to *process* that information in such a way that it can be used to achieve pre-defined goals as *output*, whereas those systems are increasingly autonomous as less human intervention is necessary in order to achieve these goals.

Road vehicles will be endowed with increasing *autonomous intelligence*. In order to illustrate that gradual process, the Society of Automotive Engineers drafted an overview of six steps, which relate to the increasing autonomy in cars. In this study, I refer to *autonomous vehicles*, which I understand to be SAE Level 5, i.e. "fully autonomous" vehicle following the SAE-classification.

[100] See European Commission 2018d, p. 8

Chapter 3. THEORETICAL CONCEPTS: INNOVATION & REGULATION

3.1 INTRODUCTION

In this Chapter, I introduce the main theoretical concepts of the study: innovation and regulation. The primary goal of this chapter is to identify factors comprised in regulation that may influence innovation, including acceptance of the results of innovation by consumers. Not only is this interesting in itself, it also fits within EU policy to foster innovation, especially within the fields of AI and robotics, and to make corresponding rules which stimulate rather than hinder innovation. The European Union strives for an Innovation Union: "a strategy to create an innovation-friendly environment that makes it easier for great ideas to be turned into products and services that will bring our economy growth and jobs",[101] as a part of the (former) Horizon 2020 framework,[102] as well as the current Horizon Programme.[103] In that, the EU aims to stimulate the development of 'robotics'[104] and 'AI'[105] in general, and autonomous vehicles as species thereof.[106] Investing in the development of robotics in Europe also stands high on the Digital Agenda.[107] Attracting innovators of autonomous intelligent technology can contribute to the competitive edge of the European Union over for instance America and Asia. However, policies on stimulating innovation do not always prove to be successful.[108] It is stated that "inconsistencies of rules and practices remain and are hampering the development of high growth innovative firms, which often find it too burdensome and risky to operate on other European markets".[109] The claim that regulation forms an obstruction to innovation in general is often made and forms a recurring concern of European regulators. As regards autonomous vehicles in particular, literature shows that the currently applicable regulatory frameworks in the EU do not necessarily stimulate innovation.[110] That these

[101] Quoted from http://ec.europa.eu/research/innovation-union/index_en.cfm (last accessed 28 January 2017).
[102] European Commission 2012.
[103] See inter alia European Commission 2021.
[104] See European Commission 2010, and the EC website on the "Digital Single Market": https://ec.europa.eu/digital-single-market/en/robotics; and on "Horizon 2020", https://ec.europa.eu/programmes/horizon2020/en/h2020-section/robotics (last accessed 28 Jan. 17); European Commission 2021, p. 9.
[105] See for example https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 (last accessed 28 April 2021).
[106] See also European Commission 2016.
[107] See European Commission 2012.
[108] See European Innovation Scoreboard 2016, and also the earlier editions thereof; furthermore Pelkmans & Renda 2014, p. 1.
[109] See State of the Innovation Union Report 2014, as cited in Pelkmans & Renda 2014. See also European Parliament 2017, p. 3.
[110] See for instance Robolaw 2014.

statements may be rather bold as general concepts is inter alia indicated by Pelkmans & Renda. They find that "regulation can at times be a powerful stimulus to innovation". Blind in turn claims that a vast amount of "studies still provide no clear picture of whether the negative impacts [on innovation] of regulation outweigh the positive effects". [111]

Against the background of these seemingly contradictory statements, I will try to distil factors from regulation which may influence innovation, on the basis of a (mainly legal academic) literature study in section 3.4. The concepts of innovation and regulation will be introduced hereunder in section 3.2 (innovation) and section 3.3 (regulation), before the impact of regulation on innovation in the field of autonomous vehicles can be explored, which will be done on the basis of a case study which is introduced in section 3.5.

3.2 INNOVATION

Innovation can be defined as "the introduction of novelties". [112] This can be measured in an objective or a subjective way: innovation may either regard the introduction of an objectively new phenomenon to society, when it has never been introduced before, or it may be perceived as novel by individual actors or groups in society to whom it is new. [113] Innovation can be distinguished from invention. Where invention may be seen as the development of ideas, innovation is the implementation or the use of invention. [114] Schumpeter held that innovation can even take place without invention. [115] The notion of innovation may furthermore refer to both a process and an outcome of a process. Black appreciates innovation as "a process in that it involves the formulation, elaboration and ultimately operationalization and implementation of a new idea". [116] In its Oslo Manual, the OECD views innovation as "the implementation of a new or significantly improved product […] or process […] in business practices, workplace organisation or external relations". [117]

Innovation and diffusion are different (although related) concepts. Diffusion can be used as a measurement of the rate, spread and speed of adoption of innovation in society. [118] Adoption in society includes the level of acceptance of innovation by citizens. Von Schomberg observes that (technological) innovations will be accepted by society, when they are aligned with societal needs

[111] Blind 2012, p. 3.
[112] Oxford English Diary, entry 1548. See also OECD 2005, p. 57.
[113] Black 2005, p. 4-6. The OECD Oslo Manual (OECD 2005, p. 57) adheres to three "concepts of novelty", being (subjective): "new to the firm", and (more objectively): "new to the market and new to the world".
[114] Black 2005, p. 6-7, and the reference to Mohr 1969, p. 112: "invention implies bringing something new into being; innovation implies bringing something new into use".
[115] Schumpeter 1939, p. 80-82.
[116] Black 2005, p. 7.
[117] OECD 2005, p. 46.
[118] Black 2005, p. 7-8.

and values.[119] Another conceptual observation relating to innovation is the notion of change.[120] The result of innovation can imply for instance an incremental or a radical (disruptive) change to products, processes or even paradigms, but it is not the same as innovation.[121]

As this study focusses on innovation in the field of AVs in the European Union, it is relevant to briefly illustrate the views of the European Commission regarding this concept, also because EU policy significantly focuses on stimulating innovation, as introduced in the previous section. The bases for the current innovation policies were laid down in 2016. In its Commission Staff Working Document *Better regulations for innovation-driven investment at EU level*, it is noted that "EU regulation matters at all stages of the innovation process from R&D to commercialisation".[122] In its vision document *Open Innovation Open Science Open to the World – a vision for Europe*, the Commission states that the focus has to be on opening up "the innovation process to all active players so that knowledge can circulate more freely and be transformed in products and services that create new markets, fostering a stronger culture of entrepreneurship".[123] This is necessary, as it is indicated that "We [the EU, *RWdB*], are too rarely succeeding in getting research results to the market. Technologies developed in Europe are most of the time commercialised elsewhere".[124] Similar statements are made in subsequent policy documents. The *renewed European Agenda for Research and Innovation* (2018) for example reads that

> "Europe is experiencing an innovation deficit. This is not down to a lack of ideas or initial start-ups: the problem is rather a lack of scale-up and diffusion, with innovations not always being translated into new market and growth opportunities. And industry investment in research and innovation has to step up".[125]

The Commission has put forward three focus points in its policy which remain relevant to date. Firstly, investments are deemed necessary in scientific and technological research; secondly business needs to be made "more innovation friendly and less risk averse";[126] and thirdly, EU citizens need to be guided through what is indicated as "a fast and, for some, turbulent transition".[127] Thus, EC's view on innovation encompasses R&D processes in science and in business (for instance through its *Horizon* programme), as well as diffusion: the deployment and acceptance of innovation among citizens.

[119] Von Schomberg 2011, p. 8.
[120] Black 2005, p. 8-11.
[121] Black 2005, p. 8-11.
[122] European Commission 2016b, p. 7, citing (and underscoring) Pelkmans & Renda 2014.
[123] European Commission 2016c, p. 11.
[124] Ibidem, p. 86.
[125] European Commission 2018c, p. 3.
[126] Ibidem.
[127] Ibidem.

> These principles are reflected in current EU-policy, for instance as enshrined in the proposal for the *Regulation on a European Approach for Artificial Intelligence* (hereafter: Proposed AIR).[128] This Proposed AIR is to form the cornerstone of future EU regulation of "trustworthy and ethical AI", aimed at creating people's "trust that the technology is used in a way that is safe and compliant with the law, including the respect of the fundamental rights",[129] and at contributing to people's "confidence to embrace AI-based solutions".[130] At the same time, the proposal aims at stimulating innovation in the field of AI, and more specifically at ensuring "legal certainty to facilitate investment and innovation in AI" as well as facilitating "the development of a single market for lawful, safe and trustworthy AI applications and [preventing] market fragmentation".[131] Thus, risks and problems related to *trust* must be prevented, although "without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market".[132]

This research is primarily focussed on innovation as the outcomes of the R&D-processes underlying autonomous intelligent technology itself, and not so much at the business processes which are taking up the technology, workplace organisations or external relations. Adoption, or the accepted diffusion and deployment of autonomous vehicles in society, will be taken to be included in the definition of innovation used in this study, but for the sake of clarity, where necessary also mentioned apart.

[128] European Commission 2021a (Proposed AIR).
[129] Proposed AIR, p. 1.
[130] Ibidem.
[131] Ibidem, p. 3.
[132] Ibidem.

3.3 REGULATION

3.3.1 INTRODUCTION

In the following sections, the notion of *regulation* will be explored in order to outline a frame of reference that is further used in this research for a) mapping the factors in regulation that may influence innovation in Part II, and b) providing recommendations for optimizing these factors in order to make the studied regulatory frameworks more innovation-friendly in Part III.[133] In that regard, the findings of the following sections will serve as (one of the) frames of reference to which the "routes for improvement" in Chapter 9 are related.

The idea of what *regulation* entails, has changed in the past years. "Classic" conceptions of *regulation* often stressed that it is about the state (the regulator) exercising "sustained and focussed control exercised by a public authority over activities valued by the community"[134] (the regulatee), by for instance issuing and enforcing laws. A more contemporary concept, reflecting the actual diverse regulatory landscape, is given by Drahos and Krygier. They – very broadly – hold that *regulation* sees to "influencing the flow of events".[135] While their notion may be a bit over-encompassing, as the definition itself does for example not directly refer to regulators nor regulatees, Drahos & Krygier do point out that it is not only the state (or a another public actor) who may issue (and ultimately enforce) rules, but that also non-public actors can play a role in the regulatory process. A definition of *regulation* that also acknowledges the (over time increasing) role of private actors, has been developed by Lodge and Wegrich, who define it as the "intentional use of authority that affects the behaviour of a different party".[136] A similar concept is used by Baldwin, Cave & Lodge, who distinguish different viewpoints regarding the question what *regulation* means, and stress that *regulation* can be seen as "*all forms of social or economic influence* – where all mechanisms affecting behaviour—whether these be state-based or from other sources (e.g. markets)—are deemed regulatory".[137] *Regulation* thus encompasses the

[133] See section 1.1.5.
[134] See for example Selznick, P., "Focusing Organisational Research on Regulation", in; Noll, R. (ed.), *Regulatory Policy and the Social Sciences, Berkeley*, University of California Press, 1985, p. 363 as referred to in Baldwin, Cave and Lodge 2012, p. 2-3, as paraphrased in De Cock Buning & Senden 2020, p. 6; also Black 2002, p. 11.
[135] Drahos & Krygier 2017, p. 7-18, referring to Parker & Braithwaite 2003, p. 119. Their concept of *regulation* must be seen broadly; regulation is about legal and non-legal norm-making, varying from for example states issuing rules on fat- and sugar levels in food, to supermarkets who influence buying behaviour of their customers by designing the most effective layouts of their aisles, based on years of observation of consumer behaviour. Also: Black 2001.
[136] Lodge, M., & Wegrich, K., *Managing Regulation: Regulatory Analysis, Politics and Policy*, Basingstoke: Palgrave Macmillan 2012, p. 16, as cited in De Cock Buning & Senden 2020, p. 6; also: Black 2001, p. 105-114; Black 2002, p. 11.
[137] Baldwin, Cave & Lodge 2012, p. 3. The other viewpoints they differentiate are: "*a specific set of commands*", and "*deliberate state influence*"; See also Black 2002, p. 11.

intentional activity from one (public or private) entity, the *regulator*, to influence the behaviour of another entity, the *regulatee*. For this study, I add that the focus will be on norms, rules and standards that have been intentionally set, rather than on *de facto* forms of regulation. *Regulation* can furthermore be viewed as a process,[138] consisting of different phases. The early stages of the process can comprise of agenda-setting (policy making), and actual rule-making, which is in the later stages followed by implementation of the respective rules, and monitoring and enforcement thereof.[139] Also the evaluation of existing rules and the revision thereof, can be held to be included in the regulatory process.[140]

Hereafter, I illustrate a brief overview of the different actors that can play a role in regulatory processes in section 3.3.2. As the role of private actors is increasingly important in the regulatory process, forms of private regulation are more specifically addressed in section 3.3.3. I will take a closer look at the "mix" of existing regulatory instruments that can be identified within the Union in section 3.3.4. With a view on the last part of the central research question, current "quality standards" for regulation in the EU are elaborated in section 3.3.5.

3.3.2 ACTORS IN THE REGULATORY PROCESS

Regulator and *regulatee* generally are the two kinds of actors that must be distinguished in the regulatory process. Where (hence the corresponding 'classic' definitions of *regulation*) regulators may traditionally have been public authorities, such as states or other governmental bodies, and regulatees were private entities (such as citizens or companies), whereby the regulator applied some kind of "command and control" regulation,[141] nowadays many forms of "private regulation" are in place.[142] As opposed to public regulation, private regulation is characterized by the fact that private actors are, to a varying extent, *regulator*, rather than, or along with public actors.

> Examples of public regulation include statutes, laws, regulations and directives, such as the – for this study relevant – Product Liability Directive, national (product- and traffic) liability laws, the General Data Protection Regulation and the corresponding national provisions on the execution thereof.
>
> Examples of private regulation are common rules, codes of conduct, memoranda of understanding, voluntary agreements, industry agreements, standards, guidelines, regulatory

[138] See for example Parker & Braithwaite 2003, p. 119, as cited in Drahos & Krygier 2017, p. 7; Senden et al. 2015, p. 35; Cafaggi & Renda 2012, p. 11.
[139] See Senden et al. 2015, p. 35; Cafaggi & Renda 2012, p. 10-11. Sometimes, enforcement is distinguished from *regulation*. See De Cock Buning & Senden 2020, p. 7.
[140] See for instance European Commission 2019 (COM(2019) 178), p. 8.
[141] "command and control" can be seen as "the exercise of influence by imposing standards backed by criminal sanctions", as defined by Baldwin, Cave & Lodge 2012, p. 106.
[142] See for example De Cock Buning & Senden 2020, p. 11; Black 2002, p. 2-3.

contracts, best practices et cetera.[143] In terms of this study, I can *inter alia* refer here to the Data Protection Principles for Connected Vehicles from the German "Verband der Automobilindustrie",[144] and the ACEA Principles of Data Protection in Relation to Connected Vehicles and Services from the "European Automobile Manufacturers Association".[145]

3.3.3 PRIVATE REGULATION IN RELATION TO PUBLIC REGULATION

The increase of the body of private regulation may be correlated with tendencies of governance decentralization, and deregulation policies, aimed *inter alia* at improving competitiveness, by removing certain regulatory burdens.[146] Furthermore, private regulation is often advocated,[147] for its capacity to respond fast and effectively to emerging problems (for instance in the field of emerging technologies),[148] where private regulation may make easy use of the (technical) expertise of the private actors concerned.[149] It also enables the involvement of all relevant stakeholders, including the (future) *regulatees* in the process.[150] Private regulation allows for transnational arrangements to be made, where that would be less easy in a 'traditional' public regulatory process,[151] and it can be more cost-efficient as opposed to public regulation.[152] Furthermore, private regulation can be said to enhance the protection of the rights, and improve confidence of consumers, as well as the image of the business.[153]

However, private regulation also has imminent risks.[154] These lie for example in the (absence of) democratic legitimacy: especially where there are no adequate mandates for the respective private regulators, the public justification of private regulation and enforcement can be questioned.[155] Furthermore, a lack of transparency of the process and accountability of private regulators is sometimes mentioned as a risk, as private regulators cannot always be held accountable for their regulating and enforcement activities under (some forms of) private

[143] See Cafaggi & Renda 2012, p. 4, De Cock Buning & Senden 2020, p. 2, and their reference to the (non-exhaustive) database on co- and self-regulation that the European Economic and Social Committee : http://www.eesc.europa.eu/?i=portal.en.smo-database.
[144] https://www.vda.de/en/topics/innovation-and-technology/network/data-protection-principles-for-connected-vehicles.html, last accessed on 11 Sep. 19.
[145] https://www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to-connected-vehicles-and-se, last accessed on 11 Sep. 19.
[146] See Senden 2005, p. 4-6; and Cafaggi & Renda 2012, p. 1-2.
[147] I have paraphrased hereafter the "positives" of private regulation as mentioned – and referred to in De Cock Buning & Senden 2020, p. 4-5. See also Cafaggi & Renda 2012, p. 3; and Kulk 2018, p. 51
[148] Cafaggi 2008, p. 8-9.
[149] See Baldwin, Cave & Lodge 2012, p. 139.
[150] De Cock Buning & Senden 2020, p. 4.
[151] See Kulk 2018, p. 51, De Cock Buning & Senden 2020, p. 4-5.
[152] Baldwin, Cave & Lodge 2012, p. 140; Kulk 2018, p. 51; De Cock Buning & Senden 2020, p. 4.
[153] OECD 2015, p 6, as cited in De Cock Buning & Senden 2020, p. 4.
[154] Also here, I have paraphrased De Cock Buning & Senden 2020, p. 4. See also Kulk 2018, p. 52, and the examples by Cafaggi & Renda 2012, p. 2-3. Both De Cock Buning & Senden and Cafaggi point at examples of where (some of) such risks manifested, including the banking crises
[155] Baldwin, Cave & Lodge 2012, p. 141-142; De Cock Buning & Senden 2020, p. 4-5., Kulk 2018, p. 52.

regulation.[156] Private regulation may also comprise the risk that other (core) values including fundamental rights of others than the respective regulators/regulates are neglected.[157] There also is a risk that not *all* relevant actors are included in the regulating process, and that there would be insufficient monitoring and enforcement of compliance with the respective rules.[158]

There are many forms of private regulation, which have been mapped *inter alia* by De Cock Buning & Senden.[159] Private, or self-regulation, with no government intervention in the regulatory- and enforcement process, can be opposed to public regulation, with full government involvement.[160] There is a spectrum of regulatory "modes" between these two extremes.[161] Roughly four main categories are indicated,[162] depending on the level of public involvement therein, being:

i. No regulation, or regulation on firm level only (such as specific types of corporate social responsibility codes, which only bind the firm itself);
ii. Self- or purely private regulation and enforcement (characterized by little or no government influence in the regulatory process, which is conducted by for instance industry and stakeholders such as NGOs, for example regarding industry codes, civil regulation and multi-stakeholder regulation);
iii. Co- or private-public regulation (referring to varying levels of government influence within different stages within the policy cycle, including forms of mandated- and non-mandated self-regulation); and
iv. Public command-and-control regulation (characterized by little or no private influence in the regulatory process, where results thereof include for example statutory regulations and statutory sanction systems)

In the first category, *regulator* and *regulatee* are more or less the same actor, whereas in the other categories, a *regulator* extends rules to a – to a varying extent – external *regulatee*. Noteworthy in this respect is the growing body within in the second category regarding one specific kind of "self- or purely private regulation and enforcement", i.e. the growing body of contracts imposed by internet platforms on all the users thereof in the same way. It can be questioned whether or not these imposed contracts should be qualified as regular contracts between two (or more) parties,

[156] See Baldwin, Cave & Lodge 2012, p. 142-143, who also indicate that accountability-risks are often low, as "self-regulators may be subject to non-member (meaning: external, even sometimes public, *RWdB*] controls".
[157] De Cock Buning & Senden 2020, p. 5.
[158] Ibidem.
[159] See Senden 2005, and the further elaboration of that work in De Cock Buning & Senden 2020. Another overview is given by Black 1996, p. 27-28. See also, for perspective on private regulation in Dutch private law: Giesen, I., "*Alternatieve regelgeving en privaatrecht*", Deventer: Kluwer 2007.
[160] De Cock Buning & Senden 2020, p. 8-9.
[161] Ibidem, p. 8.
[162] Ibidem, p. 7-11, where on p. 7 this numbered overview is given.

rather than *regulation*. Taking the *regulation* definition outlined in section 3.3.1 as a starting point, it can be observed that norm-making by internet platforms can be seen as "intentional activity" from one (public or private) entity – i.e. a platform operator, the *regulator*, to influence the behaviour of another entity, the *regulatee*, i.e. a multitude of platform users. It must furthermore be taken into account that such contracts cannot be negotiated: in order to get access to the respective platforms it is a prerequisite that the provisions drafted by the platform operators are accepted by the prospective users. When there is little or no competition on the market of the respective services and service providers (for example video sharing platforms, certain social media with a very high participation rate under the general public, or a *de facto* standard for internet search operations), it can be argued that there in fact neither is contractual freedom regarding the choice for consumers of parties to contract with (as these are mono- or oligopolists), or contractual freedom regarding the scope and contents of the agreements to be made, as these are dictated by the respective service providers.

> End User License Agreements, Terms of Service, Terms and Conditions and comparable instruments that lie at the basis of contracts between mono- or oligopolist internet platform providers (e.g. YouTube, Google, Facebook) and internet users are examples of such forms. Provisions of these contracts must be accepted by the prospective platform users, in order to be granted access to the respective platforms, while these platforms can be seen as *de facto* standards for video sharing,[163] social media,[164] and internet searching.[165] Such contracts may have far-reaching consequences for user behaviour, as strict rules are often set, and enforcement of non-compliance by the users (*regulatees*) may implicate that the use of the respective platforms is (automatically) restricted by the platform providers (*regulators*).[166]
>
> This form of "automated regulation and enforcement" is and will increasingly be used.[167] Examples include for example digital rights management (DRM) schemes[168] and other technological protection measures[169] such as upload filter mechanisms,[170] and furthermore

[163] Youtube's market share on the market for online video platforms d.d. 11 October 2019 was over 73%, according to https://www.datanyze.com/market-share/online-video/youtube-market-share.
[164] Facebook's market share on the market for social media d.d. 11 October 2019 was over 72%, according to https://gs.statcounter.com/social-media-stats.
[165] Google's market share on the market for search engines was almost 93% on 11 October 2019, according to https://gs.statcounter.com/search-engine-market-share.
[166] See for example Hassan & De Filippi 2017, p. 89; Schulz & Dankert 2016, p. 9-10.
[167] See Schulz & Dankert 2016, p. 5-6; Hassan & De Filippi 2017, p. 89.
[168] Where a copyright license is in fact translated in software code that grants access to the respective copyrighted work it applies to (for instance a movie or a song), which automatically restricts that access, when the terms of the license are no longer met.
[169] See Kulk 2018, p. 41-42.
[170] Such filters are used by for example user-generated-content platforms as Youtube, and are to prevent the user-uploading of content that infringes copyrights.

technology such as underlying the U.S. "No Fly List",[171] and smart contracts that underly transactions that use blockchain technology.[172] It is very likely that *automated regulation and enforcement* will also be applied in AVs. As one of the (envisaged) forms thereof, Schulz & Dankert mention that for instance the obligation to wear seatbelts may be embedded in the AV soft- and hardware, and that compliance can be enforced through the circumstance that a respective vehicle will not operate without properly buckled up passengers.[173] Furthermore, they illustrate that there are certain rules that need to be embedded in the AV code that are left unregulated in the traditional regulatory frameworks, such as regarding the solution of "trolley problems":[174] in some situations, an AV may for example have to decide either to harm a person outside the car, or the driver,[175] or must choose to overrun either a group of 5 elderly people, or a young person pushing a pram. Whereas there may hardly ever be a satisfactory solution of such problems in for instance a criminal- and civil liability perspective, ethical choices between such evils do have to be incorporated *ex ante* in the operating software of AVs. It can also be imagined that AVs which are offered "as a service" to end users (thus functioning as self-driving taxis), may for example be endowed with algorithms calculating the financial trustworthiness of potential passengers. In order to calculate the risk of non-payment, a background check be could carried out regarding the prospective passengers resulting in a likelihood that the ordered ride is paid for. Passengers with a "bad" outcome of that calculations may be denied of the services.

These examples illustrate, in line with Lessig's paradigm that "code is law",[176] that physical objects, such as AVs, when endowed with software enabling automated decision making on the basis of pre-programmed rules, may have a direct impact on human behaviour, which is intended by the respective (AV) manufacturers and thus be qualified as *regulation* – often of a

[171] This technology is used by a public- rather than a private actor, namely US Government, and disallows access to the US for those people who may form a risk for national security. That risk assessment is based on "data mining to make predictive assessments about threats for national security" (Hassan & De Filippe 2017, p. 89 and their reference to Citron D.K., "Technological Due Process", *Washington University Law review* 2007, vol. 85, p. 1249-1313.

[172] See for more background on the self-executory character of smart contracts used in blockchain-based technology for instance Levy, K.E.C., "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law", *Engaging Science, Technology and Society*, 2017 vol. 3, p. 1-15, DOI:10.17351/ests2017.107, also available via http://estsjournal.org/article/download/107/61 (accessed October 11 2019).

[173] Schulz & Dankert 2016, p. 7.

[174] The classic *trolley problem* (introduced by Foot, Ph., "The Problem of Abortion and the Doctrine of the Double Effect", *Oxford Review* 1967 no. 5) essentially encompasses the following question: A runaway train lorry races towards a track segment in which 5 people lie tied-up. You are in control of a lever, which will deviate the lorry to a side-track, in which 1 person lies tied up. What do you do? Kill 1, of kill 5?

[175] Schulz & Dankert 2016, p. 6-7.

[176] Lessig 2006, *inter alia* part II, p. 83-157.

private nature. One of the differences with more traditional forms of regulations is that these forms of *automated regulation* (especially when embodied in for instance AVs) are not only capable of (*ex-ante*) norm-making, but also able to enforce these themselves at the same time, where traditional forms of regulation often are prescribing certain norms, which the *regulatees* can choose to comply with or not, while the *ex-post* enforcement often (although not always) is in the hands of another actor than the *regulator*.[177]

Also within the third category, there is great diversity regarding *inter alia* the stages of the policy cycle that can be distinguished,[178] the nature and the intensity of the public involvement at hand. De Cock Buning & Senden illustrate that a further sub-categorisation can be made within that third category.[179]

The two sub-categories are:

a. Non-mandated self-regulation,[180] with limited political influence in the early stages of rule-making, regarding for example the acknowledging or support of the self-regulatory body, which can be labelled as "tacitly supported self-regulation". Regarding the later stages of regulation, including monitoring and enforcement by the self-regulatory body, public involvement may comprise of keeping an eye on the safeguarding of public interests that may be relevant. The latter can be labelled as "substitute self-regulation";
b. Mandated self-regulation,[181] where, regarding the early stages of regulation, public activity sees to for instance encouraging private entities to create their own rules, either within "general goals" formulated by the public actor, or even within framework criteria and formal conditions under which the private norm-making should take place. This can be labelled as "conditioned self-regulation". Regarding the later stages, public involvement may for instance appoint a public actor who is to monitor and enforce compliance with the rules and may also result in the adoption of the drafted rules into "public" laws. The latter can be labelled as "enforced self-regulation".

The foregoing indicates that there is a myriad of forms, modes, types and kinds of *regulations* expressing norms to be complied with by *regulatees*, stemming from different sources, resulting

[177] See also Schulz & Dankert 2016, p. 7-8; Hassan & De Filippi 2017, p. 89.
[178] These stages comprise of: "policy design and preparation, adoption, implementation ("transposition, complementary non-regulatory actions), application (including monitoring and enforcement), evaluation and revision", which is listed as such in the European Commission 2017 (SWD(2017) 350 final), p. 5, via https://ec.europa.eu/info/sites/info/files/better-regulation-guidelines-better-regulation-commission.pdf (accessed 12 August 2019).
[179] De Cock Buning & Senden 2020, p. 10-11, citing the earlier work by Senden et al. 2015.
[180] Ibidem.
[181] Ibidem.

from varying interplays between public and private *regulators*. In the following sections, I will take a closer look at (some of these) regulatory instruments that are applicable within the European Union.

3.3.4 REGULATORY MIX WITHIN THE EU

The idea that a diverse palette of policy instruments can be "mixed" in order to reach certain (in that case: environmental) goals was introduced in 1999 by Gunningham and Sinclair.[182] They advocated that a mix of diverse regulatory instruments should be used rather than a single instrument, which are tailored to reach "specific policy goals".[183] The notion of "mixed regulation and enforcement regimes in the European Union" was taken as the point of departure for research on a general level by De Cock Buning, Ottow & Vervaele.[184] They identify, extrapolating the lines of Gunningham and Sinclair's observations, currently a mix exists of "shared private-public regulation and enforcement regimes" on the one hand, and "shared national-European regulatory and enforcement regimes" on the other hand.[185] The mix sees to different modes of national (Member State) regulation in relation to EU regulation, and different modes of private regulation in relation to public regulation. Both aspects (mixed private-public regulation and EU-national regulation) will be addressed below. That is, the focus will be on EU-regulation, as observations relating to regulation stemming from the institutions of the European Union can easier be made in general terms than observations relating to Member State regulation. Member State regulation is elaborated where opportune in other parts of this study (as for example in Chapter 4, where national liability regimes are observed).

Two "hierarchical layers" of applicable regulation stemming from the institutions of the European Union are to be distinguished. *Primary EU law* is formed by the three Treaties and the protocols and annexes thereto,[186] including the Charter of Fundamental Rights of the European Union (hereinafter: "Charter"),[187] and the case law of the CJEU insofar as these concern "the fundamental principles of Union law […], including the requirement to protect fundamental rights".[188] Unilateral acts and agreements that are directly based on the Treaties are *secondary EU law*. Different sources of *secondary* law are listed in article 288 TFEU. These include regulations,[189]

[182] Gunningham & Sinclair 1999.
[183] Idem, p. 49, 69-70.
[184] De Cock Buning, Ottow & Vervaele 2014.
[185] All three citations in this sections are from De Cock Buning, Ottow & Vervaele 2014.
[186] These are: the Treaty on European Union (hereinafter: "TEU"); the Treaty on the Functioning of the European Union (hereinafter: "TFEU"); and the Treaty establishing the European Atomic Energy Community.
[187] Article 6(1) TEU states that the Charter has "the same legal value as the Treaties".
[188] See Bradley 2014, p. 103.
[189] Article 288 THFEU stipulates that regulations have general application, and that these are directly applicable in the Member States, and are binding in their entirety.

directives, [190] decisions, [191] recommendations and opinions. [192] Furthermore, international agreements and interinstitutional agreements (between the different institutions of the European Union) can be qualified as *secondary* law, insofar these are based on the Treaties, and comprise binding norms.[193] The aforementioned sources generally are forms of public regulation.

In (mainly) *secondary* law tools, the institutions of the European Union have addressed different modes of private-public regulation. This was done using for examples the instruments of "white papers" and other "communications" of the European Commission, and "interinstitutional framework agreements" between the three institutions of the European Union (European Council, European Parliament and the European Commission),[194] in order to cover the entire EU legislative process, which (at least regarding private-public regulation) did not exist until 2003.[195]

From the publication of the 2001 "White Paper on European Governance"[196] onwards, also forms of private regulation were endorsed by the European Commission, and subsequently gained popularity as complementing the existing (aforementioned) policy tools.[197] The Commission held in 2001 that, in order to reach "better and faster regulation", the palette of "formal rules" should be *inter alia* "combined with other non-binding tools such as recommendations, guidelines or even self-regulation within a commonly agreed framework", and also "co-regulation [combining] legislative and regulatory action with actions taken by the actors most concerned, drawing on their expertise" must be considered as a part of for example implementing measures.[198] Self-regulation and co-regulation furthermore became part of the Interinstitutional Agreement on Better Lawmaking of 2003,[199] however it was removed in the IIA 2016,[200] and has become part of

[190] Article 288 TFEU specifies that directives are binding "as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods", which thus need to be transposed into national law. See Bradley 2014, p. 100.
[191] Decisions are binding in their entirety – when applicable – to those who are addressed therein (art. 288 TFEU).
[192] According to article 288 TFEU, recommendations and opinions do not have binding force.
[193] See Bradley 2014, p. 102-103 and art. 295 TFEU.
[194] See for a more extensive overview Menting 2016, p. 69 – 81.
[195] See Menting 2016, p. 72.
[196] European Commission 2001. See for example p. 4.
[197] This reflected the standpoint that EU regulation should be improved, and unnecessary bureaucracy should be reduced, and fits within the "Better Regulation"-policy, which remains in place to date (https://ec.europa.eu/commission/news/better-regulation-principles-2019-apr-15_en), accessed 12 August 2019. See furthermore De Cock Buning & Senden 2020, p. 13-15.
[198] European Commission 2001, p. 20-21.
[199] European Parliament, Council and Commission, Interinstitutional Agreement on better law-making, *OJ* C 321/1, 2003. See section 17; for co-regulation sections 18-21, and for self-regulation 22-23.
[200] Interintstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on better law-making, *OJ* L 123/1, 2016. See the commentary by De Cock Buning & Senden 2010, p. 14-15. Menting 2016 remarks that self- and co-regulation are no longer addressed in the IIA 2016 (p. 72-73), however that it is unclear whether or not the IIA 2016 is binding. Menting also observes (p. 28) that the wordings of the IIA 2003 implicate that that document may be binding *inter pares*, thus between the three legislative institutions of the EU.

the EC strategy on Better Regulation,[201] as well as the regulatory fitness and performance programme of the Commission (REFIT)[202] Toolbox.[203]

In the Better Regulation Toolbox, self-regulation is defined as follows: "Self-regulation is where business or industry sectors formulate codes of conduct or operating constraints on their own initiative for which they are responsible for enforcing".[204] Added here, is that "pure self-regulation" is very uncommon within the EU, and that the EC often stimulates self-regulation by means of "instigating or facilitating the drawing up of the voluntary agreement".[205] The same document qualifies co-regulation as the "mechanism whereby the Union Legislator entrusts the attainment of specific policy objectives set out in legislation or other policy documents to parties which are recognised in the field (such as economic operators, social partners, non-governmental organisations, standardisation bodies or associations)".[206] The Commission explains here that recognition of co-regulation make take place in EU legislation, or through "cooperation agreements".

> In the Better Regulation Toolbox-documents, some examples of self- and co-regulation are highlighted. For example the (former) voluntary agreements on CO2 emission reduction between the Commission and EU/Asian car manufacturers are mentioned,[207] as well as the voluntary agreement between CEOs of internet companies and the EC regarding "better internet for kids", after a "call from the Commission".[208] Other examples are for instance embedded in the General Product Safety Directive, which aims at the development of standards on product safety,[209] and the General Data Protection Regulation, which calls on "industry" to come up with codes of conduct and certification mechanisms that can be "used as an element to demonstrate compliance" with the rules.[210] Many more examples are listed in the "Database on Self- and Co-regulation Initiatives" that is introduced by the European Economic and Social Committee. With 138 entries to date, this database is an illustration of the "mix" of regulatory instruments that is currently in place within the European Union.

[201] See De Cock Buning & Senden 2020, p. 15, footnote 75 for a detailed overview of Commission documents.
[202] See European Commission 2017 (SWD(2017) final).
[203] European Commission 2017a, section 3.1, p. 109-111.
[204] Ibidem, p. 109.
[205] Ibidem. It must however be noted that an increasing body of contracts between service providers and users can be found, which can in fact be qualified as regulation.
[206] Ibidem.
[207] which have – however – subsequently been replaced with regulation, see European Commission 2017a, p. 110.
[208] Ibidem.
[209] See cons. 14, 15, art. 3(2-3), 4(1) – and following – General Product Safety Directive.
[210] See cons. 81, 100, 166, art. 24(3), 25(3), 27(5) – and following – GDPR.

The regulatory frameworks under investigation in this study, both comprise "mixed" instruments. The extra-contractual liability regulation studied in Chapter 4, contains for example instruments of primary EU-law (stemming from the Product Liability Directive) in combination with Member State-specific rules (i.e. the national implementations of the Product Liability Directive, and the non-harmonised traffic liability frameworks. The personal data protection framework studied in 0, is an example of primary EU-law (in the form of the General Data Protection Regulation, which allows to a certain (small) extent tailor-made delegated rule-making by Member States. Furthermore, the General Data Protection Regulation relies to a large extent on rule-specification and guidance by supervisory authorities, and actively encourages private actors in the rule-making process, *inter alia* in the form of certification mechanisms and codes of conduct.

3.3.5 QUALITY OF REGULATION IN THE EU

The question whether regulation can be qualified as "good" been addressed in literature *inter alia* by Baldwin Cave & Lodge, [211] who indicate five criteria that need to be assessed in order to answer that question from a procedural point of view. First of all, there should be an adequate legislative mandate. [212] The (proposed) regulation should not exceed the competences they have been equipped with, in order to be "legitimate" from a democratic perspective. Secondly, the *regulator* should be accountable for the respective regulatory action, to those who provided the mandate to regulate.[213] Thirdly, the regulatory procedure to be followed, needs to be open for stakeholder participation, whereas standards of "equality, fairness and consistency of treatment" must be applied, in order to gain "public support" of the regulatory measures at hand.[214] Furthermore, regulations must be – where necessary and possible – be based on relevant "expert judgment".[215] Lastly, efficiency needs to be pursued.[216] These – rather general – criteria do to a certain extent reflect in the principles observed in EU policy on regulation, among some other procedural and material requirements for what is called "better regulation".

The three EU institutions have stated in their 2016 Interinstitutional Agreement on Better Regulation, underscore that they will observe the "general principles of Union law, such as democratic legitimacy, subsidiarity and proportionality and legal certainty",[217] when drafting legislation. Furthermore, they agree to "promote simplicity,[218] clarity and consistency in the

[211] See Baldwin, Cave & Lodge 2012, p. 26-31.
[212] Baldwin, Cave & Lodge 2012, p. 26-27.
[213] Ibidem, p. 27.
[214] Ibidem, p. 28.
[215] Ibidem, p. 29-30.
[216] Ibidem, p. 30-31.
[217] IIA 2016, p. 2.
[218] The efforts undertaken to simplify (existing) legislation, are elaborated in the REFIT-programme. See p. 8, section 48.

drafting of Union legislation and to promote the utmost transparency of the legislative process".[219] The outcomes of the regulatory processes within the EU, should be among other things comprehensible and clear, in a sense that *regulatees* easily understand their rights and obligations, whereas overregulation and administrative burdens must be avoided. Moreover, regulation frequently needs to be appropriately reported, monitored and evaluated,[220] and should be practical to implement by the Member States.[221] It is furthermore stressed that fundamental rights must be respected in the regulatory process.[222] Before regulation (including "legislative and non-legislative initiatives, delegated acts and implementing measures") [223] is drafted, assessments need to be carried out regarding the expected significant economic, environmental and social impacts. Stakeholders are invited to participate in the law-making process through "public and stakeholder consultation".[224]

The IIA-principles are compatible with the EC-initiative regarding "Better Regulation", which is aimed at designing EU law and policy "so that they can achieve their objectives at minimum cost",[225] and proposes "a way of working to ensure that political decisions are prepared in an open, transparent manner, informed by the best available evidence […], and backed by comprehensive involvement of stakeholders". [226] Better Regulation consists of six steps, being: 1. Forward planning and political validation, using *inter alia* "annual programs" [227]; 2. Stakeholder consultation, in order to guarantee "openness" and to "provide feedback and evidence to support evaluations, impact assessments, the preparation of initiatives and political decisions"; [228] 3. Evaluation and fitness checks, regarding *inter alia* economic, social and environmental impact, also compared to the impacts that were expected beforehand; [229] 4. Impact assessments that identify and describe the "problem to be tackled" and also regards the expected economic, environmental, social and sustainability predicted impacts of certain measures; [230] 5. Quality control, by the Regulatory Scrutiny Board; and 6. Implementation support and monitoring, in order to prevent the addition of unnecessary measures by the Member States.[231]

[219] Ibidem.
[220] Evaluations should, according to section 22, include: "efficiency, effectiveness, relevance, coherence and value added".
[221] Ibidem.
[222] Ibidem, p. 4, section 12, and p 5, section 25.
[223] Ibidem, p. 4, section 13.
[224] Ibidem, p. 5, section 19.
[225] European Commission 2017a, p. 4.
[226] Ibidem.
[227] Ibidem, p. 6.
[228] Ibidem, p. 8
[229] Ibidem.
[230] Ibidem, p. 8-9.
[231] Ibidem, p. 9.

In the IIA of 2003,[232] self-regulation and co-regulation were addressed specifically. In section 22 of the IIA 2003, self-regulation was defined as: "the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)". It is indicated that "the Commission will scrutinise self-regulation practices in order to verify that they comply with the provisions of the EC Treaty".[233] Furthermore, the Commission was to inform the other institutions of self-regulatory initiatives, and it had to maintain whether or not these would contribute to the Treaty objectives and provisions, and also whether or not these would be satisfactory in terms of "representativeness of the parties concerned, sectoral and geographical cover and the added value of the commitments given".[234] Should these criteria not be properly observed by the self-regulator, the Commission reserved the right to consider to regulate itself.[235] Co-regulation, "the mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)" was also addressed in the IIA 2003.[236] It required that co-regulation was only to be used on the basis of a legislative act "so as to enable the legislation to be adapted to the problems and sectors concerned, to reduce the legislative burden by concentrating on essential aspects and to draw on the experience of the parties concerned".[237] Furthermore, the principles of subsidiarity and proportionality must be obeyed.[238] Furthermore, the parties affected by the basic legislative act may "conclude voluntary agreements for the purpose of determining practical arrangements", after which the Commission should "verify whether or not those draft agreements comply with Community law (and, in particular, with the basic legislative act)".[239] The other institutions were also given a chance to comment on the proposed texts, and to object thereto "if it is considered that the draft agreement does not meet the objectives laid down by the legislative authority", and an opportunity to request the Commission to regulate itself.[240] A legal act which forms the basis of a co-regulation arrangement, should also indicate *inter alia* monitoring-, enforcement and

[232] See also De Cock Buning & Senden 2020, p. 16-17.
[233] IIA 2003, section 22.
[234] IIA 2003, section 23.
[235] De Cock Buning & Senden (2020, p. 16) observe that this conception of self-regulation should be qualified as some form of private-public regulation, rather than as "pure self-regulation", as "the Commission keeps a close watch on whether the self-regulatory practices comply with the EU Treaties".
[236] Sections 18-21 IIA 2003.
[237] IIA 2003, section 18.
[238] Ibidem, section 19.
[239] Ibidem, section 20.
[240] Ibidem.

evaluation measures.[241] Co- and self-regulation are not specifically addressed in the IIA 2016, however Regulatory Fitness (REFIT-)toolbox still refer to these concepts.[242]

The aforementioned criteria on Better Regulation thus only apply to what is (or was) addressed as co- and self-regulation, as defined by the EU institutions. This entails, that other forms of self-regulation, including for example those referred to as *automated regulation and enforcement* above, are not bound to Better Regulation principles. However, from an "acceptance" point of view, it would be advisable that such principles are taken into account, as will be illustrated below.

De Cock Buning & Senden, who acknowledge and reflect on the aforementioned EU-standpoints on *inter alia* better regulation, specifically focus on the "citizens perspective" that should be taken into account in forms of private regulation. They underscore that when *regulatees* are EU citizens ("consumers, employees, self-employed persons, "regular" citizens […]" [243] and (small) companies), their trust in (private) regulatory regimes and the enforcement of the rules, is vital for acceptance thereof. They indicate that legitimacy plays an important role in that respect.[244] It needs to be ensured that the *regulator* has adequate democratic legitimation in order to be "trusted", especially in private regulation arrangements. [245] Furthermore, the level of trust(worthiness) in respective regulatory regimes can be influenced by *inter alia* expertise, representativeness and reputation of the regulator.[246] Besides legitimacy, also effectiveness is found to influence citizens' trust in, and acceptance of regulation: when the outcomes of regulation and enforcement-regimes are effective, in the sense that the policy goals are achieved, there is a higher chance of acceptance thereof and vice-versa: higher acceptance of a regime leads to more effectiveness. [247] Moreover, ensuring compliance and enforcement of certain rules is said to influence trust in, and acceptance of regulatory regimes. It is stated that, besides participation by citizens in the regulatory process, accessibility of standards for regulatees as well as the accessibility of dispute resolution mechanisms (access to justice as it were) must be ensured, as well as adequate enforcement structures.[248]

3.3.6 CONCLUSION

The foregoing implicates that within the European Union, some assumptions can be made regarding the quality of regulation in general – which is characterized by an increasing role of

[241] Ibidem, section 21.
[242] European Commission 2017a, section 3.1, p. 109-111.
[243] De Cock Buning & Senden 2020, p. 22.
[244] See De Cock Buning & Senden 2020, p. 24.
[245] See also chapter 3.3.
[246] See De Cock Buning & Senden 2020, p. 24.
[247] Ibidem, p. 26-27.
[248] Ibidem, p. 27.

private actors in the regulatory process. I will use these assumptions in the third part of this study, more specifically in Chapter 9, in relation with the conclusions of the second part to the extent that there are certain steps that can be taken through regulation in order to better facilitate innovation, and the acceptance thereof. Concerning the regulatory process itself, the following factors must be taken into account as a result of the Better Regulation initiative: forward planning and political validation; stakeholder consultation; evaluation and fitness checks; impact assessments; quality control; and implementation support and monitoring, which I will further refer to as the "better regulation process". Within the better regulation process, it must be ensured that there is an adequate legislative mandate; the regulator can be held accountable for the regulatory activities it issues; stakeholder participation is characterised by principles of equality, fairness and consistency of treatment; and that rules are based on expert judgment. In order to facilitate acceptance of the results of the regulatory process, the perspective of the *regulatees* needs to be taken into account. Also here democratic legitimacy of the regulator is important, as well as and effectiveness of the regime, i.e. that policy objectives are achieved. Furthermore access to the norms at hand and dispute resolution mechanisms by the *regulatees*, is a crucial factors for trust in and – thus – acceptance of regulatory regimes.

Besides these general assumptions on the quality of regulation, certain factors in regulation can be identified that specifically regard innovation – and acceptance of innovation. Those factors are addressed in the following sections.

3.4 FACTORS IN REGULATION INFLUENCING INNOVATION

3.4.1 INTRODUCTION

The interplays between regulation (or to be more accurate: regulatory frameworks) and technological innovation are increasingly researched, as the latter has become a more important contributor to growth and welfare in the past decades, and the quality of regulation has been an issue receiving increasing attention during approximately the same period.[249] Whereas answers to this question originally surfaced from socio-economic literature,[250] more attention has been given to this subject in academic literature on law and regulation in recent years.[251] Pelkmans & Renda for example have dedicated a Special Report on this subject,[252] and provide a method for the analysis of influence of regulation on innovation, which they have based on extensive literature- and case studies.[253] Ranchordás researches in her dissertation whether or not *sunset clauses* and *experimental legislation* could work for innovation, which she bases on, amongst many other things, a qualitative analysis of academic literature on the regulation of innovation.[254] Whereas there is a certain overlap in the research carried out by Pelkmans & Renda and Ranchordás, there are a number of similarities and some differences in the outcomes thereof amongst them.

Both authors acknowledge that there is an important relationship between regulation and innovation, and that regulation is often seen as implicating hurdles to innovation in literature.[255] They equally find that regulation can also be a significant stimulus for innovation.[256] Ranchordás and Pelkmans & Renda acknowledge that it is advisable to structurally review the influence of regulation on innovation. Pelkmans & Renda indicate that "there is ample potential for fostering

[249] See *inter alia* sections 3.3.4-3.3.6.
[250] See for instance the works of Ashford, Ayers & Stone 1985; Fagerberg & Mowery 2009; Stewart 2010.
[251] See Ranchordás 2014; Pelkmans & Renda 2014 and Blind 2012. See also Hoffmann-Riem 2006, p. 256, footnote 5 for some German sources on this subject.
[252] The CEPS Special Report was adopted by the European Commission in the general strategy on innovation and better regulation, and the REFIT-programme, see European Commission 2016, p.7.
[253] Pelkmans & Renda 2014, p. 1-14.
[254] Ranchordás 2014, p. 28, 58.
[255] Pelkmans & Renda 2014, p. 1; Ranchordás 2014, p. 130-132.
[256] Pelkmans & Renda 2014, p. 7; Ranchordás 2014, p. 133, 160. Ranchordás furthermore addresses a normative aspect: "law should facilitate and support innovations that are relevant for society, instead of hindering them". She paraphrases Wolfgang Hoffmann-Riem, who argues that law has at least two roles to play in relation to innovation. Law should actively and passively stimulate innovation (*Innovationsoffenheit*, "Innovation-openness"), and should provide a framework for the responsible introduction of innovation in society, meaning that it must be assessed ex ante what the consequences of certain innovations may be in terms of impact, potential risks and fundamental rights (*Innovationsverantwortung*, "Innovation-accountability"). See Ranchordás p. 145-146; see also Hoffman-Riem 2006. Furthermore, it is suggested that *Innovationsverantwortung* comprises that legal research on innovation "should be guided not only by the goal of promoting innovation, but also the need to guarantee that innovation is developed in a 'legally sensible way'" (p. 146).

innovation by reviewing the EU regulatory *acquis*",[257] and that "impacts [of regulatory/policy options, *RWdB*] on innovation should be put at the core of the EU impact assessment methodology", [258] to be evaluated both ex ante and ex post. Both Pelkmans & Renda and Ranchordás primarily focus on the *innovators perspective*. This has been indicated as the capacity, opportunity and willingness of organisations to innovate: to develop and to bring to market new products or services.[259] They do not explicitly address the *consumers perspective*: the perspective that takes into account that innovation requires adoption of the newly developed products or services by consumers in order to be successful. In the following sections, I will address both perspectives, starting with a short overview of the aforementioned contributions on the *innovators perspective* in section 3.4.2. The *consumers perspective* is elaborated in section 3.4.3.[260]

Before I do so, a proviso is in order. The *factors* that are identified hereafter, form – at best – a theoretical model in order to assess potential interplays between regulation and innovation. I do not claim however that those factors are the only aspects that can be derived from regulation that may influence regulation and the acceptance thereof by citizens: my assessment of those factors is limited to the boundaries of this research. Moreover, to the extent that the factors implicate certain impact on the behaviour of innovators or citizens, it must be noted that those implications cannot be taken to hold "absolute" values. The potential behaviour of innovators and citizens referred to hereafter is furthermore taken to be "rational" and "uniform" when confronted with the respective factors: I do not claim that the *actual* behaviour cannot significantly differ from what is modelled in the factors in the following sections.

3.4.2 THE INNOVATORS PERSPECTIVE

3.4.2.1 INTRODUCTION

In the review of the works by Pelkmans & Renda and Ranchordás, I found that they indicate several elements that can be enshrined in regulation that may have impact on the development and bringing to market of novel technology. Although 'labelled' differently in both contributions, the authors describe, in my opinion, to a certain extent comparable mechanisms in that respect. From these contributions, I have distilled three factors: *stringency, flexibility* and *legal (un)certainty* that contain those mechanisms, as I introduce below and elaborate in the following sections.

[257] Pelkmans & Renda 2014, abstract.
[258] Ibid, p. 27.
[259] See section 3.2.
[260] As I did not find any "overarching" studies regarding the interplays between regulation and the *consumers perspective*, I have investigated separate contributions in social and economic studies.

Pelkmans & Renda identify, with Stewart,[261] three relevant factors: *flexibility*, *information* and *stringency*. *Flexibility* is described as "the number of implementation paths firms have available for compliance".[262] *Information* describes "whether a regulation promotes more or less complete information in the market".[263] *Stringency* "measures the degree to which a regulation requires compliance innovation and imposes a compliance burden on a firm, industry or market".[264] To the aforementioned categories, *uncertainty* on the "content and scope of future […] policies" is added.[265] Ranchordás follows a slightly different approach. She also uses *inter alia* the concepts of *stringency,* as permanent and stringent, 'rigid' regulation,[266] and *flexibility,* which she sees as both the number of implementation paths as described by Pelkmans & Renda,[267] and *adaptability*: "the ability […] to rapidly react to the new changes underlying innovation…".[268] However, she sees them as opposites, rather than as distinct factors. She uses both concepts (flexibility and stringency) in relation to *legal uncertainty*, which she indicates to be of major importance for innovation. [269] Ranchordás remarks that "most barriers surrounding innovation concern uncertainty regarding opportunities, constraints and excessive regulatory burdens".[270] In that, it must be noted that Ranchordás explicitly emphasizes the importance of *legal (un)certainty* more than Pelkmans & Renda do in their contribution. However, Pelkmans & Renda do indicate that uncertainty regarding scope and contents of policy plays a role, and it can furthermore be argued, that *stringency* and *flexibility* can only then be measured when there is a certain amount of predictability and stability regarding the material contents of regulation, and they also observe that "the absence of reasonable stability or certainty in the regulatory framework can significantly hinder innovation".[271]

Ranchordás occasionally mentions *information*, although she does not elaborate this factor, which has been acknowledged by Pelkmans & Renda and Stewart. Whereas neither Pelkmans & Renda nor Ranchodás provide detailed information on *information*, Stewart does. Stewart recognizes that regulation which is aimed at information asymmetries between *producers* on the one hand and *consumers* at the other hand, this may at the same time act as a compliance burden and as a compliance value for producers.[272] When for example certain drugs need to be preapproved by an

[261] Stewart 2010, p. 7.
[262] Pelkmans & Renda 2014, p. 5.
[263] Ibidem.
[264] Ibidem.
[265] Ibidem. They also add *timing,* "the amount of time that a regulation gives to the targeted stakeholders for compliance…" on p. 12, which will be considered under *stringency* below.
[266] Ranchordás 2014, p. 142.
[267] Ranchordás 2014, p. 132, 134.
[268] Ranchordás 2014, p. 143.
[269] Ibidem, and 166 – 173.
[270] Ranchordás 2014, p. 160.
[271] Pelkmans & Renda 2014, p. 12.
[272] Stewart 2010, p. 6.

authority such as the (American) Food and Drugs Administration, this may serve as an upfront compliance cost: it is costly for firms to endure the preapproval procedure. When the respective drugs however are approved and get certified, this informs consumers of the quality, which may increase the 'return on investment' for the manufacturers. The *information* concept elaborated by Stewart thus comprises of two components, which can be related to the respective two perspectives indicated above. Firstly, *information* may be viewed through the *innovators perspective* as 'compliance burden', or 'compliance value'[273] (with a short-term and a long-term aspect to it). Secondly, *information* can be related to the concept of *risk* and *trust*, which is elaborated below as forming part of the *consumers perspective*.

In this study, I will take the factors that have been identified by Pelkmans & Renda (who build upon the work of Stewart), Ranchordás and the sources that have been indicated by these authors as a point of departure: I will compare these factors as presented by the different authors as far that is possible from a legal academic background. As shortly introduced above, the factors *stringency, flexibility* and *legal (un)certainty* are identified by Pelkmans & Renda, Stewart and Ranchordás as important major anchor points in their research on the interplays between regulation and innovation. Therefore, I will also use these respective factors as main focus points in my study on the *innovators perspective*. The factor *information* is mentioned, but not elaborated by Ranchordás nor Pelkmans & Renda. It can be seen, from the *innovators perspective*, to be incorporated under *stringency.* For the reasons shortly mentioned above, I have chosen not to mention *information* as a separate factor in this research, but to integrate it in the analysis of *stringency, risk* and *trust*.

Below, *legal certainty* is addressed first in section 3.4.2.2, after which *stringency* and *flexibility* are discussed in sections 3.4.2.3 and 3.4.2.4 respectively. To conclude the analysis of the *factors*, section 3.4.2.5 ends with a cross-examination of the relationships between the three.

3.4.2.2 LEGAL CERTAINTY

3.4.2.2.1 General remarks

The concept of *legal certainty* holds that law must be precisely formulated, unambiguous and predictable for all of those who are subjected to it, in a stable and durable way.[274] Legal certainty can be associated with sustainable rules and the stability principle, which holds that these rules

[273] Assuming that this is information which the consumers appreciate in some way, and value the certified product over non-certified alternatives. See Stewart 2010, p. 6.
[274] See Raitio 2003, p. 16; Ayhan 2010 p. 151; Ranchordás 2014, p. 166-169; Hoffmann-Riem 2006, p. 258. See also Kulk 2018, p. 51-52.

should not be altered arbitrarily by lawmakers 'during the game' if that is not absolutely necessary.[275] In that, it is stated to be a cornerstone of the *rechtsstaat,*[276] and one of the materializations of the *rule of law* principle.[277] Legal certainty can be opposed to legal *un*certainty. The potential impacts of the latter are indicated by D'Amato. He has, based on economic analysis, stated that "uncertain law may deter activity that the state wants to encourage".[278] Moreover, D'Amato argues that it is undesirable that uncertain rules "leave persons unsure of their entitlements while affording unfettered discretion to official decisionmakers".[279] Some uncertainty may be however not necessarily 'bad' for innovation: it may provide innovators with some freedom regarding the ways they conduct their innovative activities when for instance standards for certain new technology are not (yet) in place – and there are to that end no compliance costs to be taken into account by the innovators.[280] However, when for example regulatory frameworks are subject to "constant and sudden revisions",[281] which is the cause of the uncertainty, this may have a negative impact on innovation.[282] There can also be too much legal certainty: very stringent rules, such as certain prescriptive standards, or other rules which specifically see to certain forms of 'older' technology, which have not evolved with technological developments may impose unnecessary burdens for innovators, as "they limit the freedom of choice to seek the most efficient form of compliance".[283]

Summarizing a number of contributions in academic literature and decisions of the Court of Justice of the European Union, Maxeiner distils five elements that follow from the principle of legal certainty:

> "(1) laws and decisions must be made public; [… they …] (2) must be definite and clear; (3) decisions of courts must be binding; (4) limitations on retroactivity of laws and decisions must be imposed; and (5) legitimate expectations must be protected".[284]

In the elements identified above, another distinction can be made: between formal and material legal certainty.[285] *Formal* legal certainty sees to the legibility, clarity and public availability of rules and decisions. *Material* legal certainty comprises *stability* and *predictability* of the contents of rules and decisions. For distilling factors in regulation that may influence innovation in terms of

[275] See also Maxeiner 2008, p. 30, Ranchordás 2014, p. 163.
[276] See also Ranchordás 2014, p. 167.
[277] Maxeiner 2008, p. 28.
[278] D'Amato 2010, p. 5.
[279] Ibidem.
[280] See for example Ranchordás 2014, p. 154.
[281] Ibidem.
[282] Ibidem, and Pelkmans & Renda 2014, p. 12; Stewart 2010, p. 4.
[283] Ranchordás 2014, p. 155.
[284] Maxeiner 2008, p. 32.
[285] See Ranchordás 2014, p. 168.

this study, it is especially relevant to elaborate a bit further upon the *material* characteristics of legal certainty that see to stability and predictability of certain rules. As the research question in this study regarding the *factors* is of a material, qualitative, nature, I have chosen to focus on *material* legal certainty.

Predictability and stability lie in line with each other, although they are not the same. *Predictability* entails that legal rules and judges' decisions must meet the reasonably foreseeable and calculable expectations of actors to whom these apply. Persons (both legal and natural) must thus be able to plan or adjust their behaviour according to clear and unambiguous material norms that apply. For example, one should be able to know which responsibilities he has in order to prevent damage and liability based on tort-rules, and what the consequences may be if he fails to comply with these. When a company processes personal data of citizens, it must be clear which legal framework regulates those processing activities, and what the (financial) risks comprise when these rules are not met.

The principle of predictability also entails that the material norms do not deviate over short periods of time: a prediction must be valid as long as possible. This means that rule makers (either the state, other regulatory actors or even judges), should refrain from material inconstancy. Sustainable *predictability* can be achieved through the *stability* of rules. Once a rule has taken shape, it is beneficial in terms of predictability that it stays unchanged for as long as possible. However, it has shown that rule makers have not always been able to draft regulation that stays fit through times of (technological or societal) change. Especially when technological innovation occurs, it happens that rules become outdated – and do not longer serve their initial purposes, and that persons to whom these apply are no longer able to predict the outcomes. In those cases, the principle of *stability* collides with *predictability* – as the consequences of certain behaviour can no longer actually be foretold. As acknowledged in literature, when societal or technological change leads to unpredictability, the *stability* principle should however not stand in the way of alteration of the respective rule,[286] taking into account the underlying values of that rule. In that, *legal certainty* benefits from flexible rules, that are responsive to the aforementioned changes, although not without losing the purposes of the respective rules out of sight: the underlying values must stay protected at all times, as I will further elaborate in the next sections.[287]

[286] See Ranchordás 2014, p. 170, and her reference to Loving, P.E., "The Justice of Certainty", *Oregon Law Review* 1994, no. 73, p. 747.
[287] See Ranchordás 2014, p. 171-173.

In its Proposed AIR,[288] The EC highlights the importance of *legal certainty* for the creation of an innovation-friendly environment. One of the objectives is to "ensure legal certainty to facilitate investment and innovation in AI".[289] It is furthermore underscored that in order to adequately protect safety, compliance with norms and standards as well as to protect the fundamental rights of citizens, it is necessary that "[p]redictable, proportionate and clear obligations are placed on providers and users of those [AI-, *RWdB*] systems".[290]

3.4.2.2.2 Technology neutrality and legal certainty

Regulators tend to respond to certain technological developments (after denying the very developments or the significance thereof) primarily with regulation addressing that specific technology in order to govern certain outcomes of that technology. De Cock Buning illustrates that the more a rule is drafted in a technology-specific way, the shorter it may last due to technological innovation on the respective area.[291] When technological innovation advances, rules applicable to specific 'older' technology, become outdated and, among other things, *legal certainty* requires the drafting of new rules – governing the new results thereof.[292] Moreover, De Cock Buning illustrates positive effects of technology neutral regulation and innovation: technology-neutral rules with a focus on the underlying values to be protected, in copyright regimes for example, have proven to be perfectly capable of handling technological innovations such as photography, gramophone and computer programs.[293] Contrarily, De Cock Buning also observes that technology specific rules tend to trouble the view of judges on underlying values that are to be protected.[294]

Regulators have also adopted the idea that regulation should be as technology-independent as possible. As Koops shows, this principle is embraced by regulators around the globe, varying from for instance the governments of the Netherlands and England, to the European Union the United States and the G8.[295] Koops furthermore specifies – in line with the views of De Cock Buning and

---

[288] See for the introduction and backgrounds of the Proposed Regulation on a European Approach for Artificial Intelligence sections 2.2 and 3.2.
[289] Proposed AIR, p. 3.
[290] Ibidem.
[291] De Cock Buning 1998, p. 221-222; Ranchordás 2014, p. 171 – 173.
[292] Ibidem, p. 223. De Cock Buning furthermore observes that the flexibility of a regulatory system may decrease when components of that system (i.e. the material rules at hand) are drafted in a technology-specific way, since a technology-specific focus (inducing a multitude of technology-specific rules) tends to trouble the view on, or interpretation of the underlying norms that should be protected.
[293] Ibidem, p. 224, 228.
[294] De Cock Buning 1998, p. 223.
[295] Koops 2006, p. 1-2, referring to *inter alia* the Dutch policy memorandum Legislation for the Electronic Highways (1998, p. 12); UK E-Policy Principles (no. 5, p. 1), available via http://webarchive.nationalarchives.gov.uk/20040722012403/http://e-government.cabinetoffice.gov.uk/assetRoot/04/00/60/79/04006079.pdf; the US Framework for Global Electronic Commerce of 1997; the EU Green Paper on European Union Consumer Protection, COM(2001) 531 Final; and in a similar vein the more recent example the Communication on European Strategy for a Better Internet for Children COM(2012) 0196 Final.

Heldeweg, Pelkmans & Renda – that the neutrality in regulation should merely be on the results, or its effects, rather than on the technological means themselves,[296] although law must not become too abstract as this would in turn detriment *legal certainty*.[297]

> A clear example of technology-specific regulation which have become ineffective, and causing uncertainty due to technological progress includes the following. The Constitution of The Netherlands stipulates in article 13(1) that "The privacy of correspondence [a rather broad translation of the original wordings "briefgeheim", which may better be translated as "the privacy of letters", *RWdB*] shall not be violated except in the cases laid down by Act of Parliament, by order of the courts."[298] Article 13(2) reads: "The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament". Whereas the purpose of this rule is to protect the privacy of citizens through any means of communication, the current formulation of this rule is a product of the 1980's, pointing to the technology which was available then – obviously without having in mind the rapid technological developments of the '90's and onwards. Strictly speaking, the current redaction of article 13 of the Constitution does no fits its purpose, for it may not be applicable to newer forms of communication such as e-mail, Whatsapp and Facebook-messaging.

In a similar vein, Heldeweg also acknowledges a negative effect of technology-specific regulation on *legal certainty* and innovation. When rules are drafted in a too technology-specific way, this could for instance, in a dynamic environment (i.e. where much innovation occurs) induce uncertainties as to *inter alia* the scope and applicability thereof,[299] and thus induce hurdles for the development and use of innovative technology.[300] Pelkmans & Renda also illustrate that new regulatory requirements must be sufficiently distant from the existing technology,[301] and that the outcomes should be "specified in a technology-neutral, non-prescriptive way" in order to render such requirements effective.[302]

Taking the considerations above into account, one may assume that *technology neutrality* could serve *legal certainty*. While on the shorter term, a technology-specific, (non-neutral) rule may

---

[296] Koops 2006, p. 6.
[297] Ibidem, p. 27.
[298] I used the official translation of the Constitution (Grondwet), available through https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brochures/2008/10/20/the-constitution-of-the-kingdom-of-the-netherlands-2008/07br2008g109.pdf. The example of article 13 is also used by Koops 2006, p. 15-16.
[299] See Heldeweg 2009, p. 93, 95 and 158.
[300] Ibidem, p. 36.
[301] Pelkmans & Renda 2014, p. 11.
[302] Ibidem, p. 12.

provide clear norms for the behaviour of addressees, these effects die out as soon as the respective technology advances away from the technology that was the primary object of that rule on the longer term.[303] While the rule may remain *stable*, the *predictability* of the outcomes of the application of that rule to new technology are likely to decrease.

3.4.2.2.3 Legal certainty and innovation

Innovation can impact legal certainty, as was illustrated above. The relationship between certainty and innovation is however broader: *legal certainty* – or negatively formulated: *legal uncertainty* – may impact the course of innovation as well. D'Amato formulated in 1983 that *legal certainty* is said to be "necessary for capitalist progress",[304] and thus for innovation. A lack of certainty, more specifically *predictability* may be an obstacle to innovation, or as Ranchordás puts it (with D'Amato): "Uncertain rules have the perverse effects of leaving private actors unsure about their rights and duties while affording unconstrained discretion to official decision makers".[305] It can be argued that innovators will refrain from investing in certain technological innovations if it is unsure whether or not these investments can be earned back, or worse, when these innovations may lead to higher costs or risks, for instance in terms of the aforementioned rights and duties than the initial investments would justify.[306] Pelkmans & Renda also acknowledge a link between legal uncertainty and the incentive for innovators to invest in R&D activities, and conclude that "the absence of reasonable stability or certainty in the regulatory framework can significantly hinder innovation",[307] which they base on a case study in which uncertainty of EU competition rules is established, and an effect is sketched on the resulting unpredictability for companies with a dominant market position. They state that this could lead to disincentives to innovate.[308]

Based on the considerations above, it seems fair to argue that when the legal consequences of specific behaviour (i.e. investing in the development and deployment of innovative technology by the industry) cannot be reasonably foreseen or calculated, this may, among many other things, be

[303] See also Kulk 2018, p. 35; De Cock Buning 1998 p. 221-222.
[304] D'Amato 1983, p. 3, paraphrasing Weber, M., *Economy & Society: An Outline of Interpretive Sociology,* Bedminster Press 1968, p. 883.
[305] Ranchordás 2014, p. 173, referring to D'Amato 1983, p. 3. See also Heldeweg 2009, p. 93, 95 and 158.
[306] See also Ranchordás 2014, p. 173, paraphrasing Weber, M. *Economy and Society*, University of California Press 1978, p. 883: "According to Max Weber, legal certainty is fundamental to capitalism, since without legal security the investment of capital shall be reduced". Pelkmans & Renda indicate that uncertainty may also be a driver for innovation, as companies may innovate in such ways that regulation can be avoided or anticipated. (p. 12 and 18.) With Ashford, Ayers & Stone 1985 (p. 426), they illustrate a spectrum between too much uncertainty, which "may cause industry inaction" vis-à-vis too much certainty, which "will stimulate only minimum compliance technology" (p.12).
[307] Pelkmans & Renda 2014, p. 12.
[308] Pelkmans & Renda 2014, p. 22.

of consideration to innovators when making business decisions regarding investments in the development or deployment of certain technology.

In this research, it will be investigated what the potential influence on legal certainty for innovators may be, when the regulatory frameworks on extra-contractual liability and personal data protection are confronted with (fully) autonomous vehicles, and what this could in turn entail for innovation. A case study is used in order to illustrate the possible (un)certain consequences of the application of extra-contractual liability and privacy regulation on fully autonomous vehicles, and what this could implicate for innovation. The case study is elaborated below in section 3.5.

3.4.2.3 STRINGENCY

Stringency, which relates to the difficulty of, and costs related to comply with certain regulation, is seen by Ashford, Ayers & Stone and Stewart as "the most important factor influencing technological innovation".[309] Pelkmans & Renda indicate that "a regulation is judged to be stringent if firms need to significantly change their behaviour or develop new technology in order to comply with regulation", which thus leads to significant costs.[310]

Ashford, Ayers & Stone advocate *stringent regulation*, as this will often be necessary to impose regulation on industries in order to help achieving societal goals concerning for instance health, safety and environment, through innovative technology.[311] Regulation should, according to them, be as stringent as possible in order to achieve maximum results.[312] Thus, regulation can be a driver for innovation – in order to comply with the respective rules. They furthermore mention that innovation-inducing rules may for example require industry to demonstrate product safety or efficacy prior to and/or after marketing; to control the production technology and to control the by-products thereof such as emissions, effluents and wastes,[313] or to reduce *information asymmetries.*[314] New, stringent rules would create business opportunities for so-called 'first movers' over slower firms: first movers can commercially exploit the fact that they were compliant earlier than others.[315]

---

[309] Ashford, Ayers & Stone 1985, p. 426 as cited in Stewart 2010, p. 4.
[310] Pelkmans & Renda 2014, p. 11.
[311] Ashford, Ayers & Stone 1985, p. 419-421.
[312] Ibidem, p. 463-464.
[313] Ibidem, p. 425.
[314] See Stewart 2010, p. 6-7; Pelkmans & Renda 2014, p. 5; Ranchordás 2014, p. 84. When for example certain drugs need to be preapproved by the Food and Drugs Administration, this may serve as an upfront compliance cost: it is costly for firms to endure the preapproval procedure. When the respective drugs however are approved and get a certificate, which informs consumers of the quality, this may increase the 'return on investment'.
[315] See Ranchordás 2014, p. 139, referring to Ashford, N.A., "Environmental Regulation, globalization and innovation", in: Gallagher, K.P. (ed.), *Handbook on Trade and the Environment*, Cheltenham: Edward Elgar Publishing 2009, p. 296-307.

However, the *stringency* in regulation Ashford, Ayers & Stone advocate, will always require a significant change in behaviour of the regulated industry, and will often not allow for a 'margin of appreciation' on the routes to follow in order to become compliant with the rules. This in turn would lead to high compliance costs. *Stringency* thus implicates a high burden (in terms of costs and difficulty) for innovators to comply with regulation.[316]

As Pelkmans & Renda observe, those who are not able to comply (in time, or at all), might go out of business, and "the innovation-enhancing potential of stringent rules is replaced by a discouraging effect on existing firms".[317] At the same time, it would be difficult for newcomers to enter into a stringently regulated market, as that would require heavy upfront compliance investments. A similar suggestion is made by Blind in his quantitative assessment for OECD-countries concerning *inter alia* liability rules, who illustrates that when liability regulation is too strict, the industry could refrain from introducing new technology in the market "because the risks are high, the expected revenues decrease, and the users of the products reduce their self-protection efforts".[318] Other effects of stringent regulation, may be that the addressees thereof try to avoid or circumvent the respective rules by for instance using new means that have not been addressed by the regulator,[319] or that they will never go beyond the minimum-levels of compliance that are required. Furthermore, as Ranchordás illustrates, stringent regulation often is technology-specific, and will become non-effective as soon as the state of the technology exceeds the levels that have been regulated, as the respective regulation will often not be able to "respond to the inherent complexity and uncertainty of innovation".[320]

In sum, *stringency* is thus not necessarily 'bad': high compliance burdens may be justified in order to achieve for instance societal, environmental or social goals which may not be achievable without these rules. However, there could be a problem if it is *inter alia* uncertain whether or not the goals set forth by regulators are likely to be met. That could for instance be the case when a stringent rule is technology specific, or when it is so strict that innovators try to circumvent the rule or would only try to achieve minimum-compliance and the rule does not invite to innovate beyond the compliance minima, or when for other reasons the rule may not lead to the required outcomes.

[316] Pelkmans & Renda 2014, p. 11; Stewart 2010, p. 4 and Ashford, Ayers & Stone 1985, p. 426.
[317] Pelkmans & Renda 2014, p. 11.
[318] Blind 2012a, p. 394. On the other hand, as Blind also indicates on the basis of several empirical studies, stringency in product liability rules, is observed to have a positive effect on consumer acceptance. The net-results seem to be "ambivalent, but slightly positive", as Blind states on p. 395.
[319] See for example Stewart 2010, p. 2. This would especially likely to be the case if the respective stringent rules are also technology-specific rather than technology-neutral.
[320] Ranchordás 2014, p. 142.

> In the Proposed AIR, the European Commission seeks to enhance citizen's trust in AI-based products and services. To that end, the EC has drafted several 'new' rules to be taken account of by AI-innovators, in order to *inter alia* protect the fundamental rights of AI-users, and to make sure that among other things (safety) standards as well as fundamental rights including privacy are complied with. The EC does observe that new rules may influence innovation, and holds that it's regulatory approach should be "limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market".[321] In that, it is observed that the new regulation may implicate *stringency* – which the Commission seeks to minimise. The EC proposes to regulate *inter alia* "principle based requirements" rather than providing technology-specific rules, which should be able to be flexible "as technology evolves and new concerning situations emerge".[322]

In the light of this study, it is relevant to assess the extent to which current personal data protection regulation and extra-contractual liability regulation are *stringent*, in view of the technological developments in AV technology. Furthermore, it will be analysed – to the extent possible from a legal academic perspective – how the identified stringency may relate to the goals (or functions) that have been indicated by the regulators.[323] Also here, a case study will be used to illustrate the *regulatory stringency* for the regulated actors to either comply with the rules (innovators), or to have their rights enforced against other actors (citizens).

3.4.2.4 FLEXIBILITY

At least two types of *flexibility* can be identified in regulation. Firstly, *flexibility* may see to the "number of implementation paths firms have available for compliance".[324] In that sense, it may illustrate the amount of freedom for innovators to determine how they are going to reach the goals that the regulator wants them to achieve. If the options for compliance are limited, this would entail higher costs or organisational difficulties for innovators, which in turn leads to less available resources for innovation.[325] Essentially, the question is whether or not *standards* are to be preferred over *rules*. *Rules* are defined in literature as "definitive criteri[a] for the resolution of a legal issue",[326] and provide high degrees of specificity of the behaviour to which the respective norms see. Legislators of rules thus created specific *ex ante* criteria, leaving – in theory – little

[321] Proposed AIR, p. 4.
[322] Ibidem.
[323] See section 4.1.2 on the functions of exra-contractual liability regulation and section 5.1.3 on the functions of personal data protection regulation.
[324] Pelkmans & Renda 2014, p. 5, citing Stewart 2010, p. 3.
[325] See Stewart 2010, p. 5.
[326] Luppi & Parisi 2017, p. 43.

margin of appreciation to judges. *Standards* provide a higher margin of appreciation to judge certain behaviour *ex post* than *rules*, and are of a more flexible nature.[327]

In terms of stimulating innovation, it would be preferable to for innovators to have *standards* in place that allow some room in order to achieve the required results.[328] According to Pelkmans & Renda, flexible, performance- or outcome-based standards are to be preferred over rules that for instance prescribe "specific materials or technology requirements", since the latter "give no market prospect to those that want to experiment with alternative solutions".[329] Stewart furthermore distinguishes between *behavioural obligations*, for instance the obligation of a firm to "lower its price output" or "to reduce pollution emissions",[330] and *incentive based regulations*. The latter may hold that certain behaviour is incentivised for instance by granting tax profits or subsidies. As an example of *incentive based regulation* that is *flexible*, Stewart mentions systems of tradeable emission schemes: "whereby the total emissions are capped, the total allowed emissions are allocated among firms, and then those firms that lower emissions below their allocation – typically those with lowest reduction costs – can trade their permits to those who exceed their allocation – those with higher reduction costs".[331] It is seen to be overall beneficial for reaching the respective societal goals, to allow companies to choose the means that suit their business best. This may be achieved by regulating through *open norms*,[332] or *performance/*[333] *outcome based standards*.[334] It is thus important that the *results to be attained* are regulated (which may well be ambitious), and that the *ways of attaining* these (i.e. the paths towards compliance or implementation), are left to the regulated actors.[335]

A second form of *flexibility* sees to the adaptable nature of the respective regulation. Ranchordás describes this as "the ability of regulation to react to new changes underlying innovation and the acquisition of more information regarding the phenomenon".[336] Here too, *standards* would provide more *adaptability* than *rules* could. Adaptability could help preventing that certain rules become outdated as technology advances. She mentions the ALARA-example. The ALARA-principle stipulates that nuclear emissions should be "As Low As Reasonably Achievable". This is a dynamical level, and relates to the current state of the art in the technology, and becomes stricter

[327] Ibidem.
[328] See also Van der Heijden 2017, p. 727-728; and Gunningham & Sinclair 2017, p. 711.
[329] Pelkmans & Renda, p. 12.
[330] Stewart 2010, p. 5.
[331] Stewart 2010, p. 5.
[332] Ranchordás 2014, p. 144.
[333] Stewart 2010, p. 5.
[334] Pelkmans & Renda 2014, p. 12.
[335] Stewart 2010, p. 5 & 23.
[336] Ranchordás 2014, p. 143.

over time.[337] A comparable example is given by Stewart, who points at the US Clean Air Act: this requires "firms to use "best available technology" to control pollutant emissions from plants or vehicles".[338] Also here, innovating firms are in principle free to choose their ways of compliance, although there is a 'moving target' which is set by the regulator.

In this study, I will assess the *flexibility* of the regulatory frameworks on extra-contractual liability and personal data protection. The component of *flexibility* that sees to the level of manoeuvring space of innovators for compliance, the assessment will comprise of the analysis of the freedom of innovators regarding the diversity of the possible implementation paths that are available for them. In order to establish *adaptability* of certain regulation, inter alia *technology neutrality* may be used here again as an indicator: a higher level of technology specificity could suggest that the *adaptability* is limited to the specified technology. Less technology specificity could suggest the opposite, and indicate a higher level of *adaptability*.

> Both forms of *flexibility* are taken account of in the Proposed AIR. Regarding the *implementation paths*, it is worth mentioning that the proposed obligations are principle-based (thus based on standards, rather than rules),[339] which can be tailored to a respective system and/or producer.[340] Regarding the *adaptability* it can be observed that for instance the definitions seem not to be tied to specific forms of technology, but rather address the outcomes of technological development processes. Insofar as the Proposed AIR relates to existing or new forms of technology, it contains an updating mechanism.[341]

3.4.2.5 *RELATIONSHIPS BETWEEN* LEGAL CERTAINTY, STRINGENCY *AND* FLEXIBILITY

There are several reciprocal influences of, and overlaps between the factors *legal certainty*, *stringency* and *flexibility* which have to be taken into account when assessing the possible influence of the respective factors on innovation. Some of these have already be indicated above, and will be elaborated a bit further in the following sections.

---

[337] Ibidem, p. 143. See also Stewart 2010, p. 5, using a similar example: the US Clean Air Act, which requires companies to use "best available technology".
[338] Stewart 2010, p. 5.
[339] Proposed AIR, p. 3.
[340] See for instance article 9 Proposed AIR, regarding the "Risk management system" to be implemented by a provider of a "high-risk AI system".
[341] An AI system is for instance defined in article 3(1) of the Proposed AIR as "software that is developed with or more techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with." Annex I, which has not been attached to the Proposed AIR, might refer to specific technology. However, this Annex I can (easily) be updated on the basis of article 4 Proposed AIR by the Commission.

When looking at *flexibility* for example, it must be noted that very 'open' or 'vague' norms, are highly flexible by nature, but may at the same time sometimes entail little *predictability*. When for example a rule holds that one needs perform a "personal data impact assessment" when a certain type of personal data processing "is likely to result in a high risk to the rights and freedoms of natural persons",[342] but does not clearly explicate what these "high risks" may constitute, or when "it is likely" that these high risks exist, this would provide little guidance to verify that the correct actions have been taken by the addressees of the rule when they decide whether or not to perform a personal data impact assessment. On the other hand, when the underlying values are clear (such as in the aforementioned example: protecting the informational privacy of citizens by *inter alia* taking adequate measures into account), this may provide at least tome guidance to the norm addressees. Furthermore, it may benefit *stability* when well-drafted norms are *flexible*, as technological progress would in that case not require constant rule changing.

A relationship between *flexibility* and *stringency* is illustrated by Ashford, Ayers & Stone.[343] The American Occupational Safety and Health Administration (OSHA) adopted at a certain point a standard for maximum exposure of 2 fiber/cc for asbestos workers, instead of a 0.1 fiber/cc standard, which was the lowest level detectable. The failure to adopt the more stringent standard, resulted in a *disincentive* for innovation by the industry, as it was rather easy to comply with the 2 fiber/cc norm.

Also, relationships can be found between *stringency* and *legal certainty*. Take for instance the rule that "every moving vehicle or combination of vehicles shall have a driver",[344] and that "every driver shall at all times be able to control his vehicle or to guide his animals".[345] These rules (which are currently being reconsidered)[346] do not leave much room for interpretation and can be considered to entail a high level of *legal certainty*. However, these are at the same time very *stringent* to those who want to develop and deploy autonomous vehicles: it will not only be difficult to comply, but rather technically impossible. Furthermore, this example also shows a lack of *flexibility* and *technology neutrality* in the respective rules: it is only flexible to the extent that one would be able to control his vehicle or animals. Should innovators want to innovate beyond this state of the technological art, the applicable regulation virtually prohibits them to do so.

[342] Article 35 GDPR.
[343] Ashford, Ayers & Stone 1985, p. 464.
[344] Article 8(1) Vienna Convention on Road Traffic 1986 (hereinafter: Vienna Convention).
[345] Article 8(5) Vienna Convention.
[346] These rules are currently being updated in order to facilitate innovation in the field of autonomous vehicles: https://www.unece.org/info/media/presscurrent-press-h/transport/2016/unece-paves-the-way-for-automated-driving-by-updating-un-international-convention/doc.html

The examples above contribute to the idea that it would not be sufficient to assess the identified factors in isolation: in order to be able to make assumptions on the possible relationships between the factors and innovation, it is necessary to take into account the possible relationships between the factors themselves.

3.4.3 THE CONSUMERS PERSPECTIVE

3.4.3.1 INTRODUCTION

Much has been written on *acceptance* and *adoption* of technological innovation by consumers within *inter alia* social and economic academic disciplines. A number of these contributions suggest a relationship between (the application of) regulation and acceptance or adoption of technology by consumers, as will be further introduced below. This is, as indicated above, also suggested in the literature on the impacts of regulation on innovation. However, literature that bridges the gap between socio-economic studies and regulatory studies, seems not to be available in large numbers to date. Therefore, in the following sections, I will try to distil elements from the social and economic contributions that I have found that can be assessed from a legal academic perspective, in order to identify factors in regulation that may influence adoption of innovative technology by consumers.

In 2015, Rezvani, Jansson & Bodin studied "Advances in consumer electric vehicle adoption research".[347] In their review of theoretical frameworks that apply to consumer adoption of electric vehicles, they acknowledge inter alia the Theory of Planned Behaviour (TPB) and the Diffusion of Innovation (DOI) theory.[348] The TPB assumes *inter alia*,[349] that consumers make decisions on whether or not to adopt certain technology, based on "rational evaluations of stimuli and the possible consequences of decisions".[350] These rational evaluations of stimuli and consequences, may include for example consumer perceptions of social norms (i.e. for instance whether or not to adopt a specific technology), their attitude towards the respective technology regarding for instance costs of purchase and maintenance, usability of the technology, and environmental issues.[351] Besides practical and rational considerations, Rezvani et al. observe that "symbols and self-identity also play a significant role in consumer adoption behavior and intentions".[352] Whereas the TPB sees mostly to *existing* technology, Rezvani et al. also consider the DOI theory, which is used to "identify and profile early […] adopters" of emerging technology, such as electric

[347] Rezvani, Jansson & Bodin 2015.
[348] Rezvani, Jansson & Bodin 2015, p. 126 – 128.
[349] Rezvani, Jansson & Bodin cite here Ajzen, I., "The theory of planned behaviour". *Organizational Behavior and Human Decision Processes* 50 1991, pp. 179–211.
[350] Ibidem, p. 126.
[351] See Rezvani, Jansson & Bodin 2015, p. 126-127.
[352] Ibidem, p. 127.

vehicles.[353] This study seeks to identify factors that may influence the adoption of AV technology, which is to a large extent still of an emerging nature, and not widely available yet. Therefore, it is especially relevant to elaborate a bit further on the DOI theory.

The Diffusion of Innovation theory was developed by Rogers,[354] and includes five factors that may influence the adoption of (technological) innovation. These are *relative advantage*, the degree to which an innovation is perceived to be better than the current state-of-the-art;[355] *compatibility*, the perceived consistency with existing values, past experiences and needs of consumers;[356] *complexity*, perceived ease/difficulty to understand and use the innovation by adopters;[357] *triability*, the degree to which an innovation ban be tried out, experienced and modified before it is adopted;[358] and *observability*, the degree to which an innovation can be observed by others.[359] Most of these factors could hardly be assessed from a legal-academic point of view. There are however two threads in DOI-literature that are worth unravelling further in this perspective. The first thread is *perceived risk*. The *perceived risk* factor is added to Rogers' five factors by Ostlund in 1974,[360] and has subsequently been acknowledged and elaborated by other authors.[361] The *perceived risk* factor will be in more detail discussed below, under 3.4.3.2. The second thread is *trust* which has been studied by *inter alia* Carter & Bélanger and Van Slyke et al,[362] which will be discussed below under 3.4.3.3. Both factors in the *consumers perspective* will be evaluated using a case study.[363]

3.4.3.2 RISK

Perceived risk can, according to Hirunyawipada & Paswan be broken down into seven sub-categories: *Financial risk,*[364] *performance risk*,[365] *physical risk*,[366] *time risk*,[367] *social risk*,[368]

[353] Ibidem, p. 128.
[354] Rogers 2003, which is an update of his first edition from 1962.
[355] Rogers 2003, p. 229-230.
[356] Rogers 2003, p. 240-248.
[357] Rogers 2003, p. 257-258.
[358] Rogers 2003, p. 258;
[359] Rogers 2003, p. 259.
[360] Ostlund 1974.
[361] See for example the empirical study by Hosseini et al. 2016, p. 499-500, and their reference to *inter alia* Cherry, J. and J. Fraedrich, "Perceived risk, moral philosophy and marketing ethics: Mediating influences on sales managers ethical decision-making", *Journal of Business Research*, 55(2) 2002, 951-962; Hirunyawipada & Paswan 2006 (an empirical study) – and the extensive literature they cite.
[362] Carter & Bélanger 2005; Van Slyke et al. 2004.
[363] See section 3.5.
[364] "financially negative outcomes for consumers after they adopt products": Hirunyawipada & Paswan 2016, p. 187.
[365] "concerns that products will not perform as anticipated": ibidem.
[366] "perception that products will be harmful to adopters": ibidem.
[367] "perception that the adoption and the use of the product will take too much time": ibidem.
[368] "has to do with the negative responses from the consumer's social network": ibidem.

psychological risk,[369] and risks related to *network externalities*.[370] The authors find *inter alia* that there is a correlation between financial *risk* and adoption of novel technology: if consumers evaluate that there may be costs that outweigh the benefits of the acquisition of a certain novel technology, this may refrain them from adopt – or even collect further information regarding innovative products.[371] Regarding *physical risk*, Hirunyawipada & Paswan find that negative associations between certain forms of emerging technology and physical risks, such as health risks that may result from cell phone radiation or the use of laptops computers on the laps of consumers, may cause a 'hurdle' in adoption, as consumers are likely to seek more information on these risks first.[372] A similar hypothesis regarding the adoption of autonomous vehicles can be found in Fagnant & Kockelman, who state that

"regardless of how safe AVs eventually become, there is likely to be an initial perception that they are potentially unsafe because the lack of a human driver. Perception issues have often been known to drive policy and could delay implementation. Moreover, if AVs are held to a much higher standard than human drivers, which is likely given perception issues, AV costs will rise and fewer people will be able to purchase them".[373]

> It is observed in the Proposed AIR that "AI can […] bring about new risks or negative consequences for individuals or the society",[374] which could – when not properly addressed – cause material and immaterial harm,[375] and negatively impact the uptake of AI-technology. The envisaged rules aim to reduce risks regarding *inter alia* health, safety and fundamental rights as much as possible, which may be inherent in AI-technology.

Again, considering the scope of this study, it will be impossible to evaluate the *consumer perceptions* of the indicated risks. However, it is possible to evaluate some of the actual allocation of risks between actors as consumers and producers through the application of regulatory frameworks.[376] The GDPR for instance allocates no-fault liability for unlawful personal data processing at controllers, or processors of personal data rather than at the data subjects, and the Product Liability Directive allocates no-fault liability for defective products at producers, rather

[369] "the nervousness arising from the anticipated post-purchase emotions, such as frustration, disappointment, worries and regret": ibidem.
[370] Which "occur when consumer's utilities from adoption of innovation depend on previous adoption or the adoption by relevant others, and estimated current and future product penetrations": ibidem.
[371] Ibidem, p. 188 (hypothesis), 192 (conclusion).
[372] Ibidem.
[373] Fagnant & Kockelman 2015, p. 177.
[374] Proposed AIR, p. 1.
[375] Recital 4 to the Proposed AIR.
[376] The assumption is that there is some overlap between the actual and future (potential) allocation of consumer risks, and their perception thereof. However, that may be tested in a study that goes beyond the boundaries of this PhD research.

than at consumers by default. It is in this regard worthwhile to evaluate the potential risks for consumers (i.e. mainly the *financial risks*) that may result from the application of the current regulatory frameworks on extra-contractual liability and personal data protection, when these would be applied to autonomous vehicles. It can be evaluated to what extent the risks for consumers might change compared to the situation without AVs. Furthermore, it can be assessed to what extent the potential situation (in which AVs are envisaged) in terms of consumer risks would be in line with the rationales and functions of the respective regulatory frameworks.

3.4.3.3 TRUST

Risk can be correlated with trust. Rousseau et al., who conducted an cross-disciplinary review of the concept of *trust*, indicate that trust would not be needed if there is no risk, or uncertainty.[377] Trust is defined by Rousseau et al., as "a psychological state comprising the intention to accept vulnerability based on positive expectations or behaviour of another".[378] Trust thus leads to the situation that despite an imminent risk, there is willingness of an actor to undertake certain risk-bearing action, because that actor expects that the other actor, who can influence the materialisation of the risk, behaves as such that is prevents that materialisation of the risk. Competence, predictability (including the absence of information-asymmetry)[379] and goodwill (regarding integrity and non-harmful behaviour) are *inter alia* seen as factors that influence the level of trustworthiness of organisations.[380]

Regarding the DOI-theory referred to above, Carter & Belanger distil from Roger's factors *trustworthiness* as a sixth one.[381] They defined *trustworthiness* as "the perception of confidence in the electronic marketer's [as "the other actor to be trusted (or not)", *RWdB*] reliability and integrity", in an empirical study on the potential adoption of e-government services.[382] From a comparable perspective, Van Slyke et al (also Belanger, and Comunale) find that "trust of the merchant, the technology and the service provider are central"[383] to e-commerce transactions.

---

[377] Rousseau et al., 1998, p. 395, as cited in De Cock Buning & Senden 2020, p. 23, and their reference to Six, F., and Verhoest, K., (eds.), *Trust in Regulatory Regimes*, Cheltenham: Edward Elgar Publishing 2017, p. 3.
[378] Ibid.
[379] See section 3.4.2.
[380] Senden & De Cock Buning 2020, p. 23-24.
[381] Carter & Belanger 2005, p. 11. They discuss this not only in the light of the DOI theory, but also place this in the context of Davis' Technology Acceptance Model (see Davis 1989), on the *perceived ease of use,* and the *perceived usefulness* of innovations.
[382] Ibidem, p. 9 and 21.
[383] Van Slyke et al. 2004, p. 2.

Carter & Belanger thus find that trust, and trustworthiness may influence adoption of (e-government) technology. They mention that – among many other things – "privacy and security are reoccurring issues" in this respect,[384] and even advise that "to increase perceptions of trustworthiness, government agencies can reassure citizens of the reliability of e-services by including easily visible privacy statements on their sites".[385] Balboni also observes that "nowadays, security and privacy seem to be at the top of the list of consumers' concerns in online transactions".[386] He does similar suggestions as Carter & Belanger regarding privacy policies, and suggests that trustworthy security measures should be taken in order to gain consumer's trust.[387] The aforementioned authors thus implicate that there is a link between (un)certainty regarding the rights to be protected – in this case: privacy rights – and *trust*, and that eliminating an information asymmetry between the consumers and the external actor – in these cases government institutions and online merchants, could help building *trust*.

Van Slyke et al. also find a relationship between the adoption of (then) innovative technology (in their research: web services) and *trust*, and also correlate perceptions of privacy and security with *trust*.[388] In a similar vein, Glancy states that observes two types of relationships between privacy protection and trust, in relation to the uptake of AV technology. Negatively, she observes that "[w]ithout appropriate legal protections for privacy, autonomous vehicles could well meet "market resistance" from potential users who perceive autonomous vehicles as threats to their privacy".[389] Positively, she indicates that "assuring respect for user privacy is one of the best ways to foster trust and confidence in new technologies such as autonomous vehicles".[390]

Fagnant & Kockelman observe in relation to the implementation (and adoption) of autonomous vehicles that *security* is serious point of concern in this perspective. They state that it "may be infeasible to create a system that is completely secure",[391] and suggest "robust defenses [that] should make attacks […] difficult to stage".[392] Besides security, Fagnant & Kockelman also mention *privacy* concerns, and suggest that "Without proper safeguards, this data [data that are gathered through AVs, *RWdB*] could be misused by government employees for tracking individuals, or provided to law enforcement agencies for unchecked monitoring and surveillance. Vehicle travel

[384] Carter & Belanger 2005, p. 9.
[385] Carter & Belanger 2005, p. 21.
[386] Balboni 2008, p. 9.
[387] Balboni 2008, p. 10.
[388] Privacy is mentioned explicitly: Van Slyke et al. 2004, p. 2; whereas they suggest future research regarding security on p. 12 and 14.,
[389] Glancy 2012, p. 1225.
[390] Ibidem, p. 1225-1226.
[391] Fagnant & Kockelman 2015, p. 177.
[392] Ibidem.

data has wide-ranging commercial applications that may be disconcerting to individuals, such as targeted advertising".[393]

Regarding the evaluation of *trust* when considering the *consumers perspective* in assessing the potential influences of regulation on innovation, a distinction can be made regarding the formal aspects of regulation on the one hand, and the material aspects on the other. The formal regulatory point of view holds *inter alia* that democratic legitimacy of the regulator, and effectiveness of the regime, i.e. that policy objectives are achieved, as well as access to the norms at hand and dispute resolution mechanisms by the *regulatees*, are crucial factors for trust in and – thus – acceptance of regulatory regimes.

Regarding the material aspect, a comparable principle applies as to *risk*: while regulation does not see to directly influence the perception of trust, or trustworthiness by consumers of technology, regulation may very well see to the creation of certain parameters for enabling trust therein – which can be evaluated from a legal academic perspective. One of the functions of personal data protection-regulation is for instance to empower consumers to 'control' their personal data, which is seen to contribute to their trust in new technology.[394] It can be evaluated to what extent consumers of AVs for example may actually trust that their informational privacy rights are protected after the (envisaged) introduction of AVs into society, and whether or not that would be different compared to the situation without AVs.

> On a more general level, the Proposed AIR assumes an important relationship between citizen's trust in AI-technology and their adoption of products in which AI is embedded. It states that the proposal is aimed at "the development of an ecosystem of trust by proposing a legal framework for trustworthy AI", which is crucial for technology-uptake.[395] Furthermore, it is highlighted that "[r]ules for AI […should be…] human centric, so that people can trust that the technology is used in a way that is safe and compliant with the law including the respect of fundamental rights".[396]

The aims of (implementations of) the Product Liability Directive include that incentives for producers are created to produce and bring to market products that are safe (i.e. not defective),[397] which may in turn contribute to the trust of consumers that they are confronted with safe products. Rationales of for instance the Dutch rules on motor-vehicle liability

[393] Fagnant & Kockelman 2015, p. 178.
[394] See for example the 7th consideration of the GDPR; Chakravorti 2018; also (on the relationship between privacy, security and trust in cloud computing): and Pearson 2012, chapter 1.6.
[395] Proposed AIR, p. 3.
[396] Ibidem.
[397] See González Castillo 2012, p. 291.

(Wegenverkeerswet) also include *inter alia* that non-motorized victims of traffic accidents involving motorized vehicles, can effectively get their damages remunerated.

After these evaluations, some assumptions can be made regarding the potential influences of regulation on innovation seen from the *consumers perspective*. A strong assumption is that there is some overlap between the levels of *trust* that may be derived from the application of the studied regulatory frameworks, and the actual *perception of trust* by consumers. Again, that cannot be tested from a legal-academic point of view within the boundaries of this PhD research, but there are enough indications to this effect.

3.4.3.4 RELATIONSHIPS BETWEEN RISK AND TRUST

Besides the more conceptual relationship between risk and trust sketched in section 3.4.3.3, some other forms overlap between the factors of *risk* and *trust* can be identified. A higher level of risk for consumers, which may result from the application of for instance the actual extra-contractual liability rules to AV accidents, may negatively amount to their *trust* that the technology is safe, and that they may eventually receive compensation for damages. Or, when a personal data breach occurs affecting a centralized database in which millions of AV data are stored, this could negatively impact the consumer's trust in the protection of their privacy by innovators in the field of AVs.

I think however that it is fair to distinguish these two factors within this study. While *risk* sees to the potential financial and physical losses by consumers, the notion of *trust* is broader as the latter relates to a higher (meta-)level of guarantees that are regulated such as integrity and reliability, than the former.

3.4.4 BALANCING PERSPECTIVES

The factors that have been presented above within the two respective viewpoints, may influence each other – in various ways. Generally speaking, one may observe *inter alia* the following. When for example a rule lacks *legal certainty*, it may be that neither innovators nor consumers can predict their (financial) risks. If a rule has the necessary level of predictability, and strongly protects the rights of consumers, this could entail that there are minimal (financial and/or physical) *risks* for consumers but at the same time a very high compliance burden for innovators. The opposite could also be thought of: when an innovator complies with very stringent regulation, this could entail that the innovator exonerates liability upon compliance, which then shifts the *risks* to the respective users. In other words, it could very well be that strong protection of innovators causes poor circumstances for consumer adoption of innovations. The other way

around, it can also be true that too strong consumer protection entails burdens for innovators that can hardly be complied with.

> In the Proposed AIR, the EC acknowledges both these perspectives in relation to stimulating innovation and the acceptance thereof, as was introduced in the foregoing sections. With the proposed regulation, the EC aims at the creation of "acceptable" AI-technology, in order to enhance the successful deployment of such technology.[398] To that end, the envisaged rules prescribe that AI-systems must *inter alia* comply with fundamental rights and safety standards. This should, from a *consumer perspective*, foster trustworthiness of the technology and minimise risks, and should create optimal conditions for the uptake thereof.[399] The Proposed AIR addresses the *innovators perspective* as equally important, states to regulate AI in a way "that is limited to the minimum necessary requirements to address risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the costs of placing AI solutions on the market".[400] Not only aims the Proposed AIR at legal certainty ("to facilitate investment and innovation in AI"),[401] whilst providing a "robust and flexible legal framework", it also specifically addresses *regulatory sandboxes* as a means to balance the consumer's and innovator's interests as much as possible. These *sandboxes* should provide "novel forms of regulatory oversight and a safe space for experimentation":[402] controlled environments must be created "to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service".[403] By doing so, innovators can be guided by the authorities to create AI-technology that complies with the envisaged rules – which are aimed at consumer trust and acceptance. At the same time, keeping the innovators close would contribute to "authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use".[404]

All in all, it is thus imperative that the factors within the realm of the *innovators perspective* are also reviewed with the *consumers perspective* in mind and vice versa. In order to do so, I have designed a case study, which is presented in the following section. On the basis of that case study, both perspectives are assessed and analysed further in Chapter 6.

---

[398] See the foregoing sections, and more generally, section 3.2
[399] See Proposed AIR, p. 1-3.
[400] Proposed AIR, p. 3.
[401] Ibidem.
[402] Recital 71 Proposed AIR.
[403] Ibidem.
[404] Recital 72 Proposed AIR. See furthermore articles 53 and 54 of the Proposed AIR.

3.5 CASE STUDY

3.5.1 INTRODUCTION

In this section, a case study is introduced in which the five factors within the two perspectives (*innovators perspective: legal certainty*; *stringency*; *flexibility*; and the *consumers perspective*: *risk*; *trust*) can be tested, in both main regulatory regimes (*extra-contractual liability regulation*, consisting of product liability and traffic liability; and *personal data protection regulation*).

The options for designing case studies are almost limitless. Differentiation in the facts and circumstances that could be presented here, may lead to a myriad of different outcomes in the analysis of the factors.[405] In order to avoid a description of a very broad range of possible scenarios, whilst still maintaining the relevance and likeliness of the presented facts and circumstances to be studied within the cases, I have made the following choices.

The facts and circumstances sketched below, are derived from an accident scenario that I assume to be typical when AVs will be deployed in the future, and are to co-exist with regular non-motorized traffic on the same roads.[406] That assumption is *inter alia* based on studies regarding the current and forthcoming state of the technological art,[407] and studies on legal challenges related to the development and deployment of AVs.[408] Further references are made to these sources in the scenarios sketched below where applicable Furthermore, the facts and circumstances have been 'fixed' as much as possible.[409] Therefore, more constants than variables are presented here. One main variable is introduced that will be used in my study of both regulatory frameworks. That is the *level of severity of the consequences* of the accident, where low-medium and high levels are distinguished, which I assume to be archetypical in relation to accidents with AVs.[410] In the analysis I will assess, how shifting the *level of severity of the consequences* could lead to different observations regarding the identified factors in section 3.4 . One of the reasons for choosing the *level of severity of the consequences* to be variable, is that different levels of severity of consequences may be (still) expected when AVs are to be deployed.

[405] Taking the product liability framework in relation to risk [RI] for example, the presentation of a high level of uncertainty regarding a causal relationship between for instance a defect in an AV and certain damage could lead to the analysis that the factor risk would be higher, as chances are that a victim would not easily be able to get remuneration. That analysis would be different when a lower level of causation uncertainty would be presented. I will, for that matter, not vary between the levels of causation uncertainty in the cases presented in these sections.
[406] This co-existence and the inherent safety issues are also foreseen by for example the European Commission, See European Commission 2018a, p. 10.
[407] See European Commission 2018d. See also SAE J3016_202104.
[408] For example Robolaw 2014; CCAM report 2018; Engelhard & De Bruin 2018; De Bruin 2016.
[409] That does however not mean every variation of these constants is avoided: some variation will take place within the analyses to the extents necessary.
[410] Also here, assumption is *inter alia* based on studies regarding the current and forthcoming state of the technological art, and studies on legal challenges related to the development and deployment of AVs.

Furthermore, my assumption is that this variable provides – in relation to the constants – the more interesting insights in the similarities and differences between the studied legal regimes. Despite the overall inspected increase in vehicle-, road- and technology safety and security after the introduction of AVs, accidents and data (privacy) incidents may still happen. The results depicted below can very well be predicted to be in line with the levels of severity of the consequences of actual (non-autonomous) car accidents and data breaches.

As regards the extra-contractual liability framework, the three levels of *severity of the consequences* incorporate further distinctions in types and amounts of damage. As will follow from the table in paragraph 3.5.3, the 'low' *level of severity of the consequences* includes forms of pure financial loss and property damage constituting relatively low amounts of damage. The 'medium' *level of severity of the consequences* includes the same types of damage, of higher amounts, and personal injury of a relatively mild nature and size, and of a relatively short duration. The 'high' *level of severity of the consequences* not only consists of high amounts of financial loss and property damage, and also includes high amounts of personal injury of longer (if not lifelong) duration, with a possible claim for noneconomic damages. Regarding the regulatory framework on the protection of personal data, it must be noted that the direct consequences will often be of a financial, non-personal nature. Therefore, the variation between the *levels of severity of the consequences* mainly consists of different amounts of damage.

All three case positions of the two regulatory frameworks, can be studied in each other's contexts. That means that the (archetypical) "low", "medium" and "high" *levels of severity of the consequences* in category 1 (extra-contractual liability) can be studied in the perspective of each 'opposite' case regarding respectively "low", "medium" and "high"-damage in category 2 (personal data protection) and vice versa. This results in 9 possible combinations. As it would be not necessary to study all these different positions, given a relatively large overlap in the individual analyses, and given the size and scope of this research, I have chosen to stick to only one of the case positions of category 2, when studying the three case positions of category 1, and vice versa. These 'fixed' cases have been marked as such in the table below.

I have chosen not to alter other possible variables (such as the type of the vehicle; the safety systems used; the amount and nature of the actors; the levels of causation uncertainty and the levels of negligence by the different actors) within the presentation of the case study hereunder. Where that may be relevant, I will elaborate on deviations regarding the 'constants' within the analysis in Chapter 6.

3.5.2 CASES – CONSTANTS

1. It is September 13th 2024, 3.00 a.m.
2. A self-driving car crashes into a group of 3 bicyclists in the city centre of Utrecht.[411]
3. The car was marketed as a Level 5 Autonomous Vehicle by its manufacturer, who is also based in the EU.[412]
4. Thus, human operation or (fall back) intervention would never be required: the car should be able to perform all aspects of the driving task itself.[413] The AV-passengers were not paying attention to the road – as they did not have to;
5. The car was equipped with an accident prevention and registration system (APRS), using vehicle to infrastructure (V2I) technology.[414] This system can help preventing accidents by sharing real time information concerning road users, which can for instance be used to calculate safe speeds, or stop cars in case of emergency. When accidents do nonetheless happen, it records and stores necessary data to help analysing accident causes.[415] The APRS uses blockchain technology in order to minimise the risk of data manipulation in individual AVs.
6. The car was directly sold by the manufacturer to its owner, a "normal consumer".
7. Regarding the causes of the accident, a lot is still uncertain. The following is however known:[416]
    - One month earlier, the supplier of the software incorporated in the AV, failed to mention a vulnerability in the operating systems, that could *inter alia* lead to the breach of confidentiality of the personal data that are processed through the operating systems;[417]

[411] I chose non-motorised actors as external victims of the crash, as there are specific rules within (some of the) the non-harmonised extra-contractual liability frameworks of the member states, which may deviate from rules regarding motorized victims. I will slightly vary on the 'type' of victims within the analysis. These victims furthermore qualify as 'data subjects' in sense of the GDPR.
[412] It would be also interesting to study partially autonomous vehicles (where human fallback would be required), but would go beyond the scope of this research, which merely sees to completely autonomous 'decisions'.
[413] See SAE 3016_202104.
[414] See section 2.3, and De Bruin 2016, p. 495. As it cannot be precisely predicted how this technology would take shape, I have made these assumptions under this bullet point.
[415] The EC recommends this type of use of such technology in European Commission 2018a, p. 10; many cars are already equipped with black-boxes and similar technology, especially in the US, see for example: https://www.hawkins.biz/insights/insight/event-data-recorders-in-passenger-vehicles.
[416] I have chosen these 'unknowns' as constants, for these will affect the analysis of *inter alia* the *legal certainty* and the *risk* factors. Slight variations will be made in the analysis. Presenting these unknowns as variables, would however unnecessarily complicate the presentation of the case study.
[417] It is not unthinkable that through that vulnerability, malevolent third parties could also have taken over (parts of the) steering software of the AVs using that piece of software (see for an acknowledgment by the EC of this type of risk European Commission 2018a, p. 12), however this does not become clear from the log files. This constant highlights the (un)certainty of the cause of the accident, and may therefore influence *inter alia* the factors *certainty, risk* and *trust*.

- The AV performed an auto-update to the operating system one day before the failure,[418] and there was a sensor-malfunction that can be related to the auto-update;[419]
- This specific auto-update was not intended by the car-manufacturer; The auto-update was installed without being agreed to by the car-owner;[420]
- The bicyclists ignored a red traffic light;[421]
- The software supplier, a relatively new player on the market who is based in California, was still in the initial stages in the process of GDPR-compliance.[422]
- The software supplier has "for software maintenance purposes" access to the (personal) data processed through the vehicle, including the APRS-data.

8. The accident generates a lot media-attention and commotion; the manufacturer considers to withdraw from the European market and his competitors (using comparable hard- and software) are considering the same.[423]

Regarding the *level of severity of the consequences* for the victims, these are the scenarios (see next page):

[418] Over-the-air-updates are nowadays (January 2019) being performed by for example Tesla: https://www.tesla.com/support/software-updates.
[419] It is known that over-the-air updates can influence the driving performance of a car, see for example https://www.theverge.com/2018/6/2/17413732/tesla-over-the-air-software-updates-brakes.
[420] Also this constant highlights the (un)certainty of the cause of the accident, and may therefore influence *inter alia* the factors *certainty, risk* and *trust*.
[421] This constant not only highlights the (un)certainty of the cause of the accident, and may therefore influence *inter alia* the factors *certainty, risk* and *trust*, it may also give rise to a *contributory negligence* defence, which can play a role within both the product liability analysis and the analysis of the non-harmonised traffic liability rules.
[422] I chose this constant as this may implicate his liability position, and it could influence the *trust* factor.
[423] I have chosen this constant as the media attention may for example influence the *trust* of consumers in the respective technology.

3.5.3 *CASES – VARIABLES: LEVELS OF SEVERITY OF THE CONSEQUENCES*

	Damage	Generic extra-contractual liability related damage	Personal data related damage
1	Low	The passengers of the AV can leave the vehicle unharmed; some light repair works on the body of the car are necessary. The external airbag of the AV prevented anything but material damage to the bicyclists.	The APRS was poorly secured. Vehicle data, including vehicle identification numbers, were publicly accessible during five months prior to the accident.
2	Medium	The passengers of the AV can leave the vehicle unharmed. The car caught fire, which could be extinguished in an early stage, however the battery compartment is burnt severely, and the exterior of the car is badly damaged by the impact. The bicyclists all have broken limbs (arms and legs), and will need approximately six weeks to fully recover. One of them needs to be hospitalized for five days. The bicycles cannot be repaired.	The APRS was poorly secured. Vehicle data and data regarding the AV-passengers (i.e. their full names and addresses) had been publicly accessible after the accident. These data have been used by a small army of personal injury lawyers offering their services to the passengers.
3	High	One of the two passengers of the AV, who was sitting in the front of the AV, suffered spine injuries and is partially paralysed. The other one, sitting in the back, has some broken limbs and must recover for two months. The AV must be considered total-loss and so are the bicycles. Two of the bicyclists suffered injuries on the head, arms and legs, and must be hospitalized for more than three weeks. The third must miss a leg and will never be able to cycle again, and also sees his future career as a doctor shredded. **[fixed facts for Personal Data-case study]**	The APRS was poorly secured. Not only vehicle data and data regarding the AV-passengers (i.e. full names, addresses, nature of their injuries and recovery prognoses, insurance details et cetera – which were added to the system by its producer for purposes of legal defence) had been disclosed, also data of the bicyclists were publicly accessible after the accident. All victims were approached by personal injury lawyers offering their services. Furthermore, with the publicly available data, third party X had used the data of one of the bicyclists and claimed remuneration of hospital costs, which was paid accordingly by the insurance company to X. When the actual victim also claimed his healthcare expenses later, the insurance company refused and placed him on a blacklist. As a result, this victim had to bear all healthcare expenses himself, until the fraud by X could be proved by him. **[fixed facts for Extra-contractual Liability-case study]**

3.6 CONCLUSION

In this Chapter, I have identified *factors* that can be distilled from academic literature, which may influence innovation. Innovation can, in terms of this research, be seen as the outcomes of the research & development processes of organisations active in the field of AVs, including the accepted societal deployment, i.e. the adoption thereof by consumers. Regulation is seen as the intentional activity (i.e. both the process itself and the results thereof) from one public or private entity (the *regulator*) to influence the behaviour of another entity (the *regulate*). In this study, I have chosen to investigate of mix of policy instruments (including both public- and private regulatory frameworks) that applies in the European Union regarding product liability, traffic liability and personal data protection.

Two perspectives were identified from which innovation-influencing *factors* can be distilled. From the ***innovators*** perspective, these are, *legal (un)certainty, flexibility* and *stringency*. *Legal certainty* can impact investments in innovation. When it is difficult or impossible for innovators to reasonably foresee and to calculate risks that may result from a regulatory framework that applies to the development and deployment of novel technology, a negative impact on investment decisions can be predicted. *Stringency* relates to the need for innovators to adapt their behaviour in order to comply with regulation. Behavioural changes are particularly evident when new regulation is introduced, which necessitates a "behavioural change" by innovators. Furthermore, when regulation requires upfront compliance efforts for new market players, this could also entail *stringency*. Two aspects of *flexibility* can be found in regulation which may influence the development and deployment of innovation. First, when regulation necessitates certain ex ante compliance, it would be better for innovation when innovators have more manoeuvring space to reach compliance than when the implementation paths are limited. Second, rules that are adaptable to (technological) change are, from a innovation-stimulating perspective, preferred over technology specific rules, which are less adaptable to changing circumstances.

From the ***consumers*** *perspective*, the factors *risk* and *trust* were identified. It was found that it may negatively impact the adoption of novel technology, when that technology – and the rules that apply thereto – results in (financial and other) *risks* for consumers. *Trust* is, besides the *risk*-factor, important for the acceptance of a novel technology by consumers. Trust regarding *inter alia* the safety of a product is found to be necessary for adoption of technology, as would be trust in the "reparative capacities" of for instance a liability framework when victims suffered damage due to a (nonetheless) unsafe product, and the trust that fundamental rights (including privacy and personal data protection) are well-observed.

In the third part of this study, it will be assessed to what extent these *factors* can be identified in the regulatory frameworks under investigation, both 'in themselves' and in view of each other, as it had also been concluded that there can be certain interplays between the factors. This will be done on the basis of the case study that was introduced in section 3.5.

PART TWO – ASSESSING THE *FACTORS* WITHIN THE REGULATORY FRAMEWORKS

Chapter 4. EXTRA-CONTRACTUAL LIABILITY REGULATION IN THE EU

4.1 INTRODUCTION

4.1.1 GENERAL OVERVIEW

Extra-contractual liability regulation in the EU plays the central role in this chapter. This area of law holds rules regarding obligations that arise for one party to compensate damage suffered by another party in situations where that latter party acted in a way that is deemed wrongful. Extra-contractual liability regulation can thus be distinguished from, for instance, contractual liability- and criminal liability regulation.[424]

Extra-contractual liability is also referred to as *tort* in the literature.[425] *Tort* has been used for a long time in common law systems as a concept meaning 'wrong', and may currently hold that "a tort is an injury other than a breach of contract, which the law will redress with damages"[426] or other remedies, but has no equivalent in civil law systems.[427] Therefore, I chose to mainly use *extra-contractual liability* (which concept is used in common- and civil law systems alike) rather than *tort* in this study, notwithstanding occasional exceptions.

Although the notion of *European (Union) tort law* is used in literature (*European extra-contractual liability law* not as such), there is no overarching system or law on extra-contractual liability in place in the European Union.[428] According to Van Dam, *European tort law* consists of three tiers, which influence one another.[429] The upper tier consists of EU legislation regarding non-contractual liability, such as "Treaty provisions, certain Regulations and Directives",[430] and case law of the Court of Justice of the European Union in Luxembourg.[431] The lower tier is formed by

[424] Contractual liability regulation sees to remuneration of damage that is the result of breach of contract between two (or more) parties. Criminal liability regulation sees to reparation of damage as a result of a criminal offense between a private party and the state.
[425] Van Dam 2013; Lunney, Nolan & Oliphant 2017, Sappideen & Vines 2011, all refer to *tort* law. Both concepts (*tort* and *extra-contractual liability*) are almost identical – and can to a certain extent be used as synonyms – but there are slight differences. The most striking of these slight differences is of a semantical nature. *Tort* derives from the past participle of the latin verb *torquere*: *tortum*, which means 'twisted'.
[426] Sappideen & Vines 2011, p. 3.
[427] See Van Dam 2013, p. 5., who – differently – adheres to the concept of *tort*.
[428] See for example Van Dam 2016; Spier 2003 and the *Journal of European Tort Law*.
[429] Van Dam 2013, p. 6.
[430] Van Dam 2013, p. 5 and p. 39-49.
[431] There is interaction between the CJEU and the (case law of the) European Court of Human Rights in Strasbourg, based on the European Convention on Human Rights. Van Dam refers *inter alia* to the fundamental rights and freedoms stipulated in articles 2-18 of the ECHR, and article 13 in particular,

extra-contractual liability regulation of the Member States, including *inter alia* national legislation and case law.[432] Van Dam observes in that regard that "although a convergent tendency is apparent at some points, it is also clear that the differences between the Member States remain substantial".[433] The two aforementioned tiers are linked together by comparative law, which is formed by (academic) comparisons between the national regimes, which is for example reflected in the (non-binding) Principles of European Tort Law (hereinafter: PETL), and Book VI of the Common Frame of Reference (hereinafter: CFR).[434]

As introduced in Chapter 1.2.3.3, the subject of this research relates to extra-contractual liability regarding accidents in which AVs are involved. In the next sections, I will study the rules of the Product Liability Directive (Van Dam's first tier) applicable to relationships between victims and producers of (possibly) defective components of AVs (0). Where the product liability regime leaves room to national legislation (Van Dam's third tier), I will study the rules that apply in the Netherlands (4.2.3), France (4.2.4) and England (4.2.5). Occasionally, where these form a significant difference from either the harmonised rules or the respective implementations, I take notice of corresponding (second tier) provisions of PETL,[435] and CFR.[436] After having elaborated on product liability rules, I will study the non-harmonised third tier regimes on extra-contractual traffic liability of again the Netherlands (0), France (0) and the UK (4.3.4), and – where relevant, second tier principles.[437] Before the analysis of the material rules that apply to the case study, I will explore the functions of the aforementioned regimes in the following sections, as this is relevant in the later analysis of *inter alia* the factors *legal certainty, flexibility, stringency, risk* and *trust*.[438]

It must be noted that my analysis is, as stated above, in principle limited to the *material* aspects of the extra-contractual liability rules, and therefore does not specifically focus on evidentiary rules. However, a strict separation between material and evidentiary rules is hard to make, and occasional reference to evidentiary rules will be made in my analysis. As will be indicated *inter*

---

holding that "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity"; See Van Dam 2013, p. 5, 25-26.

[432] Van Dam 2013, p. 5.

[433] Van Dam 2013, p. 6.

[434] Which are available at http://www.egtl.org/, respectively https://bit.ly/2F8w8yi.

[435] Product liability is not as such addressed in PETL, however article 4:202 PETL sees to "Enterprise Liability", as discussed in EGTL 2005, p. 93-100, which is of a very different nature than product liability rules as harmonized by the PLD.

[436] Accountability for damage caused by defective products is addressed in article 3:204 CFR, see also Von Bar 2009, p. 686-702.

[437] Article 3:205 CFR sees to accountability for damage caused by motor vehicles, as elaborated by Von Bar 2009, p. 703-718. PETL does not address motor vehicle liability.

[438] In all these factors, the relationship between the actual rules and the respective functions / the underlying rationales are relevant. See sections 3.4.2 and 3.4.3.

alia in the case study analysis,[439] an answer to the question whether or not an AV-innovator can successfully be held liable by a victim of an AV-related accident will be increasingly dependent on the victim's access to, and interpretation possibilities of AV and -accident data, including the algorithms that underly autonomous decisions made by the AV that might have contributed to the accident. I assume that it will in principle be possible to get hold of such data and information under the studied regimes,[440] although this may cost considerable amounts of time and money. A more serious problem relates to the interpretation thereof. As illustrated for instance by Bertolini 2020, "the most problematic aspect of […] logged data is certainly its interpretation and analysis might be extremely complicated and costly". [441] Bertolini sketches an example of a defective robotic hand-prosthesis worn by an amputee. That person drove a car which got involved in an accident. The prosthesis might have been defective, and in turn contributed to the origination of that accident. A product liability claim is started. Although the data regarding the "human machine interaction" between the person wearing the prosthesis and the activities of the device itself, were logged (stored), a claimant would *inter alia* "still need to identify all the biological signals emitted by the nervous system of the implantee, [and] identify those that have been misinterpreted, demonstrate that if they were correctly interpreted there would have been no erratic movement on the side of the amputee, and without that movement the accident would not have occurred",[442] in order to underpin that claim. Where comparable problems might arise in AV-related cases studied in this research,[443] I will indicate these as interpretation or analysis issues.

This Chapter concludes with the current vision to the future of the EU institutions regarding civil liability,[444] which is – at least partially – triggered by the advent of autonomous intelligent systems including AVs. Recently, the institutions of the European Union endorsed that some of the currently applicable regulatory regimes, including those regarding civil liability, need to be optimised in order to better facilitate development and acceptable deployment of such

[439] See Chapter 6.
[440] See for instance for The Netherlands article 843a Wetboek van burgerlijke rechtsvordering (see also A. Hammerstein, R.H. de Bock, W.D.H. Asser, *Modernisering burgerlijk bewijsrecht, Advies van de expertgroep Modernisering Burgerlijk Bewijsrecht*, Den Haag: Boom Juridisch, 2017; for France *inter alia* article 145 Nouveau Code de procédure civile, as discussed in T.A.G. Bens, "Grensoverschrijdend Bewijsbeslag", *Nederlands Internationaal Privaatrecht*, 2017 vol. 3, p. 491, referring to W. Kennett, 'The Production of Evidence within the European Community', *Modern Law Review* 1993, vol 56, p. 349-350 (Kennett 1993); and for England disclosure obligations on the basis of Rule 31 of the Civil Procedure Rules (https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31) and discovery procedure, see for instance R. Grant, "UK: Disclosure Of Documents In Civil Proceedings In England And Wales", *mondaq*, 22 november 2017, via https://www.mondaq.com/uk/civil-law/642194/disclosure-of-documents-in-civil-proceedings-in-england-and-wales. See also Giesen 2000, p. 24-27 (regarding The Netherlands); p. 30-34 (inter alia regarding France and England).
[441] Bertolini 2020, p. 84.
[442] Ibidem.
[443] Which is currently the case, as argue De Vor & Van Dijck 2020.
[444] I.e. until September 1st 2021, which is the end-date of this study.

technology. Several proposals have been made in that regard, including "generic" rules in the Proposed AI Regulation of the European Commission (Proposed AIR, introduced above in section 3.2), and the Proposed Regulation for a Civil Liability Regime by the European Parliament. The EP Proposal will be introduced in section 4.4. That proposal forms the regulatory response to the findings of the Expert Group on Liability for New Technologies, instituted by the European Commission, and the EP-reaction thereto, which had been formally given by the Juri-committee under the supervision of Bertolini, which will also be illustrated below in section 4.4.

4.1.2 COMMON FUNCTIONS OF EXTRA-CONTRACTUAL LIABILITY RULES

Given the absence of an overarching unified regulatory framework on extra-contractual liability, it is relevant to explore the functions of the national regimes to be studied and the harmonised product liability rules, As functions, *compensation*,[445] *recognition,*[446] and *deterrence*[447] are often mentioned.[448]

Compensation entails that extra-contractual liability regimes are to determine when, for which reasons and under which conditions a victim should be compensated for his losses that are the result of the conduct of someone else.[449] This is congruent with the reparative theory, according to which one who can be held responsible for harm that has occurred to another, must compensate the damage.[450] Compensation can generally take place in two forms. Reparation in kind, for instance through the replacement of a broken object, sees to the restoration of the *status quo*

[445] Sappideen & Vines 2011, p. 6; Lunney, Nolan & Oliphant 2017, p. 19-20, citing Williams 1951, p. 137; Van Dam 2013, p. 347-348;
[446] Van Dam 2013, p. 349; Lunney, Nolan & Oliphant 2017, p. 18, citing Williams 1951, p. 137, who shares *recognition* under the umbrella of *appeasement*
[447] Sappideen & Vines 2011, p. 6; Lunney, Nolan & Oliphant 2017 p. 19, discussing Williams 1951; Van Dam 2013, p. 349-353.
[448] Sometimes these 'core values' are also referred to as 'interests' or 'policy objectives' (Sappideen & Vines 2011, p. 5 and 8, or 'aims' (Williams 1951; Lunney, Nolan & Oliphant 2017, p. 18, or simply 'functions' (Van Dam 2013, p. 346. As another function also *allocation of risks* is mentioned and evaluated in Cane & Goudkamp 2018, p. 399 – 400. Where risk-allocation specifically might be one of the functions of *strict liability*, it is not necessarily one of the functions of *fault-based* liability. Furthermore, in some systems and to some extent *punishment* could also be observed as a function of extra-contractual liability regulation, as is pointed out by Cane & Goudkamp 2018, p. 401. Agreeing with these authors (see p. 402), I have left *corrective justice* out of the overview of "common functions", as there is no consensus on the definition, and more importantly, extra-contractual liability regulation could only to a small extent be seen as contributing to *corrective justice*.
[449] See Sappideen & Vines 2011, p. 5. See also Cane & Goudkamp 2018, p. 392-396, who – from a common law perspective – distinguish different types of compensation: corrective compensation (taking "as its benchmark the situation the person to be compensated was in at some earlier stage of [his] life", p. 392), redistributive compensation (where the benchmark is rather "the position that other people now occupy", p. 393), equivalent compensation (where there is a monetary compensation for lost money or other assets, such as wages, medical expenses or expectations, p. 393), and compensation as substitute and solace (where non-pecuniary losses such as pain, suffering and amenities are compensated, p. 394-395).
[450] See for example Williams 1951 as cited in Lunney, Nolan & Oliphant 2017, p. 19.

ante.[451] Monetary compensation sees to remuneration of damages that cannot be compensated in kind. Together with *inter alia* first-party insurance and social security systems, the compensation function of extra-contractual liability regulation sees to the distribution of losses.[452]

Recognition of the harm done is another shared function of extra-contractual liability regimes.[453] Especially where reparation in kind or in money cannot compensate the respective losses, or in addition to that compensation, *recognition* is important to acknowledge that a wrong has been committed, in order to satisfy the victim.[454] In that regard, Williams, who labels this as *appeasement*, observes that "the victim's vengeance is bought off by compensation, which gives him satisfaction in two ways: he is comforted to receive the money himself, and he is pleased that the aggressor is discomfited by being made to pay".[455] He adds that it is better to enable the victim to "let off steam" within the justice system, "rather than outside it".[456]

Deterrence sees to the *prevention* of damage inducing behaviour, or as Sappideen & Vines, quoting the "legal economists", state that tort liability's function is "to influence human conduct ex ante".[457] Cane & Goudkamp observe *deterrence and prevention* even as "one of the most important […] functions of personal injuries compensation law".[458] Extra-contractual liability rules can be observed to form a threat of punishment, which thus is to be a disincentive for the sanctioned behaviour,[459] or, contrarily, an incentive for desirable conduct.[460] This incentive is often of a financial nature. "Wrong" behaviour is discouraged by financial stimuli: provided that the costs for taking precautions are lower than the costs of compensating injuries, there would thus be a financial stimulus to take the precautions to avoid "wrong", damage inflicting behaviour.[461]

Whereas *compensation, recognition* and *deterrence* may be values that are shared between the regimes, there are great differences regarding the emphasis and the actual implementation thereof in national regimes. In France for example, there is a strong focus on the *compensation* function of extra-contractual liability regulation. Deterrence would, although acknowledged in for instance trademark-infringement cases, be a less important objective than compensation.[462]

[451] See Van Dam 2013, p. 348.
[452] Cane & Goudkamp 2018, p. 397-399.
[453] See Van Dam 2013, p. 349; also Cane & Goudkamp 2018, p. 403 – 405, who label this as *vindication*.
[454] Van Dam 2013, p. 349.
[455] Williams 1951 in Lunney, Nolan & Oliphant 2017, p. 18.
[456] Idem.
[457] Sappideen & Vines 2011, p. 13-14. Differently: Williams 1951, as criticly reviewed Lunney, Nolan & Oliphant 2017, p. 18-21; See also Van Dam 2013, p. 348-349; Cane & Goudkamp 2018, p. 405-414.
[458] Cane & Goudkamp 2018, p. 405.
[459] See also Van Dam 2013, p. 348-349.
[460] Cane & Goudkamp 2018, p. 405.
[461] Ibidem.
[462] Van Dam 2013, p. 352.

Prevention through (threatened) financial punishment is a more important objective under for example English (and even more so: United States) law.[463]

The similarities and differences introduced above, are elaborated further in the following sections. C*ompensation, recognition* and *deterrence* are – along with other, regime-specific rationales, including for instance *consumer protection* and *stimulation of innovation,*[464] reflected within the product liability directive and the national traffic liability systems of France, The Netherlands and England, as I will elaborate below.

4.2 PRODUCT LIABILITY

4.2.1 INTRODUCTION

In the following sections, an overview is given of the provisions of the Product Liability Directive (PLD)[465] that are relevant for the analysis of the case study introduced in section 3.5 The PLD has been implemented in all national liability regimes of the EU Member States, and is considered as an instrument of maximum harmonisation.[466] Not all elements of what constitutes product liability are harmonised however,[467] thus other parts are explicitly left to the Member States.[468] The directive does tolerate the parallel existence of pre-existing national (extra-) contractual liability regimes regarding the same subject.[469] The courts of the Member States, and, by means of answering prejudicial questions, the Court of Justice of the European Union (CJEU) have explained and further developed the provisions of the directive. In section 4.2, I will illustrate the PLD provisions and CJEU case-law that are relevant in terms of this study, whereas for matters where deviations were allowed, and for matters entirely left to the Member States, I sketch the rules that apply in the Netherlands (4.2.3), France (4.2.4) and England (4.2.5).

[463] Van Dam 2013, p. 350; Cane & Goudkamp 2018, p. 405.
[464] Which are mentioned as functions of the Product Liability Directive, as explicated in Chapter 4.2.2.2.
[465] Council Directive of 25 July 2985 on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), *OJ* 7 August 1985, No L 210/29, amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999.
[466] See Fairgrieve et al. 2016, p. 27-28.
[467] See recital 24 PLD.
[468] These elements include *inter alia* the optional inclusion of "primary agricultural produce and game" in the definition of "products" (article 15(1)(a) PLD); the option of setting a damages ceiling for producers above the threshold of "70 million ECU" (article 16(1) PLD); and the optional exclusion of the development risks defence (article 15(1)(b) PLD, see further 4.2.2.8). Furthermore, the PLD leaves to the Member States *inter alia*: "provisions […] concerning the rights of contribution or recourse" (article 5 and 8 PLD); and the determination of a causal relationship between defective products and damage (see further 4.2.3). See also (and more elaborate) Fairgrieve et al. 2016, p. 28-31, 39.
[469] Article 13 PLD.

4.2.2 PRODUCT LIABILITY DIRECTIVE

4.2.2.1 Introduction and functions

Article 1 of the PLD states that: "The producer shall be liable for damage caused by a defect in his product". This main provision introduced a novelty within the European Union: strict liability for producers vis-à-vis consumers.[470] The directive has generally two functions. It sees to the protection of consumers, while striking a balance with the interests of producers, in order to foster competitiveness and innovation in a level playing field between the Member States.[471] That the PLD was to solve two problems at once – and serves two main functions at the same time, follows *inter alia* from the consideration that:

> "approximation of the laws concerning liability of the producer for damage caused by defectiveness of his products is necessary because the existing divergences may distort competition and affect the movement of goods within the common market and entail a differing degree of protection of the consumer against damage caused by a defective product to his health or property".[472]

The no-fault liability of producers of defective products that was introduced by the PLD, is supposed to make it easier for consumers to get compensation from producers than it would be when victims would for instance also have to prove *fault* of producers.[473] Furthermore, the PLD sees to aid consumers by explicitly bringing certain heads of damage within the scope of damages to be compensated (death, personal injury and (consumer) property);[474] by the provision that contractual derogations of the PLD-provisions are not allowed;[475] and by the creation of a one-stop-shop for victims, who may seek compensation from any of several actors who can be held be liable under the PLD.[476]

A number of measures have been taken in the PLD in order to strike a balance with the interests of producers. Recital 12 stipulates that "a fair apportionment of risk between the injured person and the producer implies that the producer should be able to free himself from liability if he

[470] Since its introduction, the European Commission reported five times on the application of the PLD, and a first evaluation took place in 2018. The first report dates from 1995, See European Commission 1995, COM(95) 617, final; the second from 2000, see European Commission 2000, COM(2000) 893 final; the third from 2006, see European Commission 2006, COM(2006) 496 final; the fourth from 2011, see European Commission 2011, COM(2011) 547 final; and the first evaluation dates from 2018, see European Commission 2018, COM(2018) 246 final.
[471] See Fairgrieve et al. 2016, p. 25-26; European Commission 2018, p. 1-2; European Commission 2000, p. 5, European Commission 2006, p. 6-7; and European Commission 2011, p. 11.
[472] Fifth recital of the PLD.
[473] See for example European Commission 2018, p. 3.
[474] Recital 14, article 9 PLD.
[475] Recital 17, article 12 PLD.
[476] See recitals 8-10 and article 3-5 PLD.

furnishes proof as to the existence of certain exonerating circumstances". These defences protecting the producers' interests include the following.[477] A producer is not liable when he can prove *inter alia* that: the defect came into existence after the product was put into circulation;[478] the defect was the result of compliance with mandatory regulations issued by public bodies;[479] and when the – optional – defence applies that he can prove that it was impossible to discover the defect given the state of the technical knowledge at the time of putting the product into circulation.[480] Also the threshold of € 500,- which must be met in order to be rewarded damages,[481] the fact that the burden of proof regarding damage, defect and causal relationship rests on the shoulders of victims,[482] and the limitation periods within which damages must be claimed,[483] were intended to protect producers.

After four reports on its functioning,[484] a first full scale evaluation took place of the PLD took place in 2018 by the European Commission,[485] which was accompanied by a fifth report.[486] The directive is still considered as "a useful tool for protecting injured persons and ensuring competition", but there are some imperfections: "there are cases where costs are not equally distributed between consumers and producers", which "is especially true when the burden of proof is complex, as may be the case with some emerging digital technologies […]."[487] The European Commission thus announced to further investigate *inter alia* the PLD in relation to new technologies (including robotics, the internet of things and artificial intelligence), and may update some aspects of the PLD, "such as the concepts of 'defect', 'damage', 'product' and 'producer'," although without altering the strict liability principle.[488] These concepts are explored further below, including some general remarks in view of new (AV) technologies. Implications of the currently applicable PLD provisions on AV technology specifically, are – in the light of the case study introduced in section 3.5.

4.2.2.2 Products

Products are defined in article 2 PLD as "all movables, with the exception of primary agricultural products and game, even though incorporated into another movable, or into an immovable […]". Furthermore, electricity is expressly included in the definition. It follows from the 7th recital that

[477] See also 4.2.2.8.
[478] Article 7(1)(b) PLD.
[479] Article 7(1)(d) PLD.
[480] Article 7(1)(e) PLD.
[481] Article 9(1)(b) PLD.
[482] Article 4 PLD.
[483] Article 10 PLD.
[484] See supra fn. 470.
[485] European Commission 2018a.
[486] European Commission 2018.
[487] European Commission 2018, p. 8-9.
[488] European Commission 2018, p. 10.

these movables should be *industrially produced* in order to be addressed by the PLD. However, this notion seems to have lost most of its relevance after the *Veedfald* decision of the European Court of Justice.[489]

> *Henning Veedfald had to undergo a kidney transplantation in Skejby Hospital in Denmark. His brother offered him one of his kidneys, which was removed from the brother's body and subsequently treated with a perfusion fluid. This perfusion fluid was defective, i.e. it caused a blockage in the main artery, which rendered the kidney unusable. The fluid was specially made for this respective treatment by another (public) hospital, the Århus District Hospital. One of the prejudicial questions was whether "a defective product is not put into circulation when the manufacturer of the product makes it and uses it in the course of providing a specific medical service, consisting in preparing a human organ for transplantation, and when the damage caused to the organ results from that preparatory treatment".[490] Despite the opinion of Advocate General Colomer,[491] who argued that the respective fluid was not industrially produced, the ECJ considered the perfusion fluid to fall under the scope of the 'products' definition.*
>
> *The court held:*
>
> > *"The answer to be given to the first question must accordingly be that Article 7(a) of the Directive is to be interpreted as meaning that a defective product is put into circulation when it is used during the provision of a specific medical service, consisting in preparing a human organ for transplantation, and the damage caused to the organ results from that preparatory treatment".[492]*

The PLD does not define what must be considered as *movables* other than that they must be distinguished from *immovables*. However, the fact that *electricity* is included under the definition, leads to the (a contrario) assumption by some authors,[493] that other intangible goods are not *products* in terms of the PLD. This would implicate that for example data, information and (certain forms of) software are not within the realm of the Directive, although these assumptions are debated, *inter alia* because the CJEU has never explicitly excluded these from the Directive's reach – until recently.[494] In its decision in the *Krone Verlag*-case, the CJEU held that inaccurate medical

---

[489] ECJ 10 May 2001, C-203/99, ECLI:EU:C:2001:258 (*Henning Veedfald/Århus Amtskommune*).
It is however questionable whether for example refurbished products, or products that have been adapted after they have been put into circulation by the producers, would fall outside the scope of the definition. See European Commission 2018, p. 9.
[490] ECJ 10 May 2001, C-203/99, para. 11.
[491] Opinion of AG Colomer in case C-203/99, para. 8 & 13.
[492] ECJ 10 May 2001, C-203/99, para. 18.
[493] See Alheit 2001, p. 200; also Fairgrieve et al. 2016, p. 41-42, and the references included there, to Vansweevelt, T. & Weyts, B., *Handboek buitencontractueel aansprakelijkheidsrecht*, Mortsel: Intersentia 2009, p. 503 and Wuyts 2014, p. 5.
[494] There are authors who qualify software and (digital) information as (electromagnetic) static energy, which must therefore be considered 'tangible' (or: material ('stoffelijk'). See for example Kleve, P. & Mulder, R.V. de, "Voor een goed begrip – Weerwoord naar aanleiding van de reacties op 'De juridische

information printed in a newspaper, cannot be deemed a *product* in sense of the PLD.[495] Whether or not this decision can be extrapolated to for instance software or algorithms, cannot be derived from the CJEU-decision however.

The European Commission did pay attention to 'software' already in 1988. It has responded to the question whether or not the "EEC Directive on product liability also cover(s) computer software", that

> "Under Article 2 of Directive 85/374/EEC [...] the term 'product' is defined as 'all movables, with the exception of primary agricultural products — (not having undergone initial processing) — and game, even though incorporated into another movable or into an immovable'. Consequently, *the Directive applies to software in the same way*, moreover that it applies to handicraft and artistic products" (emphasis added).[496]

Some authors perceive this answer as that software could fall under the scope of the PLD *as long as it is stored on a tangible medium,* and that therefore the PLD does not apply in situations where software is provided in a non-physical way, for instance over the internet, or otherwise as a service.[497] The validity of the assumption that software needs a carrier in order to fall under the scope of the Directive can be questioned: the answer of the Commission cited above could also be read as holding that the product-definition entails software, as well as software embedded therein, or (slightly differently) that the directive is likewise applicable to 'products' in terms of article 2 PLD, and to software. It seems undebated that the PLD applies to software that is embedded in hardware (i.e. a movable), in case this software is essential for the functioning thereof.[498] Until the CJEU has provided more clarity in this regard, or the Commission has taken further steps as announced in the evaluation of the PLD, it will remain *inter alia* unclear whether or not software can be considered 'movable'; what the status is of for example non-embedded software; software that is provided as-a-service (without one specific physical carrier that has been provided to a consumer); and software that can be used in combination with certain

---

status van software', *NJB* 1990, p. 283 – 285, as referred to in Westerdijk 1995, p. 83, who – in my opinion correctly – observes that a too broad conception of what should be considered tangible.

[495] CJEU 10 June 2021, C-65/20, ECLI:EU:C:2021:471 (*Krone Verlag*), para 42.

[496] Answer given by Lord Cockfield on behalf of the Commission on the written question No. 706/88 by Mr. Gijs de Vries (LDR-NL) (89/C 114/76), *OJ* 8-5-1989 No. C 114/42, available via https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1989:114:FULL:EN:PDF. See also Vellinga 2020, p. 144.

[497] See Alheit 2001, p. 200; and Fairgrieve et al. 2016, p. 47; Wuyts 2014, p. 5-6; Westerdijk 1995, p. 84. Westerdijk however advocates a broader conception: where one can exercise control over certain software, which can be individualised, and which furthermore represents certain value, it should be considered a product in terms of the PLD (p. 86).

[498] See Fairgrieve et al. 2016, p. 47. Alheit advances further on p. 201 that when (AI) software has material output, for instance a robot that moves, this would amount to a product.

hardware, albeit the respective hardware could also function without the software.[499] Also, where traditionally the PLD distinguishes between *products* (in scope) and *services* (only then in scope when connected to a product),[500] it is questionable whether or not the PLD sees to non-embedded software services which is for instance "streamed" to an AV.[501]

> It seems evident that an AV can be considered a product in its entirety, and that the hardware components (mechanical parts, such as brakes, wheels, steering wheel, sensors et cetera) are products too. Software components, such as the operating software that an AV was equipped with when it was initially sold, will likely qualify as a product too, as this software will be necessary to operate the vehicle. Less obvious would be whether or not software-updates, later add-ons containing 'new' features for the AV – which may even be the result of self-learning capacities, or software that is streamed (thus without durable 'fixation' within the AV) – which may be the case with for instance real-time instructions based on live traffic information, would be products under the PLD-definition too.
>
> It is relevant to mention that it follows from a Dutch Supreme Court decision that it cannot be too easily assumed that a product must be seen as a sum of its components (in The Netherlands).[502] The court held that a hip-prosthesis which consisted of four components cannot be regarded as a single product upon implementation in a human body, but should rather – in order to determine the extinction periods for filing a product liability claim – be regarded as four individual products. Although this case did not relate to a combination of software and hardware, the "evidence" that the foregoing section started with should be nuanced somewhat, at least regarding the product-definition in The Netherlands.

There is a similar academic discussion regarding information and data.[503] Some argue that (defective, false or flawed) information that has not been bound to a specific carrier, cannot fall under the product-definition – which could be the case if the information would for instance be incorporated in a book, or on paper.[504] Fairgrieve et al. argue that

> "the acceptance that defective information as such could give rise to liability of the producer of that information would be in line with an effective application of the Product

[499] See also European Commission 2020 (report of the Expert Group on Liability and New Technologies), p. 28; Bertolini 2020, p. 57. The recent CJEU *Krone Verlag* decision does not change these observations. Contrarily, it might be derived from the courts' observation in para. 21 that a "poisonous binding of a book or poisonous ink" might render a book *defective*, that this could implicate that when a product itself (e.g. a car) becomes hazardous and causes damage as a result of defective software, may be qualified *defective* accordingly.
[500] Bertolini 2020, p. 57, referring to *inter alia* CJEU 21 December 2011, C-495/11 (*Dutreux*).
[501] European Commission 2020, p. 28.
[502] See Hoge Raad 16 July 2021, ECLI:NL:HR:2021:1172 (*Zimmer Biomet*).
[503] See for a disambiguation between data, information, knowledge and wisdom further section 2.2.
[504] See for example Geddes, A., *Product and service liability in the EEC*, London: Sweet & Maxwell 1992, p. 10 and Van de Gehuchte, *Productaansprakelijkheid in België,* Gent: Mys & Breesch 2000, p. 36, both referred to in Fairgrieve et al. 2016, p. 48; Alheit 2001, p. 200-201.

> Liability Directive. It would also attribute to an application of the directive that is favourable to the interests of consumers",[505]

although that might be not in line with the interests of producers, and similar points of view have been criticised in literature.[506] As it seems however, the current *Krone Verlag*-decision of the CJEU should be interpreted as such that defective information cannot be included under the *product* definition.[507]

4.2.2.3 Defectiveness

Consumers may reasonably expect that the products they acquire, are free of defects.[508] A product is considered *defective*, when "it does not provide the safety which a person is entitled to expect, taking all circumstances into account".[509] The PLD provides a non-limitative list of three of such circumstances, "including: a) the presentation of the product; b) the use to which it could reasonably be expected to be put; [and] c) the time when the product was put into circulation. The second section provides furthermore that defectiveness cannot result from the fact that "a better product is subsequently put into circulation".

It follows from CJEU case law that in order to determine the *expectations* that persons are entitled to, one must adhere to the "reasonable expectations of the public at a large",[510] which are to be assessed on the basis of an objective,[511] normative test.[512] The *legitimate* expectations are taken into account in this regard, rather than the *actual* expectations of the public.[513] These legitimate expectations include *inter alia* "the intended purpose, the objective characteristics and properties of the product […] and the specific requirements of the group of users for whom the product is intended".[514] Furthermore, it was held in the same case – which was about a very specific type of products, i.e. pacemakers and implantable cardioverter defibrillators – that if products of the same series have a potential defect, the entire line of products can be considered defective.[515]

---

[505] Fairgrieve et al. 2016, p. 50.
[506] See Westerdijk 1995, p. 82 and more specifically his references in footnote 31.
[507] CJEU *Krone Verlag*, para. 42.
[508] Van Dam 2013, p. 428.
[509] Article 6(1) PLD.
[510] CJEU 5 March 2015, joined cases C-503/14 and C-504/14 (*Boston Scientific Medizintechnik GMBH*), para. 37.
[511] See Van Dam 2014, p. 429; Fairgrieve et al. 2016, p. 51-52 (also pointing out that when a specific group of consumers is targeted by the producer, the reasonable expectations of the average member of that group has to be taken as a point of departure); Engelhard & De Bruin 2018, p. 16.
[512] Fairgrieve et al. 2016, p. 52-53. See also Deakin, Johnson & Markesinis 2013, p. 615-617.
[513] Deakin, Johnson & Markesinis 2013, p. 617; Fairgrieve et al. 2016, p. 52-53.
[514] CJEU Boston Scientific Medizintechnik GMBH, para. 38.
[515] Ibidem, para 41-43.

It must be noted that a distinction is made between different types of defects in the case law of the Member States: manufacturing defects, instruction defects and design defects.[516] Manufacturing defects are defects in individual products, which therefore do not meet the general quality standards that are typical for the other products of the same type or series.[517] Design defects are the result of a defective product design, and information/instruction defects may result from insufficient warnings concerning possible side effects, for instance in the user manual.[518] Consumers may especially expect products to be free of *manufacturing* defects, where design or instruction defects can to a certain extent be neutralized by providing adequate information in that regard to consumers.[519]

> For example failing brakes, or failing radar/lidar-sensors will qualify as **manufacturing defects**, as the respective AV-component-design would prescribe working brakes and radar/lidar-sensors. If a producer fails to mention certain safety hazards, for example that a vehicle may not contain more than 5 passengers of a certain weight in the instruction manual, and/or upon 'passenger-boarding', this may constitute an **instruction defect**. **Design defects** affect a multitude of AVs of the same type, and may be the result of too limited testing scenarios.[520]

The circumstances that could be taken into account in the assessment of defectiveness include the *presentation of the product*. In that regard, it is indicated that this presentation must be taken broadly, and includes "marketing, advertisements, packaging, instructions, warnings" et cetera.[521] Especially within the domain of high-tech products, omissions of and inaccuracies in information regarding risks may infer defectiveness.[522] Van Dam observes that safety warnings may not preclude defectiveness, when it would be possible to "produce a safer product without an additional financial burden and this higher safety level does not affect the benefit of the product".[523] It can be questioned however, to what extent producers may use a financial burden argument in that respect: should the financial hurdle to produce a safer product be rather low, they might have to take that hurdle in order to replace the less safer one.

---

[516] Engelhard & De Bruin 2018, p. 16-17, and Fairgrieve et al. 2016, p. 53, who distinguishes between on the one hand manufacturing defects and on the other hand design and instruction defects.
[517] Van Dam 2013, p. 428 illustrates manufacturing defects using the example of a bottle that explodes due to hairline cracks in the glass.
[518] Van Dam 2013, p. 428; Engelhard & De Bruin 2018, p. 16.
[519] Van Dam 2013, p. 428; Engelhard & De Bruin 2018, p. 17.
[520] Engelhard & De Bruin 2018, p. 16. See also Van Wees 2015, p. 172-173.
[521] See Van Dam 2013, p. 428; Fairgrieve et al. 2016, p. 56-57.
[522] Ibidem. Fairgrieve et al. et al. Furthermore hold that not *every* risk would have to be warned for by the producers under the European PLD-regime. It would for instance not be necessary to warn that one should not put a dog in a microwave oven in order to dry the animal. (p. 57-58).
[523] Van Dam 2013, p. 428.

Besides *presentation*, also the *reasonable expected use of the products* can be assessed in order to examine defectiveness. Producers are to take notice of certain forms of unintended (hence sometimes unsafe or improper) use of their products by consumers, when either designing their products, or warning for the risks involved in unintended forms of use.[524] Should the producer fail to prevent the unintended uses in his design, or fail to warn the customers for the hazards that may result from unintended use of his products, this may constitute defectiveness.[525] It is considered that "[i]gnoring explicit and multiple warnings" may construe a serious (negligent) abuse of the respective product, but would not always (automatically) lead to the conclusion that defectiveness is excluded.[526]

To conclude the non-exhaustive list under 6(1) PLD, the *time when a product was put into circulation* can also be evaluated. This implicates that the defectiveness-assessment must be carried out against the safety requirements that applied when the introduction on the market of the actual specimen of the product took place. Article 6(1)(c) PLD must be read alongside 6(2) PLD, which holds that the introduction of a new product, does not entail the defectiveness of its predecessor. However, when a product wears out too quickly, it may in some cases be considered defective.[527]

> It is not always clear when an AV product can be qualified 'defective'. A badly installed traffic-light sensor in an AV can rather easily be held defective, as the public may expect that AV are equipped with working red-light-recognition devices. It would be harder to determine which general level of road-safety may be reasonably expected: may the public expect AVs to be as good as the 'average' human driver? Or should 'excellent', or 'beyond excellent' driving skills be expected? And what does that actually entail?[528] In the literature, different opinions are reflected. Schellekens for instance observes that "automated cars are expected to be safer than human driven cars".[529] In the Robolaw-report, it is stated that "the public at a large is entitled to expect the automated car to be as safe as a human driven car".[530] The required safety levels will eventually have to correspond with the levels of safety that are technically achievable, where, in my opinion, the safety level of human driven cars should be the absolute minimum.
>
> Furthermore, it can be questioned whether or not software vulnerabilities which in turn (could) lead to hacking,[531] or software that contains bugs or errors causing AVs to malfunction,

[524] Van Dam 2013, p. 428-429.
[525] See also Pape, S.B.B., *Warnings and product liability* (diss.), Den Haag: Eleven International Publishing 2011, p. 64.
[526] Fairgrieve et al. 2016, p. 60.
[527] Van Dam 2013, p. 429. See also Fairgrieve et al. 2016, p. 60-61.
[528] See Engelhard & De Bruin 2018, p. 17.
[529] Schellekens 2015, p. 517.
[530] Robolaw 2014, p. 57.
[531] Hacking can be understood as all activities in which AV technology is used in other ways than intended by the producer. See Engelhard & De Bruin 2018, p. 49,

would render the software defective. There is evidence available that vehicles can be hacked into (i.e. by breaking through, or circumventing security measures), and that the operation of vehicles can be taken over by external actors – with severe safety risks as a result.[532] On the one hand, it can be argued that reasonable expectations of the public should include that AVs are equipped with 'safe' software. On the other hand, it is unavoidable that software will always contain certain bugs and vulnerabilities, as it is technically improbable that any flaws are eliminated. It can be construed however, that consumers may expect producers to undertake any reasonable efforts to avoid – and, should bugs be uncovered or –worse – systems hacked, warn consumers and repair the leaks. However that would still be, considering the current contents of the PLD and applicable case law, up to the courts to determine.[533] A parallel can be drawn in this regard with the renewed Consumer Sales Directive (CSD).[534] Besides traditional "tangible goods",[535] the CSD also applies to "tangible movable items that incorporate or are inter-connected with digital content[536] or a digital service[537] in such a way that the absence of that digital good or digital service would prevent the goods from performing their functions".[538] Under the CSD, sellers of "goods with digital elements" have to make sure that each "consumer is informed of and supplied with updates, including security updates, that are necessary to keep those goods in good conformity"[539] for a certain period of time. It can be argued that, apart from a non-conformity claim under the CSD, a consumer should at the same time be able to make a *defectiveness* claim under the PLD when security-updates are *not* provided in spite of the sellers (or in this case: producers) obligation to do so.

Victims have to prove defectiveness,[540] which can be challenging if it concerns a technically complicated product. Whereas it would be less complicated to prove the existence of hairline cracks in the glass of an exploded bottle (that is: when the respective specimen is still available for examination), it would be for instance far less easy to prove a bug in the operating software of AVs which lead to defectiveness, as the latter would require much more specialised skills than the former. This is acknowledged by the Commission, who stated in its fifth report that: "there are

---

[532] See Greenberg, A., *Uber hires the hackers who wirelessly hijacked a jeep*, Wired 2015, viewed March 1 2019, available at http://www.wired.com/2015/08/uber-hires-hackers-wirelessly-hijacked-jeep/. See also Garfinkel S., *Intelligent Machines - Hackers Are the Real Obstacle for Self-Driving Vehicles*, MIT Technology Review, 22 August 2017, available via https://www.technologyreview.com/s/608618/hackers-are-the-real-obstacle-for-self-driving-vehicles/ (last accessed 1 March 2019).

[533] See Engelhard & De Bruin 2018, p. 50-51.

[534] Directive (EU) 2019/77 of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, *PJ*, L 136/28 (Consumer Sales Directive, CSD).

[535] Article 2(5)(a) CSD: "any tangible movable items; water, gas and electricity are to be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or a set quantity".

[536] Article 2(6) CSD: "data which are produced and supplied in digital form".

[537] Article 2(7) CSD: "(a) a service that allows the consumer to create, process, store or access data in digital form; or(b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service".

[538] Article2(5)(b) CSD.

[539] Article 7(3) CSD.

[540] Article 4 PLD.

cases where costs are not equally distributed between consumers and producers. This is especially true when the burden of proof is complex, as may be the case with some emerging digital technologies or pharmaceutical products".[541] However, courts in the Member States tend to aid consumers sometimes, as they are generally do not require victims to deliver very specific technical details of the alleged defects.[542] In this regard, the CJEU-decision W/Sanofi Pasteur must be mentioned. In this decision, the Court held that, when the de defectiveness of a vaccine is uncertain, i.e. when there is no scientific evidence available of the defectiveness (and the causal relationship between the vaccine and specific disease), the application of evidentiary rules that aid the victims in delivering requisite proof, can be allowed to a certain extent.[543] A certain level of technological knowledge is however still required in order to underpin a defectiveness-claim.[544]

4.2.2.4 Producers

The producer is the "*manufacturer* of a *finished product*, the producer of any *raw material* or the manufacturer of a *component part*, and any person whom by putting his name, trade mark of other distinguishing feature on the product *presents himself as its producer*" (emphasis added).[545] This provision creates, together with article 5 PLD (see below) a one-stop-shop for victims of damage that resulted from defective products, as almost any actor in the production process (apart from for instance the product designer or a sole service provider[546]) can be sued. It must be noted however that component producers cannot be held responsible for instruction defects (as addressed in section 4.2.2.3), as a consequence of the specific defence in article 7(1)(f) PLD, which exempts the component manufacturer from liability who was following up on orders of the producer of the end-product.[547]

The consumers' position is strengthened further: besides that all actors in the production process, also those who import products into the EU, "for sale, hire, leasing or any form of distribution in the course of business" are deemed producers by article 3(2) PLD, whereas this provision also

[541] European Commission 2018, p. 8-9. See also Engelhard & De Bruin 2018, p. 17. Furthermore, courts of the Member States sometimes use different approaches in determining defectiveness. See sections 4.2.3 - 4.2.5 below.
[542] From the UK case *Hufford v. Samsung Elektronics (UK) Ltd.* [2014] EWHC 2956 (Technology & Construction Court), para 25, ref. to *Ide v ATB Sales Ltd. & Lexus Financial Services v. Russel* [2008] *PIQR*P13; [2008] EWCA Civ 424 (reference and following quotation taken from Engelhard & De Bruin 2018, p. 18), it follows that a claimant will "not have to specify or identify with accuracy or precision the defect in the product […]. It is enough for a claimant to prove the existence of a defect in broad or general terms, such as 'a defect in the electrics of the Lexus (motor car)'.
[543] CJEU 21 June 2017, C-621/15, ECLI:EU:C:2017:484 (*W/Sanofi Pasteur*). See for an analysis of this decision and its implications Veldt & Wissink 2017. See 4.2.3 for further elaboration of the W/Sanofi Pasteur decision.
[544] See Engelhard & De Bruin 2018, p. 18; European Commission 2020, p. 28; Bertolini 2020, p. 57-58.
[545] Article 3(1) PLD.
[546] See Fairgrieve et al. 2016, p. 61, 71; see for another thorough overview on "the parties to the action": Deakin, Johnston & Markesinis 2013, p. 607-613.
[547] See Engelhard & De Bruin 2018, p. 13, and furthermore section 4.2.2.8.7.

entails that a victim does not have to sue a non-EU producer, when there is an importer 'available' who can be sought for compensation.[548]

Should it be impossible for a victim to identify a producer, he may instead sue "each supplier of the product", which implies that also the sellers of products can be held liable in those cases, *unless* the supplier "informs the injured person within a reasonable time, of the identity of the person or the person who supplied him with the product".[549]

> When for example the radar sensor of an AV is defective, article 2(1) PLD entails that both the sensor producer and the car manufacturer (given that these are different actors) can be held liable. The victim cannot however sue the manufacturer of another component (for example the tyres) than the one that was defective.
>
> Rental, or lease companies other than the first seller of a defective AV, or service providers such as garages may not be held liable under the PLD.[550] These parties may however be liable under general (national) liability rules.

Article 5 PLD provides that when there are "two or more persons liable for the same damage, they shall be liable jointly and severally, without prejudice to provisions of national law concerning the rights of contribution or recourse". This implicates that a victim does not have to sue all possible actors in the production chain, whereas the victim may 'choose' the actor who he deems most fit to receive a damages claim.[551]

4.2.2.5 Victims

Article 4 PLD states that "the injured person" has to prove the "damage, the defect and the causal relationship between defect and damage", and does not specify any further who is considered to be a victim. Article 11 also mentions the "injured person", and article 10(1) refers to the "plaintiff". It can be deduced that any "injured person" (i.e. victim) who suffered either injuries or other damages covered by article 9 PLD can claim damages, as further elaborated in section 4.2.2.7. Whether or not the victim owned or possessed the defective product seems irrelevant.

4.2.2.6 Causation

Whereas article 1 provides that producers are liable for damage *caused* by defects in their products, and article 3 prescribes that it is the victim who should prove damage, defect and *causal relationship between defect* and *damage*, the PLD does not contain rules on how such causation

[548] See Deakin, Johnston & Markesinis 2013, p. 612; Fairgrieve et al. 2016, p. 66.
[549] Article 3(3) PLD.
[550] See for example Van Dam 2013, p. 427 and Engelhard & De Bruin 2018, p. 15.
[551] See Fairgrieve et al. 2016, p. 72.

should be determined.[552] This implicates that it is left to the Member States to stipulate whether or not, or how, for example (just) a *condicio sine qua non*-relationship between defect and damage must be proved, and/or whether or not "additional qualification is necessary, such as directness of the causal link, normality, foreseeability of the damage, lack of remoteness"[553] et cetera. It follows from CJEU case law that it is also up to the Member States to determine

> "the ways in which evidence is to be elicited, what evidence is to be admissible before the appropriate national court, or the principles governing that court's assessment of the probative value of the evidence adduced before it and also the level of proof required."[554]

The fact that causation (largely) remains a matter for regulation in the Member States is seen as "a significant restriction on the harmonisation pursued by the Directive",[555] especially since this may detriment "competition and affect the free movement of goods […] and entail a differing degree of protection of the consumer against damage caused by a defective good to his health or property".[556]

In its *W/Sanofi Pasteur*-decision, the CJEU clarifies however in this regard that it follows from EU law that national rules may not "render [it] practically impossible or excessively difficult [to] exercise […] rights conferred by EU law",[557] which implies that consumers must remain able to prove causation, also in cases where that would be difficult for them to establish, for instance given the technological knowledge required to do so.

> *Mr. W. took Hepatitis-B vaccinations in December 1998, January and July 1999. The vaccines were produced by Sanofi Pasteur. He was diagnosed with Multiple Sclerosis in November 2000, and died in 2011.[558] In 2006, W. started with three family members proceedings against Sanofi Pasteur. As there was no scientific evidence for a causal link between the respective vaccines and the development of Multiple Sclerosis, W et al. relied on an evidentiary rule that follows from French case law. This rule, applicable to the area of liability for pharmaceutical laboratories for the vaccines they produce, holds that*

[552] This was also emphasized in CJEU 21 Juni 2017, C-621/15, ECLI:EU:C:2017:484 (*W/Sanofi Pasteur*), para. 22 and 24; and CJEU 20 November 2014, C-310/13, ECLi:EU:C:2-142385 (*Novo Nordisk Pharma*), para. 25-29.
[553] Fairgrieve et al. 2016, p. 86; see also Deakin, Johnston & Markesinis 2013, p. 622-623.
[554] CJEU 21 Juni 2017, C-621/15, ECLI:EU:C:2017:484 (*W/Sanofi Pasteur*), para. 25.
[555] Fairgrieve et al. 2016, p. 86. Under common law regimes, it is observed that "[t]he rules of causation and remoteness which apply in the tort of negligence may pose a significant barrier to product liability claims […]", Deakin, Johnston & Markesinis 2013, p. 622.
[556] Ibidem Fairgrieve et al. 2016, who however consider that inferring in the current national rules on causation (which are at the heart of the national tort-systems), would "negatively impact the internal cohesion of those systems").
[557] CJEU 21 Juni 2017, C-621/15, ECLI:EU:C:2017:484 (*W/Sanofi Pasteur*), para. 26.
[558] CJEU 21 Juni 2017, C-621/15, ECLI:EU:C:2017:484 (*W/Sanofi Pasteur*), para's. 9-10.

> *"proof of a causal link between the defect in the product and the damage suffered by the person injured can be derived from serious, specific and consistent presumptions, which falls within the remit of the court ruling on the merits in the exercise of its exclusive jurisdiction to appraise the facts".*[559]

The CJEU observes that the PLD does not provide other (evidentiary) rules than that article 4 stipulates that the victim has to prove defect, damage, and a causal relationship between the two.[560] *National courts are, to a certain extent free to*

> *"establish the ways in which evidence is to be elicited, what evidence is to be admissible before the appropriate national court, or the principles governing that court's assessment of the probative value of the evidence adduced before it and also the level of proof required".*[561]

These rules may not render it practically impossible or excessively difficult for victims to deliver such proof,[562] *but on the other hand the apportionment of the burden of proof as regulated in article 4 PLD may not be undermined: national rules may not reverse the burden of proof for example.* [563] *The French rules in question, which*

> *"do not require the victim to produce, in all circumstances, certain and irrefutable evidence of a defect in the product and of a causal link between the defect and the damage suffered, but authorises the court, where applicable, to conclude that such a defect has been proven to exist, on the basis of a set of evidence the seriousness, specificity and consistency of which allows it to consider, with a sufficiently high degree of probability, that such a conclusion corresponds to the reality of the situation",*[564]

is considered to be in line with article 4, as these do not lead to a reversal of the burden of proof. [565]

It is furthermore observed that the effectiveness of the PLD is undermined when only "certain proof based on medical research" would be admissible to prove causation in this respect.[566] *However, unjustified presumptions that detriment the producers are not allowed, which could be the case "where national courts apply those evidentiary rules in an overly rigorous manner by accepting irrelevant or insufficient evidence",*[567] *or "where one or more types of factual*

---

559 Ibidem, para 12.
560 Ibidem, para's. 19, 24.
561 Ibidem, para. 25.
562 Ibidem, para. 26.
563 Ibidem, para. 27, 29.
564 Ibidem, para 28.
565 Ibidem, para 29.
566 Ibidem, para 30-31. This "would also be inconsistent with the objectives pursued by Directive 85/374, seeking to ensure, in particular, as is apparent from the second and seventh recitals thereof, a fair apportionment of the risks inherent in modern technological production between the injured person and the producer (see, to that effect, judgment of 5 March 2015, Boston Scientific Medizintechnik, C-503/13 and C-504/13, EU:C:2015:148, paragraph 42) and, as evidenced by the first and sixth recitals thereof, that of protecting consumer health and safety (see, to that effect, judgment of 5 March 2015, Boston Scientific Medizintechnik, C-503/13 and C-504/13, EU:C:2015:148, paragraph 47)." (para 32). See also Veldt & Wissink 2017, p. 255.
567 Ibidem, para. 35.

evidence were presented together, an immediate and automatic presumption would operate of there being a defect in the product and/or a causal link between that defect and the occurrence of the damage".[568]

Veldt & Wissink, who critically reflect on *inter alia* the ways that the CJEU came to the decision, state that the Court missed the opportunity to further harmonise the material concept of "defectiveness". [569] They observe that four aspects of national evidence rules have been harmonised. In cases like *W/Sanofi Pasteur*, not every form of circumstantial evidence may be precluded by national courts, and it would furthermore be a too high burden for victims to be required to deliver irrefutable evidence based on medical research.[570] Furthermore, a defect and a causal relationship may be presumed when it follows from the seriousness, specificity and consistency of the available evidence, that it is sufficiently probable that such a conclusion corresponds with the reality, especially when this is the most plausible explanation for the occurrence of the damage.[571] Also the number of (possible) occurrences of the damage may play a role in this regard,[572] however automatic and/or irrefutable presumptions at the expense of producers are not allowed.[573]

> An AV (A) crashes into another AV (B). It seems that the radar sensors of B may have failed. It also seems that A was driving at the wrong side of the road, which could be due to a defect in its GPS sensors, which has not been corrected by the road-position camera's. Furthermore, AV A seems to have been hacked; criminals have exploited a previously unknown vulnerability in the software.[574] X, the owner of AV A was injured in the crash and claims damages from producer Y of AV A. Where the financial means of X are limited, and he is not an expert in AV technology, he experiences difficulties in establishing (*inter* alia) the causal link between the defect(s) and the damage he suffered.[575] A court may not reverse the burden of proof: the onus to prove the causation remains with X. X may however be helped: a courts may – as long as national evidence rules would allow so – given the probable defects in the hardware and software of AV A, assume the causal link between the defects and the damage, allowing the producer Y to refute that assumption. In this case, Y may argue that there may have been another obvious cause, by adducing that AV B's radar sensor had failed. Should Y's plea convince the court, the assumption is taken away: it is again up to X to provide evidence of the causal link between the defects in AV A and his damage.

---

[568] Ibidem, para. 36.
[569] Veldt & Wissink 2017, p. 259-260.
[570] Veldt & Wissink 2017. P. 260, referring to para's. 28 and 37 of the decision.
[571] Ibidem,
[572] Ibidem; see their reference to para 41 of the decision.
[573] Veldt & Wissink 2017, p. 260-261; see their references to para's. 35-37, 41 and 45 of the decision.
[574] From 8(1) follows that a producer may still be liable after "a third party has intentionally sabotaged the product"; the laws of the Member States may address the right of recourse vis-à-vis the saboteur. See also Van Dam 2013, p. 433.
[575] That proving causality is a serious challenge for victims, is *inter alia* underscored in Bertolini 2020, p. 58-59; see also European Commission 2020, p. 29-30.

4.2.2.7 Heads of damage

The PLD sees to compensation of

> "damage caused by death or personal injuries", and "damage to, or destruction of, any item of property other than the defective product itself, with a lower threshold of 500 ECU [Euro], provided that the item of property: (i) is of a type ordinarily intended for private use or consumption, and (ii) was used by the injured person mainly for his own private use or consumption".[576]

The PLD does not stand in the way of "national provisions relating to non-material damage. The concept of "damage" is however not defined in the Directive.[577]

It follows from recital 14 that the € 500,- threshold,[578] and the provision that the PLD only relates to non-commercial goods, are meant to "avoid litigation in an excessive number of cases", and that the "Directive should not prejudice compensation for pain and suffering and other non-material damages payable, where appropriate, under the law applicable to the case".

Member States are allowed to place a cap on "a producer's total liability for damage resulting from a death or personal injury and caused by identical items with the same defect", although this cap may not be below € 70 million.[579]

The PLD can thus not be used to base *inter alia* claims of pure economic losses, or claims regarding damage to commercial property, or the defective product itself.[580] This might however be done using other national rules. Also claims regarding damage below the € 500,- threshold, should be based on other than the (implemented) PLD provisions. Furthermore, from the ECJ *Veedfald*-decision follows that claims regarding non-pecuniary loss cannot be awarded on the basis of the PLD.[581] Also, in *Veedfald*, the ECJ has decided that Member States may not limit the types of damage resulting from death, personal injury or property damage.[582]

---

[576] Article 9 PLD.
[577] See Fairgrieve et al. 2016, p. 83, where is observed that "the concept of damage […] is also treated differently in national legal systems. A given type of loss may constitute damage in one legal system, while another legal system might not perceive it as such".
[578] Which is by most Member States seen as a deductible, and not as a threshold, See European Commission 2006, p. 11.
[579] Article 16(1) PLD.
[580] See Van Dam 2013, p. 431.
[581] See Van Dam 2013, p. 432 and ECJ 10 May 2001, C-203/99, ECLI:EU:C:2001:258 (*Henning Veedfald/Århus Amtskommune*).
[582] Van Dam 2013, p. 432 and ECJ 10 May 2001, C-203/99, ECLI:EU:C:2001:258 (*Henning Veedfald/Århus Amtskommune*), para 27; see also Fairgrieve et al. 2016, p. 81-82, where the *Veedfald*-decision and the rather unclear provisions on damages to be compensated are critically reviewed.

Personal injuries caused to *passengers and other road users* will be eligible for remuneration; as will be damage to the vehicles of the victims. Damage to the AV itself cannot be remunerated on the basis of a PLD-claim.

If defective software in an AV leads to a data breach, which in turn leads to identity theft of AV-users, which is subsequently used by criminals to conclude for instance loan agreements, the damage that might result from non-compliance of the contractual obligations to repay the loans, would not have to be remunerated by the producer of the defective software on the basis of the PLD, as it concerns non-economic damages; however there may be other remedies, based on national rules.

4.2.2.8 Limitation of liability

4.2.2.8.1 Time

The PLD provides two limitation periods. Article 10(1) states that the period within which proceedings must start is *three years* from "the day on which the plaintiff became aware, or should reasonably have become aware, of the damage, the defect and the identity of the producer". Article 10(2) stipulates that national rules on suspension or interruption of the limitation period remain applicable to this limitation period. In article 11 PLD, a longer limitation period is regulated: the rights of injured persons shall

> *"be extinguished upon the expiry of a period of 10 years from the date on which the producer put into circulation the actual product which caused the damage, unless the injured person has in the meantime instituted proceedings against the producer".*

Regarding the 10-year-period, the CJEU ruled that a product is put into circulation "when it is taken out of the manufacturing process and enters a marketing process in the form of which it is offered to the public in order to be used or consumed".[583] Furthermore, it has been established at a number of occasions, that national rules stretching the limitation periods, may not be maintained in relation to the PLD-provisions.[584] The rather stringent limitation and extinction periods are commented on in literature, as they inter *alia* imply that the PLD will often not be applicable to defects that manifest themselves after a longer period, which may be the case with previously unknown long-term effects of medicine,[585] or innovative products "which are particularly questionable from a safety perspective and which contain latent defects that first become apparent after a long period of time".[586] For other products, this period can be considered

[583] ECJ 9 February 2006, C-127/04, ECLI:EU:C:2006:93 (*O'Byrne/Sanofi Pasteur*), para. 32.
[584] See Fairgrieve et al. 2016, p. 94, and the references in footnote 376 to applicable ECJ case-law.
[585] See Van Dam 2013, p. 437.
[586] Fairgrieve et al. 2016, p. 95; also: Van Dam 2013, p. 437-438, and Deakin, Johnston & Markesinis 2013, p. 626-627.

too long "and only purely theoretical for rapidly deteriorating products such as food stuffs".[587] Fairgrieve et al. observe furthermore that "[d]espite all justifiable criticism, it also guarantees a high level of legal certainty, especially for manufacturers 0who use new technologies to manufacture their products and who often had high investment costs."[588]

> Some innovations turn out to have harmful consequences or side-effects after long periods of time. Should it at some point appear that for example radar-technology, or other forms of vehicle-to-infrastructure communication may contribute to the development of certain types of disease suffered by AV passengers, the ten-year extinction period may be too short for victims.

4.2.2.8.2 Non-distribution

A producer can defend himself from a product-liability claim invoking the non-distribution defence, if he can prove that "he did not put the product into circulation".[589] A product is already put into circulation as "it is taken out of the manufacturing process and enters a marketing process in the form of which it is offered to the public in order to be used or consumed".[590] It is not relevant whether a manufacturer offered the product to a consumer, or for example another producer. The sole dissemination of a product to a third party constitutes "putting into circulation" in sense of the PLD.[591]

4.2.2.8.3 Later existence of the defect

A producer

> *"shall not be liable if he proves […] that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him, or that this defect came into being afterwards".*[592]

This exception implicates that a producer will not be liable for defects that can be traced back to alterations that happened by another producer, or by the consumer himself.

> When a defect in an AV is the result of an update of the core-software that was executed by another party than the original manufacturer, that original manufacturer may escape liability

[587] Ibidem.
[588] Ibidem, p. 96. Fairgrieve et al. et al. Conclude that "In summary, it can be stated that the present time restrictions in arts 10 and 11 […] do not, in principle, require changes in order to overcome the challenges presented by new technologies as they already contain solutions appropriate to the circumstances.", where they actually point to national regimes which may be applicable after the extinction periods of the PLD.
[589] Art. 7(a) PLD.
[590] ECJ 9 February 2006, C-127/04, ECLI:EU:C:2006:93 (*O'Byrne/Sanofi Pasteur*), para. 32; see furthermore Van Dam 2013, p. 433.
[591] Ibidem Van Dam 2013, p. 433.
[592] Art. 7(b) PLD.

on the basis of this defence, if he can prove that it was "probable" that it was the respective update, rather than the original software, that caused the defect.

It is interesting to evaluate what would happen in terms of this "later existence"-defence when a defect in for example the core-software, occurred or developed after the initial sale, and is the result of the self-learning capacities of an AV (which were present at the time of the initial sale). On the one hand it can be argued that strictly speaking, the respective defect did not exist at the time the AV was deployed. However, on the other hand, the self-learning capacities – and thus the risk of defects as a result thereof, were built in by the producer(s). It will be up to the courts to determine whether this type of "self-learning-defects risks" are to be borne by either the producers or the consumers of AVs.

4.2.2.8.4 Non-commercial manufacture

The defence of article 7(c) PLD holds that a producer will not be liable if he can prove that "the product was neither manufactured by him for sale or any form of distribution for economic purpose or distributed by him in the course of his business". Products that are manufactured "in the course of a specific medical service […] financed entirely from public funds"[593] can however not escape liability on the basis of 7(c).

Such non-commercial production may for example include the manufacture of prototypes that are intended for "inspirational purposes" only.

4.2.2.8.5 Compliance with mandatory rules

When a producer can prove that he complied with "mandatory regulations issued by the public authorities"[594], which caused the defect, he may free himself from being liable for the damage that resulted from that defect.

When an AV manufacturer for instance followed up on mandatory safety standards, which later seemed wrong or incorrect, with a defective product as a result, that producer cannot be held liable.

4.2.2.8.6 Development risks

Article 7(e) PLD provides that a producer can escape liability when he proves "that the state of the scientific and technical knowledge at the time when he put the product into circulation was not as such as to enable the existence of the defect to be discovered". This *development risk defence* was optional for the Member States to include in their national regimes,[595] and has not been incorporated in Finland, Luxembourg,[596] and Norway,[597] Spain regarding medicines and food, and

[593] This follows from CJEU 10 May 2001, C-203/99, ECLI:EU:C:2001:258 (*Henning Veedfald/Århus Amtskommune*), as elaborated by Van Dam 2013, p. 434.
[594] Art. 7(d) PLD.
[595] Art. 15(1)(b) PLD.
[596] See European Commission 2006, p. 10 (third report).
[597] Norway is not a member of the European Union, the PLD is applicable for Norway is within the European Economic Area – and has thus chosen to ecxclude the development risk defence.

France regarding human products, as blood (products).[598] In Germany the development risks defence cannot be used by drug manufacturers.[599]

The ECJ has been strict in considering the obligations for producers in their requisite research of the available "scientific and technical knowledge", as this should include "the *most advanced level of such knowledge*, without any restriction as to the industrial sector concerned" (emphasis added).[600] This entails that it should have been objectively impossible to discover the defect for the producer (regardless of the financial means necessary for the discovery), although the respective information must have been accessible for the producer when he put the product into circulation.[601] While this will include the scientific and technical knowledge that can be accessed via (publicly accessible/indexed parts of) the internet, or found in an (academic) journal, may count as sources that should be taken into account, it may be construed that "knowledge [that] has only been published in a journal which is disseminated in one country and which is not written in a primary language",[602] could be excluded from the diligent search that is due in the producers' discovery.

It follows from German case law that in cases where a defect is, or can be known (hairline cracks in glass bottles), but cannot be avoided, this would not free producers from liability in sense of the development risk defence.[603]

The development risks defence is hardly ever accepted by the courts of the Member States, but this has been the case in The Netherlands,[604] and France.[605] These two will be elaborated further in sections 4.2.3 and 4.2.4.

> Many aspects of AV technology may contain uncertain risks.[606] To name a few: will radar- and vehicle-to-infrastructure communication technology be free of harmful consequences? Which are the yet unknown side-effects of self-learning algorithms on for example collision avoidance after it has been running a few years? How will changes in passenger and other traffic participants' behaviour affect the driving features? Should an unknown risk in a specific AV-

[598] See Van Dam 2013, p. 436.
[599] Ibidem.
[600] ECJ 29 May 1997, C-300/95, *ECR* 1997, I-02649 (*Commission/United Kingdom*), summary and para's 26-29.
[601] See Van Dam 2013, p. 435.
[602] Van Dam 2013, p. 435.
[603] BGH 9 May 1995, VI ZR 158/94 (Sparkling Water Bottle) BGHZ 129, 353; NJW 1995, 2162, as commented on by Van Dam 2013, p. 438, see further references in his footnote 136. See differently Fairgrieve et al. 2016, p. 78, stating that "In essence, the defence contained in art 7(e) boils down to the producer freeing himself from liability by declaring that, while in possession of all knowledge available at a given moment, […] the defect in the product *cannot be avoided*" (emphasis added).
[604] Rechtbank Amsterdam 3 February 1999, *NJ* 1999, 621 (*Scholten/Sanquin Bloedvoorziening*) – although it is questionable whether the Dutch Rechtbank applied this provision correctly.
[605] Cour d'Appel Paris 23 September 2004, D. 2005. 1012.
[606] See Engelhard & De Bruin 2018, p. 20-21.

type materialize after it has been put into circulation, and the producer could not have been aware of its existence, the producer's liability can be excused.[607]

4.2.2.8.7 Component manufacturers

Article 7(f) PLD holds that a component-manufacturer can escape liability if he proves "that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product". This defence is to some extent similar to the defence for "compliance with mandatory rules" (see 4.2.2.8.5) – as it relates to 'external actors' to which a defect can be attributed, but is considered "superfluous […] since it is clear from the other provisions of the Directive that the manufacturer of the component is only liable if its product [i.e. the respective component, *RWdB*] is defective".[608]

4.2.2.8.8 Contributory negligence

When a producer can prove that "the damage is caused both by a defect in the product and by the fault of an injured person […]"[609] his liability may be reduced (pro rata) or disallowed at all. The notion of 'fault', and for example also the standard of care to be expected from victims, is not specified further in the PLD – and is thus left to the Member States.[610]

> Contributory negligence may for instance be construed when the passenger of an AV failed to follow up on instructions, regarding for instance the maximum load of the vehicle; or when an AV-owner who failed to have its vehicle maintained well.[611]

[607] It is observed in the Robolaw-report that the effects of the development risk defence could be very burdensome for consumers, p. 215.
[608] Van Dam 2013, p. 434.
[609] Art. 8(2) PLD.
[610] See Fairgrieve et al. 2016, p. 87-88.
[611] See Engelhard & De Bruin 2018, p. 21.

4.2.3 IMPLEMENTATION IN THE NETHERLANDS

4.2.3.1 Introduction

The PLD is implemented in the Dutch Civil Code (Burgerlijk Wetboek, hereinafter referred to as 'BW') in articles 6:185-193. The scope and wordings of the applicable BW-articles are almost identical to those of the PLD.[612] Whereas the PLD leaves the implementation of the development risks defence open to the Member States, it must be noted here that this defence has been incorporated in the Dutch regime.[613] Furthermore, the option that follows from article 16(1) PLD to place a cap on "a producer's total liability for damage resulting from a death or personal injury and caused by identical items with the same defect", was not used by the Dutch legislator.[614]

A product liability claim can, notwithstanding the implemented PLD, also be based on the general fault based liability rules that are incorporated in articles 6:162 and following BW by an injured person,[615] or, when defectiveness of a product constitutes a breach of contract, on the general provisions of contractual liability law as incorporated in articles 6:74 and following BW.[616] Both regimes (6:162 and 6:74 BW) will be referred to occasionally, however focus is on the PLD in the next sections. I will address the main aspects of the PLD implementation that were left to the national regimes of the Member States, and some 'local' interpretation of the European rules as follows: the notion of defectiveness and unlawfulness (section 4.2.3.2), the concept of damage (section 4.2.3.3), aspects of causation (section 4.2.3.4) and issues of proof (section 4.2.3.5).

4.2.3.2 Defectiveness and unlawfulness

The Dutch Supreme Court interprets the defectiveness criterion that is implemented in article 6:186(1) BW, as such that a product is defective, when it causes damage when used normally, in conformity with the purposes it was marketed for.[617] Should it be that a product, which was used normally, i.e. in conformity with its purpose, causes damage, it can be held that it does not "provide the safety which a person is entitled to expect". As stated in section 4.2.2.3, some Member States differentiate between several kind of defects. Such a differentiation has not been made in the Dutch implementation of the PLD, but from the literature, it follows that (for sole categorisation

[612] See Giesen, De Jong & Muslat 2017, p. 6-7; Keirse 2016, p. 314; see also Hartkamp & Sieburgh 2019, no. 260.
[613] Article 6:185(1)(e) BW, see furthermore section 4.2.2.8.6.
[614] See also Van Dam 2005, p. 126k Keirse 2016, p. 314.
[615] See Keirse 2016, p. 313; Hartkamp & Sieburgh 2019, no. 258-259; and Van Dam 2005, p. 126-128.
[616] See Hartkamp & Sieburgh 2016, no. 257.
[617] See Hartkamp & Sieburgh 2019, no. 259, and their references to HR 6 December 1996, *NJ*1997/219 (*Du Pont/Hermans*); HR 22 October 1999, *NJ* 2000/159, ECLI:NL:HR:ZC2994, C98/043HR (*Koolhaas/Rockwool*); HR 22 September 2000, *NJ* 2000/644, ECLI:NL:HR:2000:AA7239 (*Haagman/Vaessen-Schoenmaker);* also HR 13 January 2017, ECLI:NL:HR:2017:32 (*DAF/Achmea*).

purposes) one can distinguish *manufacturing, design (or presentation)*,[618] and *instruction* defects.[619]

Furthermore, it must be noted that, although that does not follow from the PLD nor the Dutch implementing provisions, certain duties of care have for producers been developed in Dutch case law and literature.[620] From the Supreme Court decision in the *Koolhaas/Rockwool* case, it follows that producers are obliged a) to take those measures that can be expected from a 'careful producer' which are necessary to prevent that the products that he puts into circulation cause damage; and b) to ascertain which effects can be expected from a new or a renewed product, on the obviously potential ('voor de hand liggende') applications thereof; and c) to inform end-users and/or consumers accordingly of changes in his product (rather than just the direct purchasers of semi-finished products).[621]

Whenever a claim is based on article 6:162 BW rather than 6:185 BW, which is allowed as this generic system is an 'older' regime in sense of article 13 PLD, there are different criteria that must be met in order to assess whether or not a producer can be held liable. These include (put very simply) *inter alia* that: a person must have committed an unlawful *act* which can be *attributed* to him and which *caused* another person to have suffered *damage*.[622] In order to establish whether or not a producer acted 'unlawfully' by putting a litigious product on the market, the Dutch Supreme Court connected with the criteria from art. 6:185 BW, and ruled that it is unlawful to put a product on the market "that does not offer the safety that the user/consumer is entitled to expect, taking all circumstances into account"[623] and assesses defectiveness in sense of 6:185 in order to constitute unlawfulness in the sense of 6:162.[624]

---

[618] Keirse 2016, p. 320; Hartkamp & Sieburgh 2019, no. 263.
[619] Hartkamp & Sieburgh 2019, no. 263.
[620] There are however obligations to warn for certain dangers, which follows from case law regarding general tort-law rules (art. 6:162 BW), including for instance HR 5 November 1965, ECLI:NL:HR:1965:AB7079 (*Kelderluik*); and HR 28 May 2004, ECLI:NL:HR:2004:AO4224 (*Jetblast*).
[621] HR 22 October 1999, ECLI:NL:HR:ZC2994, C98/043HR, (*Koolhaas/Rockwool*), *NJ* 2000, 159, as annotated by A.R. Bloembergen, and as analysed in Keirse 2016, p. 322-333. Keirse furthermore underlines that more general information-obligations towards consumers have been advocated for in the literature. These obligations of a careful producer were later affirmed in *inter alia* HR 13 January 2017, ECLI:NL:HR:2017:32 (*DAF/Achmea*).
[622] See http://dutchcivillaw.com/legislation/dcctitle6633.htm (last accessed 28 May 2019); and do note that there is a fifth criterion in art. 162(3), which is formulated as a defence, which holds that "There is no obligation to repair the damage on the ground of a tortious act if the violated standard of behaviour does not intend to offer protection against damage as suffered by the injured person." (source ibidem).
[623] See Giesen 2001, p. 217 for a commentary on this subject, and his references to HR 30 juni 1989, *NJ* 1990, 652 , annotated by C.J.H Brunner (*Halcion*). Giesen cites the quote translated above by me, which reads in Dutch: "[indien het product] 'niet de veiligheid bidet die de gebruiker/consument gerechtigd is te verwachten, alle omstandigheden in aanmerking genomen'".
[624] See for example HR 13 January 2017, ECLI:NL:HR2017:32 (*DAF/Achmea*), section 3.3.3-3.3.4; HR 22 September 2000, ECLI:NL:HR:2000:AA7239 (*Haagman/Vaessen-Schoenmaker), and* HR 30 juni 1989, *NJ* 1990, 652 , annotated by C.J.H Brunner (*Halcion*).

4.2.3.3 Damage

Article 6:190 BW quite literally implements article 9 PLD, and relates to damage caused by death or personal injuries and damage to or destruction of consumer property (other than the respective product), which are eligible for remuneration. As article 9 PLD does not prejudice "national provisions relating to non-material damage", it is relevant to mention article 6:106 BW, which sees to the remuneration of "other damage than financial losses".[625] In short, there may be a right to compensation when either 1) the victim is physically injured, or 2) when his honour or reputation is injured, or 3) if he is harmed otherwise in his person. It must be noted, that unlawful behaviour resulting in mental harm can under certain circumstances result in the obligation to remunerate damages, under the third point addressed above. That may be so in cases of "objectifiable mental harm" (objectiveerbaar geestelijk letsel).[626] Mental harm is deemed objectifiable, when this can be substantiated by psychiatric or psychological evidence, for example based on clinical pictures recognised in psychiatry.[627] Evidence of objectifiable mental harm is however not always necessary to get awarded damages: sometimes *other harm in person* suffices. Besides more or less traditional defamation cases, also infringements of other fundamental rights or interests *could* form a source for an obligation to remunerate damages, such as discrimination, sexual abuse, child abduction and kidnapping.[628] However, such other harm needs to be substantiated with evidence, and a general reference to "principles of reasonableness and equity" (*redelijkheid en billijkheid*) is in that respect not sufficient.[629] Thus, concrete evidence is necessary in order to be successful in an immaterial damages-claim based on *other harm in person*. Substantiation is only then not (entirely) necessary, when the norm violation which gave rise to the damage, was of such a nature or severity that the negative consequences for the victims were "so obvious that *other harm in person* can be presumed".[630] It is not (yet) entirely clear when these

[625] "Nadeel dat niet in vermogensschade bestaat". Such damage may be eligible for an equitable remuneration if a) "the liable person had the intention to inflict such damage"; or if b) "the injured person sustained physical injuries or if his honour or reputation is injured or if he is harmed otherwise in person"; or if c) "the damage consists of harming the memory of a deceased and is inflicted to the not legally separated spouse, the registered partner or a blood relative up until the second degree of the deceased, provided that the memory of the deceased is harmed in such a way that the deceased himself, if he would still be alive, could have claimed damages for injuring his honour or reputation." See for the source of this non-official translation of article 6:106 BW: http://www.dutchcivillaw.com/legislation/dcctitle6611bb.htm (last accessed 19 April 2019; please note that this translation does *not* include the act concerning the remuneration of emotional loss (Wet Vergoeding Affectieschade) which entered into force on 1 January 2019).

[626] See Hoge Raad 15 maart 2019, ECLI:NL:HR:2019:376, *NJ* 2019/162, annotated by S.D. Lindenbergh (*EBI*), in that respective annotation, no. 8-9. See also R. Rijnhout, "Het EBI-arrest, historisch onrecht, effectieve remedie en de AVG", *Tijdschrift voor Personenschade* 2020, no. 1., p. 1-6.

[627] Ibidem.

[628] Ibidem, no. 13-16.

[629] Hoge Raad 15 October 2019, ECLI:NL:HR:2019:1465.

[630] Ibidem, cons. 2.3.2: "[…] indien de aard en de ernst van de normschending meebrengen dat de in dit verband relevante nadelige gevolgen daarvan voor de benadeelde zo voor de hand liggen, dat een aantasting in de persoon kan worden aangenomen".

situations occur, although it follows from case law that a burglary (which qualifies as a violation of the fundamental right of privacy) in which jewellery with emotional value is stolen, is not sufficient for such a presumption.[631]

Non-material resulting from physical damage in relation to awarded product liability claims can be eligible for remuneration, as follows from case law of the lower courts in Netherlands.[632]

> When as a result of a defective AV that crashed into a tree, an injured passenger would for example have to miss a limb, the victim may be awarded immaterial damages, besides damage that directly relates to the respective injury (such as medical costs, losses resulting from the capacity to earn money et cetera). For example, the victim who suffered severe burns on the legs as a result from coming into direct contact with liquid concrete, was awarded € 5.000,-; and the victim who had to miss an eye due to defective fireworks was awarded with € 25.000,- in immaterial damages.[633]

When the damage caused by a defective product led to the death of a victim, the liable producer can be required to remunerate the damage that exists in the "loss of the deceased's prospective income", which follows from article 6:108(1) BW.[634] Such claims can be awarded to a) the legal spouse or registered partner and minor children of the deceased; b) other blood- or legal relatives who were financially supported by the deceased; c) persons who lived together with the deceased before the damage-inflicting event; and d) those who co-habited with the deceased in a family relation. The heads of damage in such cases may also include the costs of the funeral and the disposal of the dead (by anyone who bore these costs, irrespective of the relationship with the deceased).[635] Next to the victim who suffered personal (or mental) injury and who can claim damages under 6:190(1)(a) BW, also a third party who made costs on behalf of the victim may opt for remuneration, which can be awarded as long as the victim could have recovered these damages himself.[636] Since January 1st 2019, also immediate next-of-kin of a person who suffered serious and permanent injury,[637] or of a person who died, for which another person is liable,[638]

---

[631] Ibidem, cons. 2.4.2.
[632] District Court Middelburg 13 July 2005, ECLI:RBMID:2005:AZ5281 (*Claimant/Vlissingse Transportbeton Onderneming*) and Court of Appeal Leeuwarden 8 February 2011, ECLI:NL:GHLEE:2011:BQ0194 (*Claimant/Evuco Vuurwerk*), as both discussed in Keirse 2016, p. 331.
[633] Ibidem.
[634] See for the source if this non-official translation of article 6:108 BW: http://www.dutchcivillaw.com/legislation/dcctitle6611bb.htm (last accessed 19 April 2019). See regarding the applicability of this respective provision Hartkamp & Sieburgh 2019, no. 268 and Keirse 2016, p. 327-328.
[635] Article 6:108(2) BW; See furthermore Keirse 2016, p. 329.
[636] Article 6:107 BW; See furthermore Keirse 2016, p. 328; Hartkamp & Sieburgh 2019, no. 268.
[637] This must considered to be *very* serious injury. See Lindenbergh 2018, p. 3, who mentions that in this respect situations must be considered as for example 70% permanent functional invalidity, or very serious mental impairment.
[638] See also Lindenbergh 2018, p. 2, elaborating that the right of those next-of-kin is derived from the right of the injured or deceased against a tortfeasor.

may claim non-material damages from a tortfeasor.[639] Which injuries qualify as "serious and permanent",[640] and the amounts of damages to be remunerated, are elaborated in orders by council ("algemene maatregelen van bestuur").[641] These amounts of so called "affectieschade" to be remunerated vary from €12.500 to € 20.000,- depending on the nature of the relationship with the injured or deceased, the nature of the norm-violation and type of damage (injury or death), and is seen to serve an acknowledgement purpose rather than a compensation purpose.[642]

Article 9(b) PLD mentions a threshold of € 500,- for damage to "any item of property, other than the defective product itself". This threshold is seen by the Dutch legislator as a franchise: any property damage below € 500,- will not be remunerable under the implementation in article 6:190(b) BW. But, if property damage exceeds € 500,-, the whole amount of the damage (thus without deduction of the first € 500,-) is eligible for remuneration.[643]

Purely financial losses fall outside the scope of damages that could be remunerated based on a product liability claim, however these losses could be remunerable under the general provisions of non-contractual liability law ex article 6:162 BW.[644]

4.2.3.4 Causation

In the Netherlands, there are two requirements that must be met in order to assume a causal relationship – in terms of product liability – between a defect and damage.[645] These comprise of both a factual causal relationship and a legal relationship, (hereinafter referred to as *factual causation* respectively *legal causation*).[646] Factual causation sees to the physical connection between an event and the occurrence of damage. This is assessed using the (negatively formulated) *condicio sine qua non* (CSQN) test: would the damage also have occurred without the defective product, a causal relationship cannot be assumed.[647]

---

[639] This is addressed in articles 6:107(1)(b)-(5) and article 6:108(3)-(6) BW. The "next-of-kin" who may exercise rights against tortfeasors are stipulated in article 6:107(1)(b) and 6:107(2): husband/spouse or (registered) partner; parents; children; caretakers; care-receivers; or other persons who can be deemed close relatives on grounds of fairness and equity, of the injured or the deceased (article 6:108(4)BW) person.
[640] Article 6:107(3) BW.
[641] Article 6:107(1)(b) and 6:108(3) BW.
[642] Lindenbergh 2018, p. 6.
[643] See Giesen, De Jong & Muslat 2017, p.30; Hartkamp & Sieburgh 2019, no. 267; and Keirse 2016, p. 371.
[644] See Keirse 2016, p. 330.
[645] Article 6:188 BW uses virtually the same wordings as article 4 PLD, and article 1(1) PLD is literarily implemented in the first sentence of article 6:185(1) BW.
[646] See Giesen & Rijnhout 2017, p. 84-85; Giesen 2012, p.18-21; Keirse 2016, p. 332 and Sieburgh 2017, no. 50, and Boonekamp 2018, no. 1.2.2.
[647] The CSQN-test resembles the *but-for* test that is used in for example Anglo Saxon regimes, which can be put as follows: "would the loss have been sustained but for the relevant act or omission of the defendant?" (Deakin, Johnston & Markesinis 2013, p. 218).

Subsequent to factual causation, legal causation has to be established.[648] This is regulated in article 6:98 BW. That article reads as follows: "*Only damage that is* connected *in such a way to the event that made the debtor liable, that it, in regard of the nature of his liability and of the damage caused, can be attributed to him as a* consequence *of this event, is eligible for compensation*".[649] This provision implies *inter alia* that – despite the factual causal relationship – the liability of the debtor can be annulled, or reduced when it would not be reasonable to attribute certain damage to the debtor.[650] Factors that can be assessed include *inter alia*[651] the nature of the liability,[652] the nature of the damage,[653] foreseeability of the damage,[654] and the directness (or remoteness) of the connection between the cause and the damage.[655]

4.2.2.4.1 Alternative causality

The Dutch Supreme Court furthermore developed the *alternative causality* rule in its famous *DES daughters* decision.[656] The DES-drug was prescribed to pregnant women between 1946 and 1977 to prevent miscarriage. DES was a non-patented drug, produced by many pharmaceutical companies. Although the drug did indeed prevent early birth, daughters of the women who took DES also had a severe chance of developing clear-cell carcinoma as a side-effect. The daughters who developed this type of cancer, claimed damages that resulted from the unsafe drugs from the producers. However, based on the CSQN-doctrine, it was hardly possible to construe factual causation: the damage could be the consequence of the pills of a multitude of manufacturers, and it seemed impossible to exactly pinpoint the specific manufacturers that provided the drug to specific mothers. As a result, DES-daughters could not be compensated for their losses. The

---

[648] See on the "staging" of factual and legal causation also Rijnhout & Giesen 2017, p. 84.
[649] See for the source if this non-official translation of article 6:98 BW: http://www.dutchcivillaw.com/legislation/dcctitle6611bb.htm (last accessed 26 April 2019)
[650] See the analysis of the "four Brunner-rules" and other relevant factors Sieburgh 2017, no. 63-69. See also 6:100 and 6:101 BW: once factual and legal causation has been established, the obligation to remunerate damages can be reduced inter alia to the extent that "the damage is caused as well by circumstances which are attributable to the injured person himself" (article 6:101 BW), and to the extent that the victim also profited from the event – insofar as that would be equitable (6:100 BW).
[651] See for a more elaborate overview: Giesen 2012, p. 19-20.
[652] Damage resulting from culpable behaviour of a tortfeasor himself will sooner judged to be "attributable" in sense of art. 6:98 BW, than damage that is the result of a 'qualitative liability' for example for damage-inflicting actions of an employee or an animal. Also relevant is the degree of the blame in this respect (see Giesen 2012, p. 19.
See further Sieburgh 2017, no. 63, 65.
[653] A claim for remuneration of personal damages would be granted easier than a claim for purely financial loss. See further Sieburgh 2017, no. 63.
[654] Attribution of damage that would be more likely to occur – which is to be assessed on the basis of rules of 'experience', would be granted easier than less-likely forms of damage. See Sieburgh 2017, no. 64
[655] Where a certain occurrence of damage is further removed from the cause, it is less likely that this would be considered as "attributable" then when it would concern damage that is a more direct result of the respective cause. See further Sieburgh 2017, no. 69.
[656] HR 9 October 1992, ECLI:NL:HR:1992:ZC0706, *NJ* 1994/286, annotated by C.J.H. Brunner, and explicated in English in Giesen & Rijnhout 2017, p. 93-94. See further their references in footnote 36. See also Giesen, De Jong & Muslat 2017, p. 41-42.

Supreme Court held that the *alternative causality* rule should be applied here.[657] This rule, which is now encoded in article 6:99 BW, holds that when damage can be caused by two or more possible events for each of which another person is liable, and when it is certain that the respective damage is caused by at least one of those events, each of the contributors is jointly and severally obliged to remunerate the damage, unless he proves that the damage is not caused by the respective event for which he is liable. Article 6:99 thus holds a reversal of the burden of proof regarding the factual causation (thus regarding the *condicio sine qua non* relationship between unlawful action and damage of the specific victim). When it is certain that one of several events has led to damage, but it is not certain which of those events is the actual cause of the damage, *and* when it is known who bears liability for the respective events, it is the defendant who must prove that he was not to blame rather than the plaintiff who would, in other circumstances, have to prove that the defendant can be held responsible for the damage causing event.[658] It must be noted that it is necessary that the whole amount of damage could have been caused by the respective events individually, for the *alternative causality* rule to be applicable. It is not sufficient that for example "event A" may have contributed to 25% of the total damage, and "event B" to 75%; both "event A" and "event B" must individually have resulted in a 100% chance to amount to 100% of the suffered damage.[659] It may however not be necessary that the damage-causing events are of the same type, or nature.[660]

> Alternative causality could play a role in (product) liability questions as a result of AV-accidents. When for example an AV-crash resulted in personal damage to one of the passengers, and that damage could be both the result of a defective sensor, produced by Manufacturer X, and a defective radar, produced by Manufacturer Y, and it cannot be determined which of the two

[657] Idem, no. 3.4.
[658] See also Sieburgh 2017, no. 91. See also Giesen & Rijnhout 2017, p. 94, who explain that the rationale for the reversal of the burden of proof is that it would be unfair to leave those who suffered damage without remuneration when it can be proven that there are several entities who acted wrongfully (and who are therefore liable), when it cannot be established which of them was the *actual* tortfeasor to whom the damage can be attributed.
[659] See Hartkamp & Sieburgh 2019, no. 95.
[660] See Hartkamp & Sieburgh 2019, no. 91 and 94. Klaassen & Kortmann 2012 also refer to the applicability of the *alternative causality* rule in case more than one unlawful action could have caused the damage ("[…] schade het gevolg kan zijn van meerdere aansprakelijkheidsvestigende omstandigheden"), p. 21. See also R.J.B. Boonekamp, "Alternatieve veroorzaking", *BW-krant Jaarboek* 1991, (p. 79-94), p. 94, who observes that similarity of events would not be necessary: "Gelijksoortigheid van gebeurtenissen is m.i. niet vereist. […] De gebeurtenissen mogen van geheel ongelijksoortige aard zijn, mits die geschikt zijn om de schade zoals die in concreto is toegebracht te veroorzaken en als mogelijke oorzaak van de schade in aanmerking komen". See furthermore Boonekamp 2018, no. 3: "Voor de toepasselijkheid van art. 6:99 is niet vereist dat de verschillende personen die aansprakelijk zijn voor de verschillende gebeurtenissen waarvan de schade het gevolg kan zijn, op dezelfde grond (bijvoorbeeld art. 6:162) aansprakelijk zijn. Allerlei combinaties zijn mogelijk. Het kan zijn dat de een uit wanprestatie aansprakelijk is en de ander uit onrechtmatige daad. Mogelijk is ook dat de een aansprakelijk is op grond van art. 6:162 en de ander op grond van een van de risico-aansprakelijkheden in afd. 6.3.2 of 3, enz., enz.".

is the actual cause, either one of those manufacturers can be sought for remuneration under 6:99 BW.

Another example of possible alternative causality in the context of AVs may be the following. Imagine that the algorithm deciding on when its safe (or not) for the AV to change lanes is developed by several programmers (employed by different companies) together, and that the respective algorithm gets defective at some point. The error in the code is not noticed by anyone of the co-working programmers. The result is the 'updated' AVs risk executing lane changes without taking due notice of other road users, with multiple crashes as the inevitable consequence. When it can be construed that all contributing programmers either wrongfully adapted the source codes of the algorithm, or failed to notice the error, and the precise 'event' causing the defect cannot be pinpointed, all programmers may be sought for damages individually in my opinion, as all of these events (either making the error, or failing to spot it in the code) could have caused 100% of the respective damage.

4.2.2.4.2 Proportional causality

The CSQN-test entails an "all or nothing" approach: based on this test there either *is* a causal relationship, or not.[661] Sometimes, this leads to unfortunate outcomes, and, to remedy such situations, under special circumstances, *proportional liability* is used in case law of the Dutch Supreme Court (Hoge Raad, HR).

> *This was for instance the case when an employee (Karamus) contracted lung cancer after having been in contact with asbestos during his employment at Nefalit. Since Karamus also had a tobacco smoking habit, a c.s.q.n. relationship between the asbestos-exposure during his employment at Nefalit, and the contraction of Karamus' lung cancer could not be established. As a result, Karamus would not be able to hold his former employer liable. The Hoge Raad observed this to be unreasonable, and held that proportional liability could in such cases be in order.[662] An expert estimated that in this case the likelihood that Karamus' disease was the result of the asbestos exposure, could be calculated at 55%, while the other 45% could be held to be due to Karamus' smoking habit, and other (genetic) factors attributable to him. The Hoge Raad allowed the employer to be held liable for the whole amount of the damage – based on a well-reasoned (expert) estimate –reduced with the estimated percentage (55%) of the cause that can be attributed to other causes of the damage – in this case tobacco smoking.[663]*

Proportional liability was subsequently upheld by the Hoge Raad in other cases with different case positions,[664] but the Hoge Raad also noted that *proportional liability* is not to be applied

[661] See Keirse 2016, p. 332-333, see also Giesen & Rijnhout 2017, p. 89, and Leemhuis, B., "Bewijs bij het conditio sine qua non-verband", *Advocatenblad* 2017, no. 4, p. 67.
[662] HR 13 March 2006, ECLI:NL:HR:2006:AU6092 (*Nefalit/Karamus*). See also the analysis on the *Nefalit/Karamus* decision in light of the Dutch implementation of the PLD: Keirse 2016, p. 333-334.
[663] HR *Nefalit/Karamus* para 3.5.
[664] As also referred to in Keirse 2016, p. 334, fn. 78: HR 24 December 2010, ECLI:NL:HR:2010:BO1799 (*Fortis/Bourgogne*); HR 14 December 2012, ECLI:NL:HR:2012:BC8349 (*Nationale Nederlanden/Moeder en Zoon*); HR 21 December 2012, ECLI:NL:HR:BX7491 (*Deloitte/H&H Beheer BV*).

throughout liability law in general, and it should be applied reservedly.[665] In its Fortis/Bourgonje decision, the Hoge Raad stated that the *proportional* liability rule may only be administered when a) the liability of the defendant has been established; b) there is a "not very small chance" that a *CSQN*-relationship exists between the norm that was violated by the defendant and the damage; and c) application of the rule is justified by i) the rationale of the violated norm; and ii) the nature of the violation.[666] Since the Fortis/Bourgonje decision, it has not become absolutely clear which "norms" (rationales) and " violations" (natures) justify proportional liability. As it appeared, the violation of a generic duty for asset managers to warn their clients in order to prevent financial loss would not vindicate a proportional liability claim,[667] although the violation of a specific traffic norm that is installed to prevent that people sustain personal injury, would.[668] The proportional liability rule has until now not been applied in product liability cases, but it can be seen as a well-established exception to the all-or-nothing approach that used to be the traditional outcome of the c.s.q.n. assessment.[669]

> A half year old AV crashes in the middle of the night into a tree. The passenger, the owner of the vehicle, suffered serious injuries. After a thorough expert analysis of the event data recorder that has been built in the car, there seem to be two probable causes of the accident. As it occurred, the night-vision sensor did not function correctly for 100% of the operation time; due to a loose connector (it had not been soldered properly, converse to specifically applicable norms) there were hitches in the functioning of the sensor, although it is not clear whether or not a hitch occurred in the seconds before the accident. Furthermore, the owner performed a chip-tuning update to the car, in order to make it faster: certain speed-limiters and braking indicators had been disabled in the AV's steering software. The expert estimates that there is a chance of 60% that the crash was caused by the defective sensor, and a 40% chance that the AV crashed due to the chip-tuning operation. Although there is no clarity on the c.s.q.n. relationship, it may be unreasonable not to award any damages to the victim. In this case it can be argued that the judges may apply the *proportional liability* rules, and decide that 60% of the damages have to be remunerated by the AV producer.

Another troublesome consequence of the all-or-nothing approach emerges when a certain violation of a norm (or rule/standard) can be established, but the (height of the) damage is unclear. This happens when for example a lawyer forgets to file an appeal to a court decision in due time, resulting in the deprivation of a chance of success in appeal for his client,[670] or when a doctor fails to spot a certain condition in a patient, resulting in serious disabilities for that patient,

---

[665] See HR 24 December 2012, ECLI:NL:HR:2010:BO1799 (*Fortis/Bourgonje*), para. 3.8 and Giesen & Rijnhout 2017, p. 90.
[666] HR Fortis Bourgonje (see footnote 665), para 3.8; Giesen & Rijnhout 2017, p. 90.
[667] HR Fortis Bourgonje, para 3.10.
[668] HR 14 December 2012, ECLI:NL:HR:2012:BX8349, *(Nationale Nederlanden/S&L)*, para. 4.3; Giesen & Rijnhout 2018, p. 91.
[669] Keirse 2016, p. 334.
[670] Which was the case in HR 24 October 1997, *NJ* 1998, 257 (*Baijings*), as analysed in Keirse 2016, p. 335.

where there was a significant chance of better outcomes for that patient, should the said condition have been noticed earlier.[671] In such cases, judges in the Netherlands may award damages based on the probability of a 'better outcome', should the respective chance not have been lost due to the violation of the norm.[672] As such "loss of a chance"-cases do not seem to be of major importance in terms of AV (product) liability, as application of this doctrine is – to date – limited to faults made by professionals such as medical specialists and lawyers, these cases will not be elaborated further here.[673]

4.2.3.5 Issues of proof

With the – limited – harmonization of the CJEU on matters of proof in mind, as elaborated in section 4.2.2.6, it must be noted that there are several ways in which courts in The Netherlands may assist victims in the requisite delivery of proof regarding defects, damage and causal relationship between defects and damage.[674] Whereas the burden of proof as regulated in art. 4 PLD (and 6:188 BW) may not be reversed regarding these topics,[675] other aids, such as presumptions, may be allowed under CJEU case law. As a general rule, which was developed in the case law of the Hoge Raad, a causal relationship will be presumed whenever a safety norm is violated that sees to the prevention of a specific danger, when that specific danger materializes.[676] This rule is applicable in product liability cases in sense of the Dutch implementation of the PLD, as the notion of *defectiveness* implicates the violation of a norm regarding the level of *safety which a person is entitled to expect*.[677] Once causation has been presumed, it is however still possible for the defendant to refute ("ontzenuwen") the causal relationship – which does not hold the obligation to prove the contrary ("tegendeelbewijs"), a mere invalidation of the causal relationship ("tegenbewijs") will suffice. Thus, the burden of proof remains with the victim, who is however aided by the respective presumption of causation.[678]

---

[671] Rechtbank (District Court) Amsterdam 15 December 1993 and subsequently Hof (Court of Appeals) Amsterdam 4 January 1996 ECLI:NL:GHAMS:AB8628 (not published on rechtspraak.nl), *NJ* 1997, 213 (*Wever/De Kraker*), as analysed in Keirse 2016, p. 335.
[672] See Sieburgh 2017, no. 79-80b; Keirse 2016, p. 335.
[673] Furthermore, in academic literature the (dogmatic) difference between the so called "loss of a chance doctrine" and proportional liability is questioned. See for example B.C.J.. van Velthoven, "Verlies van een kans en proportionele aansprakelijkheid: verschillende figuren voor verschillende gevallen?(II)", *Nederlands Tijdschrift voor Burgerlijk Recht* 2018/15, no.35(4), p. 102-112.
[674] Article 6:188 implements article 4 PLD.
[675] CJEU 21 Juni 2017, C-621/15, ECLI:EU:C:2017:484 (*W/Sanofi Pasteur*), para. 27, 29; one may argue that national provisions on reversal of the burden of proof regarding other topics, would still be allowed, including those where there are multiple possible causes of the same damage, as regulated in art. 6:99 BW. See inter alia Giesen 2001, p. 196-198; Hartkamp & Sieburgh 2019, no. 269.
[676] See HR 10 January 2020, ECLI:NL:HR:2020:27 (*Soldeermachine*). See also HR 17 November 2000, ECLI:NL:HR:2000:AA8368 (*Unilever/Dikmans*); and Giesen 2001, p. 199.
[677] Giesen 2001, p. 198-199. Giesen does however comment that such assumptions may not be as easily made regarding instruction defects (p. 199-200).
[678] See Hartkamp & Sieburgh 2019, no. 269; Keirse 2016, p. 343; Giesen 2001, p. 64-66.

It is also assumed in some cases that proof of damage, negligence and/or causation more or less logically follow from the facts of the case (*res ipsa loquitur*). The Hoge Raad for example presumed that a bottle of cola that caused injuries to the victim who tried to open it in a normal manner could be deemed defective – notwithstanding the existence of special circumstances rendering the presumption invalid, and/or refutation of the presumption by the producer.[679] Another, more recent, example of *res ipsa loquitur* is the *Ladder*-case.[680] A ladder, which consisted of several foldable parts, suddenly folded when in use, which caused serious injuries to the victim who stood at that ladder when it happened. The District Court presumed that a ladder that suddenly folds when used in a normal manner can be deemed defective, in conformity with the *res ipsa loquitur*-rule, notwithstanding the possible refutation of that presumption by the producer.[681] In appeal, the producer was however successful in his attempt to rebut the presumption of the District Court; an expert was appointed, who has to advise on the respective matters.[682]

It is observed in the literature that standards of proof must not be set too high, as this would detriment the protection of consumers contrary to the rationales of the PLD.[683] This would be especially relevant in high-tech cases. Keirse observes that "[i]n some situations, it might be very difficult for the injured person to prove his claim, due to the technical complexity of certain products, the high costs of expert evidence, or because of limited access to certain information (for instance laboratory data).[684] She furthermore observes that in such cases, victims may indeed be helped by the judge who applies *res ipsa loquitur* rules, or the (incidental) reversal of the burden of proof.[685] Regarding the latter (reversal of the burden of proof), it can however be questioned whether or not that would still be opportune after the *W/Sanofi Pasteur* decision of the CJEU.

> Presumptions such as following from the *res ipsa loquitur* rule may likely be applied to AV product liability matters. As it will be very troublesome and expensive for victims to either access, analyse, or have analysed the vehicle data, it would – considering the rationales of consumer protection of the PLD – be an aid to victims to presume that an AV is defective, or that there is a causal relationship between defect and damage when it for example crashes during normal use, while still allowing the producer(s) to invalidate that presumption. It must be noted here on the side, that based on established case law of the Hoge Raad, it is up to the

[679] HR 24 December 1993, ECLI:NL:HR:1993:ZC1197 (*Leebeek/Vrumona*), para 3.6, as discussed in Giesen 2001, p. 72-73; Keirse 2016, p. 343, and Hartkamp & Sieburgh 2019, no. 258.
[680] Rechtbank (District Court) Oost-Brabant 20 March 2013 and 24 December 2014, ECLI:NL:RBOBR:2014:8103, and subsequently Hof (Court of Appeals) 's-Hertogenbosch 10 January 2017, ECLI:NL:GHSHE:2017:31 (*Ladder*).
[681] Rechtbank Oost Brabant *Ladder* (ibidem), para. 3.1
[682] Hof 's-Hertogenbosch *Ladder* (ibidem), para. 6.4.8.
[683] Giesen 2001, p. 197 and his references in footnote 26; Keirse 2016, p. 343-344.
[684] Keirse 2016, p. 344.
[685] See also Giesen 2009, p. 51-53 considering aim and functions of (reversal) of the burden of proof, and p. 56-58 on presumptions.

party who has information at its disposal that is critical for the proof of defectiveness or a causal relationship, to present such information, even if it detriments his own position.[686]

4.2.4 IMPLEMENTATION IN FRANCE

4.2.4.1 Introduction

The Product Liability Directive was implemented in the French Code Civil (hereinafter: CC) in 1998. Currently,[687] product liability is addressed in article 1245-1/17 CC.[688] It took the French legislator almost 13 years to implement the PLD provisions. The development risks defence (also known as "state-of-the-art defence"[689]) formed one of the main bottlenecks in the implementation process.[690] During the period between 1985 and 1998, the highest court in France, the *Cour de cassation,* developed rules that were strongly inspired by, and based on the PLD provisions, and served as a means for victims to be able to claim damages resulting from defective products from producers.[691] This regime operated alongside generic CC-rules holding possibilities for victims to claim damages based on breach of contract, such as the statutory "*garantie des vices caches*" (warranty against latent defects),[692] the *"responsibilité du fait des choses*" (liability for acts of persons for whom he is responsible, or things in his custody),[693] and a fault-based liability claim.[694] Eventually, the judge-made "half-way-house" was abandoned in 2007,[695] and the implemented PLD-provisions remain as the designated rules to base a product-liability claim upon, although the general fault-based rules and contract-law principles still remain in force.[696] It is observed that

[686] See e.g. Hoge Raad 20 November 1987, *NJ* 1988/500 (*Timmer/Deutman*), as discussed in Thoe Schwartzenberg 2013, p. 112. See furthermore Giesen 2009, p. 58-59.
[687] In 2016 a "reform" of the Civil Code was effectuated by means of Ordonnance n° 2016-131 of 10 February 2016. Beforehand, the implemented PLD-provisions were to be found in article 1386-1/18 CC.
[688] For these sections, I have used the English translation of the provisions in the CC which is made by J. Cartwright, J., Fauvarque-Cosson, B., and Whittaker, S., commissioned by the *Direction des affaires civiles et du sceau, Ministère de la Justice, République française*. It is available online, via http://www.textes.justice.gouv.fr/art_pix/THE-LAW-OF-CONTRACT-2-5-16.pdf (last accessed 11 march 2020).
[689] See 4.2.2.8.6.
[690] See Fairgrieve 2005, p. 93-94 (more specifically: footnote 30); and Borghetti 2015, p. 209.
[691] See Borhetti 2015, p. 210-211. See furthermore Rochère, J. De La., and Milhac, O., "Chapter 7 – France", in: Campbell, D., and Campbell C., (eds.), *International Product Liability*, London: Lloyd's of London Press Ltd 1993, pp. 231-274, p. 231-232; and Fairgrieve 2005, p. 84-85.
[692] Article 1641 CC, see also Sportes & Ravit 2019, sec. 1.1, Borghetti 2016, p. 206, 210-211.
[693] Article 1242 CC; see also Fairgrieve 2005, p. 90-91, who remarks that this *responsibilité du faits des choses* does not exclude product liability, as the French courts have drawn a distinction between "*garde du comportement* and *garde de la structure"* (p. 91). A producer is seen as a *garde de la structure*, even after a respective product is out of his control, and in the ownership of someone else. Therefore, he remains responsible under the implemented product liability rules. In product liability cases, the *responsibilité du faits des choses* is said to be of limited importance (ibidem, p. 91, and the references to case law in footnote 91).
[694] Which could be based on the general rule of art. 1240 CC.
[695] See Borghetti 2016, p. 213.
[696] Article 1245-17 CC.

the CC-provisions exactly follow the scope of the PLD,[697] however there have been – and remain, some deviations of the PLD, which will be elaborated in the following sections.[698]

First, it must be noted that the development risk defence has eventually been implemented. However, it does not apply to "an element of the human body or products derived from it".[699] Furthermore, the possibility for national legislators to install a ceiling for the amount of damages to be awarded resulting from a successful product liability claim was not used in France.

4.2.4.2 Defectiveness and unlawfulness

Defectiveness is addressed in article 1245-3 CC and corresponds with article 6 PLD. Borghetti observes that the definition of defectiveness is rather vague, but – despite the absence of case law on this matter – that an assessment of the objective "legitimate expectations" of the general public must be taken as a point of departure.[700] Furthermore, he argues that a product is not safe "when it is abnormally dangerous", however without describing what 'abnormal dangerousness' might consist of.[701] Another approach for determining defectiveness has been advocated in literature and before court in relation to pharmaceutical products. Rather than the *legitimate expectations test*, it has been argued that a *risk/benefit* test should be carried out in order to assess whether or not the benefits of for instance a certain medicine outweigh its (potential) risks.[702] The *Cour de cassation* held however that "a vaccine's defectiveness could not be ruled out on the sole ground that the risk/benefit balance of the vaccine was positive".[703] From this case law thus follows, that the *legitimate expectations test* is to be used as means for assessment of defectiveness. Furthermore, there is no explicit distinction made in France between design, manufacturing and presentation defects.[704]

Where some authors (from other jurisdictions than France), as well as the European Commission, seem to endorse the view that also software can under certain circumstances be qualified as a

[697] See Borghetti 2016, p. 212.
[698] In its implementation, the French legislator at first aimed to protect consumers more than the PLD provided for. On several occasions, the Court of Justice of the European Union penalised this protective approach. See for example ECJ 25 April 2002, C-52/00 (*Commission/France*); ECJ 9 February 2006, C-127/04 (*O'Byrne/Sanofi Pasteur*); ECJ 24 March 2006, C-177/04 (*Commission/France*).
[699] Article 1245-10(5) CC.
[700] Borghetti 2016, p. 216.
[701] Ibidem.
[702] This approach was followed in *inter alia* the following decisions of appellate courts (as referred to in Borghetti 2016, p. 216): CA Versailles 17 March 2006, no. 04/08435 and of the same court: 16 March 2007, no. 05/09525; 29 March 2007, no. 06/00496; 5 November 2007, no. 06/06435 and CA Paris, 19 Jun2 2009, no. 06/13741.
[703] Quotation taken from Borghetti 2016, p. 216, referring to Cass. 1re civ. 26 September 2012 (fn 48) and Cass. 1re civ., 10 July 2013 (fn. 48).
[704] See De La Rochère & Milhac 2007, p. 253-254.

product (which can thus be defective),[705] Borghetti clearly does not: mentioning the absence of case law on this matter, he observes that

> "the dominant scholarly view is that programmes [i.e. computer programs/software, *RWdB*] or information as such should not be regarded as a product in sense of the CC provisions; however, there is no doubt that the digital content of a product, such as a programme, can make a product defective, for example if it causes a product to malfunction".[706]

Other authors hold different opinions. Prebost & Walter for example observe that "[i]t is not impossible that jurisprudence will extend the scope of the law to include intangibles".[707]

> Thus, Borghetti, Oudot and Le Tourneau seem to implicate that the producer of a defective piece of software (for example AV steering software that is not embedded in a piece of hardware (for example: streamed software), cannot be held liable under the French implementation of the PLD, while the AV manufacturer can be held responsible and liable in France,[708] while authors as Prebos & Walter foresee that it may follow from future case law that software (sec) will be included in the realm of "products" under the French product liability provisions.

Also in France, it is deemed unlawful to put defective products into circulation.[709] As the PLD did not provide what "putting products into circulation" exactly entails, the French legislator interpreted that this is the case "when a producer voluntarily relinquishes it", which can be done only once. The ECJ provided however in 2006, that this requirement must be interpreted as holding that a product is put into circulation when "it is taken out of the manufacturing process and enters a marketing process in the form of which it is offered to the public in order to be used

[705] See section 4.2.2.2.
[706] Borghetti 2016, p. 217.
[707] F. Prebost & A. Walter, "Introduction to Software Protection under French Law", in: Y. Van den Brande, S. Coughlan & T. Jaeger, *The International Free and Open Source Software Law Book*, Open Source Press 2014, online, via: http://ifosslawbook.org/france/ (last accessed 16 January 2020). They refer to P. Oudot, *Le risque de développement: Contribution au maintien du droit à reparation*, Dijon: ELD 2005, and Ph. Le Tourneau, *Droit de la responsabilité et des contrats - Régimes d'indemnisation*, Paris: Dalloz Action 2009-2010, who hold, with Borghetti, the opinion that software does not fall under the scope of the French PLD provisions.
[708] It must be noted however that it was indicated that software can be seen as a product under French product liability law in European Commission 2018b, p. 67, Question N° 15677, de M. de Chazeaux Olivier, Question publiée au JO le 15/06/1998 page 3230, Réponse publiée au JO le 24/08/1998 page 4728,. See: http://questions.assemblee-nationale.fr/q11/11-15677QE.htm (last accessed 26 November 2019).
[709] Article 1245-4 CC.

or consumed".[710] It must thus be concluded that the French explanation of "putting into circulation" is not in conformity with the ECJ-decision.

The CC originally contained a provision holding that a producer could not successfully invoke the development risk defence and the "compliance with mandatory rules"-defence when he had "failed to take appropriate measures to avert harmful consequences"[711] of a certain defect. This implicated *inter alia* a duty for producers to warn for certain (newly discovered) dangers or defects in products. However, this provision was annulled by the French legislator in conformity with a decision of the ECJ in which it was observed that this deviation of the PLD was not allowed.[712] Duties to warn may however follow from general (fault-)liability rules.[713]

In the first edition of the implemented PLD-provisions, the CC stated that rather than the 'producers' mentioned in the PLD, any 'professional supplier' of a defective product could be held liable. The ECJ considered this French conception of the entities to be held liable too broad.[714] The ECJ-decision eventually led to the current article 1245-6 CC, which is actually *narrower* than article 3 PLD.[715] Article 3 PLD stipulates that where the producer cannot be identified, each supplier shall be treated as producer, unless that supplier identifies the actual producer within a reasonable time. Article 1245-6 CC holds a comparable obligation, however, its scope is limited to any suppliers "in the course of business or a profession", including sellers and hirers, although *excluding* finance lessors and a hirer comparable to a finance lessor. Furthermore, the "reasonable timeframe" allowed by the PLD to inform the victim of the true identity of the producer, is limited to three months in France, which provision also deviates from the PLD.

4.2.4.3 Damage

Article 1245-1 CC states that the product-liability regime applies to "the reparation of harm which results from personal injury", and also "to the reparation of harm above [€ 500,-],[716] which results from damage to property, other than the defective property itself". Different from article 9 PLD, the CC-provision is not restricted to property "of a type ordinarily intended for private use or consumption", and that "was used by the injured person mainly for his own private use or

[710] See ECJ 9 February 2006, C-127/04, ECLI:EU:C:2006:93 (*O'Byrne/Sanofi Pasteur*), para. 32, as elaborated in 4.2.2.8.2 above. See also Borghetti 2016, p. 217-218.
[711] Borghetti 2016, p. 218.
[712] ECJ 25 April 2002, C-52/00 (*Commission/France*), fn. 26 as referred to by Borghetti 2016, p. 217. See furthermore Rouhette, Gallage-Alwis & Houssel 2018, who indicate that duties to warn may follow from Article 521-17 and 423-2 Consumer Code.
[713] Ibidem Rouhette, Gallage-Alwis & Houssel 2018, Borghetti 2016, p. 217 (referring to the old article 1382 CC, now 1240 CC) and Sportes & Ravit 2019, under no. 2.4; and De La Rochère & Milhac 2007, p. 254-256.
[714] ECJ 25 April 2002, C-52/00 (*Commission/France*); see also Fairgrieve 2005, p. 95.
[715] See Borghetti 2016, p. 219-220.
[716] In France, this is not treated as a franchise, but rather as a threshold, as Borghetti 2016 observes on p. 223-224.

consumption". Borghetti observes that this deviation from the PLD is allowed, as its article 9 "shall be without prejudice to national provisions relating to non-material damage", and that it follows from the ECJ-decision in *Leroy Somer* that "types of damage not covered by the Directive lie outside its scope of application, and that national laws are thus free to organise their compensation as they wish".[717] It is however questionable whether this observation is correct, as article 9 PLD is rather specific on its scope of application, and article 1245-1 clearly deviates therefrom.[718]

In France, there are in principle no restrictions in types of damages, as long as these were not "suffered in an illegitimate interest" (*intérêt illégitime*).[719] This implicates that for example "damage to business property, consequential economic loss, pure economic loss, loss of a chance, and non-economic loss",[720] are remunerable under the product liability provisions of the CC. How far these remuneration obligations reach, can be illustrated by a decision of the *Cour de cassation*, which held the producer of a pacemaker liable to remunerate non-pecuniary damages to the person in whose body it was implanted "resulting from the exposure to the risk that the pacemaker should fail".[721] Also "*prejudie d'anxieté*" (anxiety) may have to be compensated under French law, when one has been exposed to hazardous products, "irrespective of whether or not the claimant actually suffers from a disease or injury".[722] However, it is necessary that the victim fears that a disease might at some point strike,[723] that it concerns severe damage, and that the fear must have caused "sufficiently severe psychological trouble".[724]

Not only the victims themselves, but also "victimes par riochet" (rebound victims,[725] or indirect victims) can claim damages under the French system "if they suffer pecuniary or non-pecuniary

---

[717] Borghetti 2016, p. 222-223, referring to ECJ 24 Juni2 2009, C-285/08, *Moteurs Leroy Somer/Dalkia France and ACE Europe*. In a similar vein, Borghetti argues that the broad French conception of heads and types of damages to be compensated through regular contractual and extra-contractual liability claims, should also apply to product liability claims. See also Sportes & Ravit 2019, no. 6.2; and Rouhette, Gallage-Alwis & Houssel 2018, no. 19.
[717] Van Dam 2013, p. 354. See furthermore Borghetti 2016, p. 222-223 and Sportes & Ravit 2019, no. 6.2.
[718] See Fairgrieve 2005, p. 95.
[719] Van Dam 2013, p. 353-355. See furthermore Borghetti 2016, p. 222-223 and Sportes & Ravit 2019, no. 6.2. As Van Dam explains (on p. 354-355), the notion of "illegality" is developed in case law: "Until the 1970s an unmaried partner did not have the right to compensation for the loss of maintenance because of the death of her companion. Her infringed interest was considered to be illegitimate (*intérêt illégitime*) but this has since changed"; see furthermore his references to case law in footnote 43. He also explains that a public transport passenger, who did not pay his fare, and who suffered damage in an accident, *did* have a legitimate interest, i.e. the protection of his bodily integrity, despite is "illegal travel".
[720] Borghetti 2016, p. 223; also: De La Rochère & Milhac 2007, p. 263-264.
[721] Ibidem, referring to Cass. 1re civ. 19 December 2006, *D*. 2007, 2897, obs. Ph Brun, *JCP* G 2007, II, 10052, note S Hocquet-Berg, *RTD civ.* 2007, 352, obs. P Jourdain.
[722] Rouhette, Gallage-Alwis & Houssel 2018, no. 19, referring to Cass. 1re, 19 December 2006, no. 06-1113, and Cass. 1re, 2 July 2014, no. 10-19206. See also Overheul 2018, p. 119 (fn. 6 and 8).
[723] Overheul 2018, p. 120.
[724] Overheul 2018, p. 120, footonetes 25 – 27.
[725] Van Dam 2013, p. 353; Borghetti 2016, p. 222.

damage as a result of a relative being physically injured due to a product's defect".[726] However, this principle does not apply to all third parties. As Van Dam indicates, it is required that the damage that has been suffered is "personal"; "a grandmother who became custodian of her grandchild after his parents died in an accident was not considered to be a *victime par riochet*",[727] as her grandchild may have opted for remuneration, and in that way compensate the damage suffered by the grandmother.

> When a defective AV crashes into another AV, which was rented out by a professional car-rent company, the producer must thus compensate the professional owner of that second vehicle, under the French product liability system. Should, as a result of the crash someone die or be seriously injured, third parties with a close connection to the victim may also have to be remunerated for their grief and sorrow.[728] It is questionable whether or not people who also own a (potentially) defective AV of the same kind as the one that crashed, may successfully opt for compensation of their "prejudice d'anxiété" (anxiety) for having been exposed to a hazardous AV, as they might not have to fear that they will eventually suffer injury, *unless* the respective defect is not fixed and they remain exposed to the respective risks of severe damage – and their fear causes sufficiently severe psychological trouble to the victims..

4.2.4.4 Causation

In conformity with the PLD, article 1245-8 CC provides that the victim must prove causality (and defectiveness of the product as well as the damage suffered). As mentioned above in section 4.2.2.6, causation is not harmonised by the PLD. In France, there are not many rules on how a causal relationship between a defect and damage should be established, as long as the causal link is "certain et direct" (certain and direct).[729] Sportes & Ravit observe that there is a large margin of appreciation for (lower) courts to determine whether or not causation can be proved.[730] However, they indicate two "main theories" – which may be deviated from.[731] The first is the "theory of equivalent conditions", which they explain as follows: "any event without which the damage would not have occurred shall be considered as the cause of the damage".[732] This resembles the but-for test used in England & Wales,[733] and the condicio sine qua non test used in The Netherlands.[734] The second is the "theory of adequate causality", meaning that "only the events

[726] Borghetti 2016, p. 222. See also Van Dam 2013, p. 345, who refers to Civ. 22 October 1946, *JCP* 1946, II, 3365, regarding the compensation of non-pecuniary loss for personal injury.
[727] Van Dam 2013, p. 354.
[728] See Van Dam 2013, p. 353.
[729] See van Dam 2013, p. 319; Borghetti 2016, p. 224; and Sportes & Ravit 2019, no. 2.
[730] See also Taylor, Fairgrieve & Wester-Ouisse 2018, p. 319.
[731] Sportes & Ravit 2019, no. 2.2.
[732] Ibidem.
[733] See section 4.2.4.4.
[734] See section 4.2.3.4.

that constitute the determining cause of the damage shall be considered the cause of the damage".[735]

Several authors point furthermore to causation questions that arise in healthcare issues.[736] The *Cour de cassation* for instance considered that a causal link could be established by 'strong, decisive and concurring evidence' between the administration of a hepatitis B vaccine, and the development of demyelinating diseases as Multiple Sclerosis, "despite the state of scientific uncertainty concerning the aetiology of demyelinating diseases and the absence of epidemiologic evidence".[737] In such cases, where scientific evidence cannot underpin the claim that causality exists, French courts may *presume* causality on the facts of the case, on the basis of article 1382 CC.[738]

> In AV-accident cases, it will often be hard for victims to prove (whether or not with scientific certainty) an actual causal relationship between a (also complicated to prove) defect, and suffered damage. Presumptions on the fact of the case, in similar vein as the *Cour the cassation* allowed in the decision referred to above, may indeed aid the victims in delivering proof, without a reversal of the burden of proof – which is not allowed under the PLD.

Another example is formed by the *DES*-case law of the *Cour de cassation*.[739] In these cases, the use of the DES-medicine by mothers during pregnancy, resulted in physical damage suffered by their daughters (and granddaughters). A DES-daughter only has to prove the fact that her mother used the DES-medicine during pregnancy in order to be able to claim damages from any of the commercial DES-manufacturers: a causal link can then be assumed. A respective producer may defend himself by proving that is was not him who provided the specific medicines, but rather another producer, which is in fact a rather theoretical possibility.[740]

When damage could have been caused by multiple tortfeasors, these are jointly and severally liable. This follows from article 1245-13 PLD (implementing article 8(1) PLD) as follows: "The producer's liability to the victim is not reduced by the action of who contributed to the occurrence

[735] Sportes & Ravit 2019, no. 2.2.
[736] Taylor, Fairgrieve & Wester-Ouisse 2018, p. 318-320; Sportes & Ravit 2019, no 2.2.; Borghetti 2016, p. 224-225.
[737] Borghetti 2016, p. 224, referring in footnote 82 to Cass. 1re civ. 22 May 2008, *inter alia*: *Bull. civ.* I, no. 148 and 149; also Taylor, Fairgrieve & Wester-Ouisse 2018, p. 320, who further refer in footnote 96 to Cass. 1re Civ. 5 April 2005, nos 02-11947 & 02-12065, *inter alia Bull* 173, *RTDCiv.* 2005, 607, obs. P. Jourdain.
[738] See Taylor, Fairgrieve & Wester-Ouisse 2018, p. 319. They note however, that since 2008 the *Cour de Cassation* has been more conservative in the presumptions made in those decisions; See also Sportes & Ravit 2019, no. 2.2.
[739] Referred to by Borghetti 2016, p. 224, footnote 83: Cass. 1re civ., 24 September 2009, *Bull. civ.* I, no. 186, *RTD civ.* 2010, 111, obs. P Jourdain, *RDC* 2010, 90, obs. J-S Borghetti.
[740] Ibidem.

of the harm", in relation with the general rules of French liability law.[741] This implicates that a victim may claim full compensation from any of the tortfeasors. After one of the tortfeasors has compensated the victim, that tortfeasor may have recourse from the other tortfeasor(s). Should the liability of the other party be of a strict-liability nature, the amount of the damages is equally split between the parties. When the liability of the other party is based on fault, that party has to remunerate 100% of the damages.[742]

4.2.4.5 Development risk defence

The French implementation of the development risk defence has been controversial. As referred to above, it can be seen as one of the factors which caused the delayed implementation of the PLD into the French legal system, and the original implementation was considered to be contrary to the PLD provisions.[743] The defence has been incorporated in article 1245-10 CC as follows: "The producer is liable by operation of law unless he proves […] (4) that the state of scientific and technical knowledge at the time when he put the product into circulation did not allow discovery of the existence of the defect". It must be noted that article 1245-11 CC stipulates that this exception cannot be invoked "where the harm was caused by an element of the human body or by products derived from it".

The French legislator included another requirement for producers in the original PLD-implementation. The CC stated that a producer could not free himself from liability relying on the development risk defence "if, in the event of a defect manifesting itself within a period of ten years after the product was put into circulation, he has failed to take appropriate measures to avert the harmful consequences thereof".[744] In effect, this constituted a post-sale duty to warn consumers of (later discovered) defects in their products, and to take appropriate action when those defects emerged.[745] This provision was held contrary to the PLD by the ECJ in 2002,[746] and was removed by the French legislator in 2004.[747]

4.2.4.6 Issues of proof

The PLD provision that the claimant has to prove defectiveness, damage and causality has been implemented in article 1245-8 CC. Under French law, there are little dogmatics concerning

[741] Borghetti 2016, p. 225 and 221, referring to *inter alia* Cass. 1re civ., 26 November 2014, *D.* 2015, 405, note J-S Borghetti; see furthermore Sportes & Ravit 2019, no. 2.3; Rouhette, Gallage-Alwis & Houssel 2018, no. 4.
[742] Borghetti 2016, p. 225.
[743] See section 4.2.4.1 and 4.2.4.2, where reference is made to ECJ 25 April 2002, C-52/00 (*Commission/France*), and furthermore Taylor, Fairgrieve & Wester-Ouisse 2018, p. 317-319.
[744] Translation of a part of the former article 1386-12(2) CC by Borghetti 2016, p. 218; see also De La Rochère & Milhac 2007, p. 259-260.
[745] See Fairgrieve 2005, p. 96; Borghetti 2016, p. 218.
[746] ECJ 25 April 2002, C-52/00 (*Commission/France*).
[747] Fairgrieve 2005, p. 96 and Borghetti 2016, p. 218, referring to the *Loi* no 2004-1343 d.d. 9 December 2004.

standards of proof, and courts are rather free in their valuation of evidence (*"intime conviction*").[748] Facts can for instance be established by any possible means – and once established by a (lower) judge, the *Cour de cassation* has no further say in their appreciation of evidence.[749] Furthermore, facts may also be presumed by courts: "judges are allowed to deduce the existence of a fact that has not be proven directly from the existence of other facts"[750] (which have been proven), as follows from article 1382 CC.

In a similar vein, under general French evidentiary rules, it is rather easy for claimants to prove causation. It is for example possible to establish causation by means of "proof by exclusion". When one can for example show that there are no likely alternative sources of certain damage, a source of damage may be deducted therefrom, and indicated as *the* source.[751] Furthermore, French judges are also allowed to use a presumption of a causal link between a defective medicine and damage even in a situation of scientific uncertainty of the stated defectiveness.[752] In 2015, the *Cour de cassation* referred preliminary questions in the *Sanofi/Pasteur* case. As elaborated in section 4.2.2.6, the Court of Justice of the European Union evaluated (many of) the ways in which presumptions are made by French judges to be in line with European law,[753] as long as *inter alia* the burden of proof is not reversed in effect.[754] The French evidentiary rule that formed one of the bases of the preliminary questions, did "not require the victim to produce, in all circumstances, certain and irrefutable evidence of a defect in the product and of a causal link between the defect and the damage suffered, but authorises the court, where applicable, to conclude that such a defect has been proven to exist, on the basis of a set of evidence the seriousness, specificity and consistency of which allows it to consider, with a sufficiently high degree of probability, that such a conclusion corresponds to the reality of the situation".[755] This is considered to be in line with the PLD-provisions, as that rule does not lead to a reversal of the burden of proof. [756] A rule holding that when "one or more types of factual evidence were presented together, an immediate and automatic presumption would operate of there being a defect in the product and/or a causal link between that defect and the occurrence of the damage",[757] is considered too broad, however. Also

[748] See Giesen 2000, p. 54; and for further elaboration of the theory of *intime conviction*: B. Allemeersch, *Taakverdeling in het burgerlijk process*, Antwerpen: Intersentia 2007, p. 463-465. See also, for an elaboration of the French rules in product liability cases: Borghetti 2016, p. 228-229.
[749] Ibidem Borghetti 2016; Giesen 2000, p. 71.
[750] Ibidem.
[751] See Van Dam 2013, p. 325-326, who refers to Civ. 1re 9 May 2001, *D.* 2001, 2149.
[752] Cass. 1re civ., 22 May 2008, as cited in Borghetti 2016, p. 229
[753] CJEU 21 Juni 2017, C-621/15, ECLI:EU:C:2017:484 (*W/Sanofi Pasteur*).
[754] Ibidem, para. 27, 29.
[755] Ibidem, para 28.
[756] Ibidem, para 29.
[757] Ibidem, para. 36.

irrefutable presumptions,[758] and "predetermined causation-related factual evidence"[759] rules are not allowed, according to the CJEU.[760]

4.2.5 IMPLEMENTATION IN ENGLAND

4.2.5.1 Introduction

The PLD is implemented in Part I of the Consumer Protection Act (CPA) 1987,[761] and the amendments made by means of Directive 1999/34/EC were enacted in 2000.[762] While judges in the common-law system of England & Wales, mainly decide on the basis of earlier cases and precedents, the CPA provides statutory rules that need to be applied in product liability cases.[763] The strict-liability rules of the CPA were until recently (upon the enactment of the AEVA 2018, see section 4.2.5.7) the only ones in their kind that were introduced in England and Wales in the 20th century.[764] The CPA-rules operate alongside the (pre-existing) common-law rules based on contract- and tort-actions.[765] Hereafter, my main focus is on the implementation of the PLD.[766] The relation between the CPA and the PLD is addressed in Section 1(1) CPA, stating that the provisions of the CPA are "in order to comply with the product liability Directive and shall be construed accordingly", which has been upheld in case law.[767]

The option the PLD provides for Member States not to implement the development risks-defence was not taken used by the English legislator in the CPA, which includes the defence (that is: an altered version of the one provided in the PLD)[768] in section 4(1)(e) CPA. The other option, to place a cap on liability, was not implemented in the CPA either.[769]

4.2.5.2 Defectiveness and unlawfulness

Section 3 CPA addresses defectiveness. The *legitimate expectations test* encompassed in article 6 PLD ("A product is defective when it does not provide the safety which a person is entitled to

---

[758] According to Van Dam 2013, p. 326, there are some "*legal* 'policy' presumptions" that are deemed irrebuttable under French law.
[759] See Sportes & Ravitt 2019, no. 2.1.
[760] See Veldt & Wissink 2017, p. 260-261; and para's 35-37, 41 and 45 of the *Sanofi/Pasteur* decision.
[761] In 2016, when this research started, there was no concrete indication that Brexit would eventually take place. Therefore, I included England as a part of my research into (implemented) EU regulation. As to date the respective rules have not significantly changed (yet), there is still relevance to include the respective English regulatory frameworks in this study.
[762] See Oliphant & Wilcox 2016, p. 175-176.
[763] See van Dam 2013, p. 94-95.
[764] Van Dam 2013, p. 124.
[765] See Deakin, Johnston & Markesinis 2013, p. 590-591; Oliphant & Wilcox 2016, p. 174-175, and especially the references to *Donoghue v. Stevenson* [1932] AC 562; and *Daniels & Daniels v R White & Sons and Tarbard*. [1938], 4 All ER 258.
[766] See for more on contract- and tort-based actions for example Deakin, Johnston & Markesinis 2013 Chapter 20.
[767] See Burton J., in *A v National Blood Authority* [2001], 3 All ER 289, as discussed in Oliphant & Wilcox 2016, p. 176.
[768] See section 4.2.5.5.
[769] See Oliphant & Wilcox 2016, p. 177.

expect, taking all circumstances into account[…]") has been implemented in a more detailed way in section 3(2) CPA than the PLD prescribes. It extends to *inter alia* (a) "the manner in which, and purposes for which the product has been marketed, its get-up, the use of any mark in relation to the product and any instructions for, or warnings with respect to, doing or refraining from doing anything with or in relation to the product;". By comparison: section 6(1)(a) PLD sees to "the presentation of the product"; and (b) "what might reasonably expected to be done with or in relation to the product", which is to a large extent comparable with the PLD text; and (c) "the time when the product was supplied by its producer to another", whereas a product can be deemed to be supplied "when it enters a marketing process in the form in which it is offered to the public in order to be used or consumed".[770] The implemented version thus is slightly broader than the text of art.6(1)(c) PLD, which refers to "the time when the product was put into circulation".

> Burton J's landmark decision in *A v National Blood Authority* is exemplary for the application of the *legitimate expectations test* under English law.[771] In that case was (*inter alia*) held that, despite the absence of means for determining the existence of hepatitis C in blood in respective specimens, the National Blood Authority was found liable for the contamination of blood that was supplied to patients, who may have relied on a legitimate expectation, taking all *relevant* circumstances into account (emphasis added *RWdB*),[772] that the blood they were supplied with, was free of that virus,[773] also given the fact that the National Blood Authority did not inform the public of the possibility of hepatitis C contamination risks.

In English case law, a distinction is made between three kinds of defects, being 1) defects occurring in the "design" stage of a product ("design defects");[774] 2) defects occurring in the manufacturing stage, resulting in products that do not comply with the specifications ("manufacturing defects");[775] and 3) defects that result from a failure of the producer to warn for the existence of specific risks, or a failure to instruct consumers carefully how to use the respective

[770] Oliphant & Wilcox 2016, p. 186.
[771] This decision also holds important rulings for *inter alia* determining the scope of the development risks defence.
[772] Howells (2005) observes (p. 143) that whereas the PLD refers to *all* circumstances, it was "brave" of Burton J to specify that only the *relevant* circumstances should be taken into account, and that "[t]he object of the law is not to force all products to have the highest safety standards, merely to make them acceptably safe".
[773] See for an analysis of the case and an introduction to the academic debate it caused: Howells 2005, p. 140-141.
[774] For example unanticipated side effects in a new medicine, or a motor vehicle that does not behave as it should, with "a tendency to swerve", see for more on both examples Deakin, Johnston & Markesinis 2013, p. 615.
[775] Ibidem; they refer here to *Donoghue v. Stevenson*, where a dead snail in a bottle caused illness of the consumer who drank the ginger beer that was alongside the snail captured in the bottle.

product ("instruction defects").[776] The *legitimate expectations test* is held to be most useful regarding manufacturing defects, but the sensibility of this test regarding instruction- and (especially) design defects has been debated.[777] It has been questioned how far the duties to warn for producers would reach, and it is observed regarding instruction defects that it is not clear how to address "different expectations which particular groups of consumers might have".[778] Those who oppose against the *legitimate expectations test* sometimes advocate another test that is used under US law, the *risk-utility test*. Opponents of the *legitimate expectations test* argue that is incoherent, as "in many situations […] the consumer would not know what to expect, because he would have no idea how safe the product could be made".[779] The *risk-utility test*, mostly used to determine design- and instruction defects, would however allow a case-by-case analysis (by courts) of the balance between on the one hand the "social utility of a product" and on the other hand the "risk and seriousness of any injury that might occur from its use".[780] For this test, the "reasonably prudent manufacturer" stands model, whereby notion is taken of his "capacity to eliminate the defect and his capacity to spread the risk through insurance or through price variations",[781] or, alternatively, "the role of the consumer by considering whether an alternative product was available, how far the consumer was aware of the danger in question, and how far he could have avoided it".[782] Whereas different approaches were taken for establishing defectiveness by English courts before the *A v National Blood Authority* decision, it was concluded in that case that the *legitimate expectation test* must be taken as a point of departure for the determination in any defectiveness-assessment,[783] but it is also considered

> "premature to infer from the silence of the Directive on this point that the English courts will not take something from the American practice of setting a consumer expectation

[776] Ibidem, and their reference to *Vacwell Engineering v. BDH Chemicals* [1971] 1 QB 88. In this case, a producer of chemicals contained in glass ampoules put a label on these ampoules warning for "harmful vapour". As a scientist washed the label of an ampoule with water, it cracked and the liquid contained therein, leaked in the water and caused a massive explosion, causing the roof of the lab to blow off, shattered walls and the death of the scientist. It was held that the producer not only had to warn for the harmful vapour, but also for the risks for the explosive character of the liquid when reacting with water.
[777] See Deakin, Johnston & Markesinis 2013, p. 613-614.
[778] Ibidem, p. 613. Also: Howells 2005, p. 146-147.
[779] Quotation taken from Deakin, Johnston & Markesinis 2013, p. 616, who in turn cite Wade, J.W., "On the Nature of Strict Tort Liability for Products", *Mississippi Law Journal* 1974, no. 44, 825, cited by the Supreme Court of California in *Barker v Lull Engineering Co*., 573 P 2d 443, 454 (1978).
[780] Deakin, Johnston & Markesinis 2013, p. 616.
[781] Ibidem.
[782] Ibidem, and the reference to *inter alia* Birnbaum, S., "Unmasking the Test for Design Defect", *Vanderbilt Law Review* 1980, 33, p. 593.
[783] *A v National Blood Authority*, no. 56, as analysed by Deakin, Johnston & Markesinis 2013, p. 681; see also Oliphant & Wilcox 2016, p. 184-195.

standard for manufacturing defects and a broader risk-utility calculus for design defects and failures to warn".[784]

The CPA does not establish a duty to warn for newly discovered defects,[785] after they have been put into circulation. However, as Oliphant & Wilcox observe, "it may be said that producers owe a strict duty to ensure that their products are not defective", [786] where they refer to safety regulations for more concrete obligations for producers to warn consumers.[787] However, these regulations are not of decisive influence for establishing (product) liability. Deakin, Johnston & Markesinis read in section 3(2) "to the promotion and packaging of the product [an implied obligation to warn consumers, RB] generally of possible dangers",[788] which can also be read in the *legitimate expectations test.* Such warnings should see to the dangers that were known by the manufacturer, or reasonable foreseeable, and should "include a duty to warn for foreseeable but unintended uses and misuses".[789]

4.2.5.3 Damage

Parallel to the provisions of the PLD, recoverable damages under section 5 of the CPA are limited to death or personal injury, or any loss or damage to any property (including land). Damage to product itself or "for the loss of or any damage to the whole or any part of any product which has been supplied with the product in question comprised in it",[790] is not eligible for remuneration. Furthermore, (property) damage is only awardable when it concerns non-business property, when used for private purposes.

> This implicates for example that the producer of a defective car tyre, which caused a crash of the vehicle (manufactured by another producer than the tyre-maker) of which the tyre formed part, might not be held liable under the CPA, if the car is seen as "the product itself".[791] Following the decision of the House of Lords in *Murphy v Brentwood District Council*,[792] Deakin, Johnston & Markesinis consider it "highly likely that different parts will be seen as the same whole for this purpose, denying the consumer recovery for the damage to the product as a

[784] Deakin, Johnstin & Markesinis 2013, p. 618.
[785] The general obligations to warn following from the PLD do apply however, see section 4.2.2.3.
[786] Oliphant & Wilcox 2016, p. 186-187.
[787] Reference is made to Part II of the CPA and the General Safety Regulations 2005 contained therein.
[788] Deakin, Johnston & Markesinis 2013, p. 619.
[789] Ibidem. They furthermore refer to general negligence duties, which constitute a duty to warn for defective products that are first sold (and which do not apply to for example auction sales, where a car was sold "as seen and with all its faults"), as was decided in *Hurley v Dyke* [1979] RTR 265. Moreover, a producer can be held liable when he fails to correct a false safety-statement (see their reference to *E. Hobbs Farms Ltd v. Baxendenden Chemical Co. Ltd* [1992] 1, Lloyd's Rep. 55, 65.
[790] Section 5(2) CPA.
[791] This question is brought up in Deakin, Johnston & Markesinis 2013, p. 624.
[792] *Murphy v Brentwood District Council* [1991] 1 AC 398.

whole".[793] However, this observation might contradict article 2 PLD, which defines products as "all movables even if incorporated in another movable".[794]

Section 5(4) CPA holds that no damages will be awarded when the amount of property-damage (excluding interest) would be under £275. This amount is seen as a threshold under English law.[795]

There are different points of view regarding the remunerability of pure economic loss under the CPA. Deakin, Johnston & Markesinis observe that it is uncertain to what extent pure economic loss is recoverable under the CPA.[796] They define pure economic loss as "economic losses that do not flow directly out of either personal injury to the consumer or damage to his property".[797] In line with Fairgrieve et al.,[798] (and in the same volume) Oliphant & Wilcox observe that pure economic loss is not recoverable at all, as "it does not fit in the categories of damage giving rise to liability specified in sec 5 CPA", although it may be "readily recoverable in contract".[799] Deakin, Johnston & Markesinis add that it is uncertain whether or not "economic losses that do not flow directly out of either personal injury to the consumer or damage to his property"[800] would qualify for remuneration. They explain that breach of warranty, constituting an action in contract, will lead to the obligation to remuneration of also economic losses, "subject to the normal rules of remoteness of damage in contract".[801] When a claim is based on a negligence-action, chances are less that damages consisting of pure economic loss will be awarded,[802] unless liability "for negligent misstatement" can be established,[803] which may be the case "as a result of misleading labels on articles, or more speculatively through misleading promotion",[804] although there is not much case law available to prove these assumptions. Whereas situations of pure economic loss

[793] See Deakin, Johnston & Markesinis 2013, p. 624-625.
[794] It will thus depend on the definition of "movables" under English law, and the question when a movable stops to be a single movable, and is to be seen as "incorporated" in another movable. Cf. the concepts of "natrekking" and "bestanddeelvorming" under Dutch law. See furthermore Fairgrieve et al. 2016, p. 33.
[795] Oliphant & Wilcox 2016, p. 190; Deakin, Johnston & Markesinis 2013, p. 624.
[796] Deakin, Johnston & Markesinis 2013, p. 624.
[797] Ibidem.
[798] They observe that, despite *Veedfald* (see section 4.2.2.7 in this study), "[b]oth the structure of art 9 and recitel 9 of the Directive's preamble […] clearly indicate that pure economic loss which is not a consequence of physical deterioration of property is outside the scope of the Directive", on p. 32-33.
[799] Oliphant & Wilcox 2016, p. 189.
[800] Ibidem.
[801] Ibidem, and their references to *Hadley v Baxendale* (1854) 9 Exch.; and Treitel G.H., *Law of Contract*, London, Thomson Sweet & Maxwell, 2003, p. 965 ff.
[802] As a consequence of the *Murphy v Brentwood* decision, referred to above.
[803] *Hedley Byrne & Co. Ltd. v Heller & Partners* [1964] AC 465.
[804] Deakin, Johnston & Markesinis 2013, p. 624.

will, in my view, not be the most prominent consequences of AV-defects, further elaboration on the remunerability of this type of loss in England will not be done in this study.[805]

Regarding personal injury, it must be noted that there may be an obligation to remunerate damages related to "nervous shock", which can be derived from the definition of personal injury in section 45 CPA, which "includes any disease and any other impairment of a person's physical or mental condition".[806] Although more difficult, also third parties, with a close family or personal tie with the person who suffers injury from a defective product, may be awarded damages, when "the plaintiff must witness the accident or come to the scene shortly afterwards",[807] and when a causal link between the defect an the nervous shock can be proved. It seems that mere anxiety or distress are not recoverable under the CPA.[808] When a defect in a product causes death, the "personal representatives" (relatives) of the deceased can claim damages from the producer.[809] This could include bereavement damages, as is indicated in section 6(1)(a) CPA which refers to the Fatal Accidents Act 1976. Bereavement damages consist of a fixed sum of £ 12,980,- which can be claimed by the wife, husband or civil partner of the deceased,[810] and, when the deceased is an non-married minor, by his or her parents.[811]

4.2.5.4 Causation

As matters of causation were not harmonized by the PLD, the rules of "causation and remoteness" that are used in negligence cases are applied in England and Wales. [812] Also in English law, distinction is made between factual and legal causation. Factual causation is in product liability cases decided using the "but-for" test, which can be put as follows: "would the loss have been sustained but for the relevant act or omission of the defendant?".[813] When the probability is over 50% that a certain action or event (a defect in case of product liability) caused

[805] However, the fact that there is some uncertainty in this regard, this will be taken into account in Chapter 7.
[806] Ibidem, p. 625.
[807] Ibidem; they refer to *McLoughlin v O'Brien* [1983] AC 410, and *Alcock v Chief Constable of South Yorkshire* [1993] 1 AC 310.
[808] See Williams, A. & Spencer, M., "England & Wales: Product Liability 2019", in: Williams, A. & Fox, T., *Product Liability Laws and Regulations 2019*, London: ICLG 2019, chapter available online via https://iclg.com/practice-areas/product-liability-laws-and-regulations/england-and-wales (last accessed 13 November 2019). Wiliams & Spencer refer to *AB and others v Tameside & Glossop Health Authority and Others* [1997] 8 Med LR 91.
[809] Oliphant & Wilcox 2016, p. 189.
[810] Section 1A(2)(a) Fatal Accidents Act 1976.
[811] Section 1A(2)(b) Fatal Accidents Act 1976. See furthermore Oliphant & Wilcox 2016, p. 196; Deakin, Johnston & Markesinis 2013, p. 849-850.
[812] See Deakin, Johnston & Markesinis 2013, p. 622; Oliphant & Wilcox 2016, p. 191-192; Van Dam 2013, p. 316.
[813] Deakin, Johnston & Markesinis 2013, p. 218.

certain loss, factual liability may be established, and that liability is denied when the probability is under 50%.[814]

> In *McTear v Imperial Tobacco Ltd*,[815] the claimant, who contracted lung cancer after having smoked for many years, did not succeed in proving factual causation: The judge found "that individual causation, in the sense of a link between cigarette smoking and he pursuer's lung cancer, had not been made out either, given the possibility that he could have contracted lung cancer from one of a number of different sources. It could not be shown, on a balance of probabilities, that the pursuer would not have contracted lung cancer had he not been exposed to tobacco smoke from the defenders' cigarettes".[816] It must be observed that proportional liability, which is sometimes and under special circumstances assumed by courts in The Netherlands,[817] has not (yet) been applied in England and Wales,[818] in other than cases of "invisible disease".[819] Furthermore "loss of a chance"-doctrine does not play a critical role in the CPA-context, as elaborated in *A v. National Blood Authority*, as this would (only) result in pure economic loss,[820] which is probably not remunerable.

When there are two (or more) events or acts that could have individually led to certain damage, but it is uncertain i.e. the claimant is unable to prove which one was the specific cause of loss, the English *alternative causality* rule holds that "it is sufficient to show that the defendant's conduct 'materially contributed' to the claimant's injury or to the risk of the same".[821]

When factual causation has been established, legal causation can limit the obligation to remunerate damages by the defendant. This follows *inter alia* from the *remoteness of damage* rule. It follows from the Privy Council decision in *The Wagon Mound (No. 1)* case,[822] that too remote damage, i.e. that consequences of a certain act cannot be foreseen by a reasonable person, is not eligible for remuneration.[823] It must be noted however, that "foreseeability of consequences is often accepted even if they occur in an unusual way, particularly in personal injury cases".[824]

---

[814] See Van Dam 2013, p. 316.
[815] *McTear v Imperial Tobacco Ltd.* [2005] 2 SC 1.
[816] Citation from Deakin, Johnston & Markesinis 2013, p. 622.
[817] See 4.2.3.4.
[818] See Wilcox & Oliphant 2016, p. 191.
[819] In *Fairchild c Glenhaven Funeral Services Ltd* [2003] 1 AC 32, it was held that "proportionate liability" can be applied in cases where invisible diseases, such as mesothelioma, are involved.
[820] Ibidem, p. 190-191.
[821] Wilcox & Oliphant, p. 192, and their references to *Bonnington Castings Ltd v Wardlaw* [1956] AC 613 (regarding the *actual* injury); and *McGhee v National Coal Board* [1973] 1 WLR 1; *Fairchild c Glenhaven Funeral Services Ltd* [2003] 1 AC 32 (regarding the *risk* of injuries). See also Deakin, Johnston & Markesinis 2013, p. 622-623.
[822] *Oversees Tankship (UK) Ltd v Morts Dock & Engineering Co. (The Wagon Mound (No. 1)* [1961] AC 388.
[823] See Van Dam 2013, p. 317; Deakin, Johnston & Markesinis 2013, p. 623.
[824] Van Dam 2013, p. 317.

Another ground for limitation of liability can be formed by *contributory negligence*, which follows from section 6(4) CPA and the Law Reform (Contributory Negligence) Act 1945,[825] or *intervening acts of a third party*.[826]

4.2.5.5 State of the art defence

As the "state of the art defence" (also referred to as "development risk defence") is implemented in the CPA in a different way than has been provided in the PLD, the wording and scope of the English version is shortly elaborated here. The PLD prescribes in the (non-mandatory) provision of article 7(e) that a producer can free himself from liability if he proves "*that the state of scientific and technological knowledge at the time he put the product into circulation was not such as to enable the existence of the defect to be discovered*". The scope of section 4(1)(e) CPA is different, and stipulates that a producer is not liable when he can show that

> "*the state of scientific and technical knowledge at the relevant time was not such that a producer of products of the same description as the product in question might be expected to have discovered the defect if it had existed in his products while they were under his control.*"

The European Court of Justice assessed whether or not the English implementation accorded to the PLD-provision.[827] It was held that section 4(1)(e) CPA did accord to the PLD. [828] The court observed *inter alia* that the PLD provision does not refer to the subjective knowledge of a respective producer, or the applicable industrial standards, but rather "unreservedly, [to] the state of scientific and technical knowledge, including the most advanced level of such knowledge, at the time when the product in question was put into circulation".[829] Furthermore, the ECJ emphasized that article 7(1)(e) PLD sees to the

> *"objective state of scientific and technical knowledge, including the most advanced level of such knowledge, at the time when the product in question was put into circulation [... which…] must have been accessible at the time when the product in question was put into circulation".*[830]

The ECJ concluded that section 4(1)(e) CPA does not conflict with article 7(1)(e) PLD.[831]

---

[825] See Wilcox & Oliphant 2016, p. 192; Deakin, Johnston & Markesinis 2013, p. 317.
[826] See Wilcox & Oliphant 2016, p. 192.
[827] ECJ 29 May 1997, C-300/95, ECLI:EU:C:1997:255 (*European Commission/United Kingdom*).
[828] See Deakin, Johnston & Markesinis 2013, p. 620-621; Oliphant & Wilcox 2016, p. 194-195.
[829] ECJ *European Commission/United Kingdom*, cons. 26.
[830] Ibidem, cons. 29. Oliphant & Wilcox observe that "only serious or scientific opinions are relevant" in this respect (p. 194).
[831] Ibidem, cons. 33-39.

The development risk defence played a role in *A v National Blood Authority* referred to in section 4.2.5.2 above. In that case, the National Blood authority was aware of the fact that blood (products) to be transfused might be infected with the Hepatitis C-virus. However, there were, at that time, no means available for actually discovering the virus in blood samples. Despite the absence of such means for discovery of Hepatitis C in respective specimens, the National Blood Authority could not free itself from being held liable on the basis of the development risk defence.[832]

4.2.5.6 Issues of proof

Also in the English academic literature, it is observed that "[c]laimants frequently argue that the complexities of products make it almost impossible" and "also […] extremely costly for claimants to obtain expert evidence to prove a specific defect".[833] As a means to assist claimants in proving defectiveness, a court may however, based on the facts at hand, presume that a product was defective, if there is for example no other plausible explanation available.[834] Inferences may also be made regarding the proof of causality between a defect and damage.[835] Such inferences are not a reversal of the burden of proof, which rests on the claimant.[836] This is illustrated by for instance (recent) decisions in *Love v Halford,*[837] and *Hufford v Samsung Electronics*.[838] In the *Love v Halford* case, a steerer tube of a bike cracked. While in *Ide v ATB Sales Ltd* it was held that a defect was not improbable where the handlebars of a bike cracked, in this case it was judged that there was no appropriate evidence, and that the crack in the steerer tube may have also been caused by earlier accidents, and insufficient repairs.[839] In *Hufford v Samsung Electronics*, a fridge-freezer caught fire. The fire could have originated inside the apparatus (as was stated by the claimant), or on the outside (argued by the defendant). The judge was not convinced by the arguments of the claimant, and did not assume defectiveness.[840] In *Hufford* however, it was stated that it was enough for a claimant to prove in general terms the existence of a defect, rather than that he has to prove that defect very precisely.

An instrument that is used by courts in The Netherlands to relief the sometimes heavy burden of proof, is to assume defectiveness or causality when a safety standard (either expected or

[832] Burton J. in *A v National Blood Authority* [2001], 3 All ER 289, paragraph 47 and following.
[833] See East 2017, p. 71. In a similar vein:
[834] See East 2017, p. 71 and Oliphant & Wilcox 2016, p. 184, both referring to *Ide v ATB Sales Ltd* [2008] EWCA Civ. 424.
[835] Wilcox & Oliphant 2016, p. 191, again referring to *Ide v ATB Sales Ltd*.
[836] See East 2017, p. 71.
[837] [2014] EWHC 1057 (QB), referred to by East 2017, p. 72.
[838] [2016] EWHC 2956 (TCC), also referred to by East 2017, p. 72.
[839] See East 2017, p. 72.
[840] Ibidem.

advertised) is violated.[841] This instrument seems not to be of major importance under English law, if applicable at all.[842] *Res ipsa loquitur* is not applied as such by English courts in CPA-cases, although this notion that "the facts speak for themselves" may be taken into account when courts infer for example defectiveness or causality.[843]

4.2.5.7 Product liability aspects of the Automated and Electric Vehicles Act 2018 (AEVA)

As indicated above, the current provisions of the CPA may implicate problems for those who want to claim remuneration for damage they have suffered from AV-defects, for example regarding their obligations to prove a defect, damage and causality. Some of these problems will be relieved, as a result of the effectuation of the Automated and Electric Vehicles Act of 2018 (AEVA).[844] The AEVA provides, notwithstanding "any other person's liability",[845] that: "*where— (a) an accident is caused by an automated vehicle when driving itself on a road or other public place in Great Britain, (b) the vehicle is insured at the time of the accident, and (c) an insured person or any other person suffers damage as a result of the accident, the insurer is liable for that damage*".[846]

When there is no sufficient insurance and a person is injured, it is the owner of the vehicle who can be held liable.[847] The damage to be remunerated means in this respect "*death, personal injury and damage to property, other than (a) the automated vehicle, (b) goods carried for hire or reward in or on that vehicle or in or on any trailer (whether or not coupled) drawn by it, or (c) property in the custody, or under the control, of (i) the insured person […], or (ii) the person in charge of the automated vehicle at the time of the accident […]*".[848] Contributory negligence will be allowed as a defence for the insurer or the owner.[849] This may include the situation that a vehicle is allowed in "self-driving mode" when it was not appropriate to do so.[850]

[841] See section 4.2.3.5.
[842] See Deakin, Johnston & Markesinis 2013, p. 614-615; and Giesen 2001, p. 199 (footnote 35).
[843] See Deakin, Johnston & Markesinis 2013, p. 593-594.
[844] Other, traffic liability, aspects of the AEVA are elaborated in section 4.3.4.4. See for further elaboration on product liability aspects De Bruin 2020. The AEVA, i.e. the relevant articles entered into force on 21 April 2021 (see https://www.legislation.gov.uk/uksi/2021/396/regulation/3/made).
[845] Section 2(7) AEVA.
[846] Section 2(1) AEVA.
[847] Section 2(2) AEVA.
[848] Section 2(3) AEVA.
[849] Section 3 AEVA.
[850] Section 3(2) AEVA.

The allocation of liability may furthermore be refused or limited when the insured person makes (or allows to make) alterations to the AV-software in conflict with the insurance policy,[851] or when the insured person fails to install safety-critical software-updates.[852]

When liability is imposed on the insurer or AV-owner, and the amount of the liability has been settled, there will be a right to claim against the person who was actually responsible for the accident,[853] including for instance a producer of a defective AV-component. Then, the "traditional" CPA-rules will apply.

The AVEA thus extends the scope of the currently existing compulsory liability insurance schemes in the UK, in the sense that such schemes traditionally applied to (human) drivers when driving their vehicles, which is now extended to the driving of the cars themselves (without human operation).[854]

> It can be an easier route for victims to claim damages that result from accidents in which AVs are involved under the AEVA than under the English PLD-implementation. That mainly follows from the fact that a victim does not have to prove defectiveness, damage and causality, where producers have ample possibilities to exonerate liability on the basis of *later existence*-; *development risk*-; and *contributory negligence* defences. Under the AEVA, victims 'only' have to prove the involvement of an AV while in autonomous mode, and the causal relationship with suffered damage. Although the AEVA-defences (contributory negligence; inappropriate use of autonomous driving mode; unallowed software alteration or the failure to install critical safety updates) do require a more thorough analysis of facts and data, the onus of proof rests at the insurer or uninsured owner who has, or ought to have, better access to, and interpretation possibilities of those data than the victim.[855]

[851] Section 4(1)(a) AEVA.
[852] Section 4(1)(b) AEVA. See the other sub-sections for more detailed provisions.
[853] Section 5 AEVA.
[854] See for example Bond, J, "Automated and Electric Vehicles Act 2018 Becomes Law", Penningtons Manches Cooper 24 July 2018, via https://www.penningtonslaw.com/news-publications/latest-news/2018/automated-and-electric-vehicles-act-2018-becomes-law (last accessed 13 November 2019).
[855] See also De Bruin 2020, p. 747-748.

4.2.6 *CONCLUSION*

Having assessed the outlines of the European Product Liability framework and the implementation thereof in The Netherlands, France and England, some conclusions can be drawn from the findings above, and assumptions can be made regarding the application of the rules in view of the expected innovations in the field of AVs. These conclusions and assumptions, which will be further evaluated in the third part of this study, include the following.

The *products* definition may be problematic, as it is unclear to what extent (stand-alone) AV-software would be included under the scope of the PLD. Although it seemed to be the intention of the European regulator to include software under its scope, it is, given the current case law of the CJEU, uncertain whether or not software as such may be qualified as a product. However, it can be assumed that when software that is embedded in hardware is malfunctioning, this could implicate defectiveness of the hardware product.

Also the *defectiveness* criterion does not exactly prescribe the level of safety that consumers may expect regarding the operation of autonomous vehicles. The question will be, for instance, whether or not a comparison must be made with the "average" human driver, or that the standard would be higher, i.e. conforming to the most excellent, failsafe human driver. Also, it remains an open question whether or not a lack of cybersecurity could constitute defectiveness, when for instance an AV is hacked into due to inadequate security measures taken by a producer. It can be argued, also further to the recent adaptations of the CSD, which result therein that "sellers of goods with digital elements" must make sure to provide (security) updates, that AVs should be qualified as *defective*, when such updates have not been provided and AVs become unsafe as a result thereof.

Also, I observed that the actual product liability framework contains potential proof-issues for victims. As *inter alia* technical complexity shall increase as vehicles become more autonomous, it will for example not always be easily possible to easily establish defectiveness of an AV(-component), and/or to prove a causal relationship between an established defect and the damage of a victim. This will often require access to technical data, and the expertise to interpret these. It is however possible, within certain boundaries, that judges aid victims in their proof-position, as long as the burden of proof regarding defectiveness, damage and causality, is not reversed. It must be noted, that the willingness to aid victims differs between the studied regimes.

Furthermore, it was observed that the catalogue of *defences* is currently in favour of producers of allegedly defective AVs. The *development risk* defence could allow producers for instance to escape liability rather easily, when they can prove that a defect could not have foreseen the existence of a defect. Also the *later existence* defence might apply to self-learning AVs, when a producer can

establish that the product he brought into circulation did not contain a certain defect that materialised afterwards.

Although the PLD stipulates which heads of damages may (not) qualify for remuneration, there are certain differences between the studied implementations. It seemed that in France and The Netherlands, it is easier to have immaterial damages or pure economic loss remunerated than under the English implementation.

4.3 TRAFFIC LIABILITY

4.3.1 INTRODUCTION: NO HARMONISATION OF SUBSTANTIAL TRAFFIC LIABILITY RULES

In the following sections, an overview is given of extra-contractual traffic liability rules that are relevant for the analysis of the case study introduced in section 3.5. These rules can be applied in order to determine whether or not damages of victims of AV accidents have to be remunerated by for instance a driver, owner or keeper of an autonomous vehicle. Despite several harmonisation attempts, extra-contractual liability for motor vehicle related accidents is still a matter of national law.[856] Roughly two types of regimes can be identified.[857] First – and oldest – are the regimes (usually within common-law systems) that adhere to *fault* of a motor vehicle driver in order to determine whether or not and to what extent an accident victim must be compensated for his losses. Second, most continental European (civil law oriented) systems have a *risk*-based liability regime in place. In the following sections, the systems are studied that apply in England (and Wales), comprised of the traditional *fault*-based negligence-rules, and the new risk-based AEVA-regime, as well as France and The Netherlands – which are primarily *risk*-based (France), and of a mixed nature (The Netherlands).

Although the rationales behind both different regimes are not elaborated in detail, some general observations can be made that illustrate the difference between the two systems. An "accusation of misconduct" lies at the core of *fault*-based liability.[858] It must therefore be assessed in principle to what extent a driver of a motor vehicle who was involved in an accident, acted negligently, and if so, it is his "moral obligation" to remunerate damages to the extent resulting therefrom.[859] In *risk*-based liability systems, the question of who was at fault is not (or at least: less) relevant, as it departs from the Betriebsgefahr-idea, "that someone who is permitted to use a particularly dangerous thing for his own advantage should equally bear the associated risk".[860] Whereas *risk*-based liability regimes often operate alongside and without prejudice to *fault*-based liability (i.e. a claim can be based on both a *risk*- and a *fault*-liability rule at the same time, which can be necessary if for instance the *risk*-regime does not provide for remuneration of all (types of) damages that one might want to be compensated for), the opposite is often not true.

[856] See Ernst 2010, p. 7, 10; Engelhard & De Bruin 2018, p. 32.
[857] See Karner 2018, p. 366-367.
[858] Ibidem,p. 368, and his reference to Widmer, P., "Comparative Report on Fault as a Basis of Liability and Criterion of Imputation", in Widmer, P. (ed.), *Unification of Tort Law: Fault*, Den Haag: Kluwer Law International 2005, p. 331-367.
[859] Karner 2018, p. 368 refers here to Koziol, H., *Basic Questions of Tort Law from a Germanic Perspective*, Vienna: Jan Sramek Verlag 2012, p. 171.
[860] Karner 2018, p. 368.

An important novelty must be noted: where *risk*-liability regarding motor vehicle accidents was never recognized until recently in England and Wales, the regime of the Automated and Electric Vehicles Act 2018 (AEVA 2018) does just that: also in England combinations of *risk*- and *fault*-based liability claims will become possible.

Thus, there are significant differences between the applicable regimes of the Member States. France for example has installed with the *Loi Badinter* a very strict liability regime, providing that in almost every circumstance victims of motor vehicle related accidents have to be fully compensated by the driver or keeper of the vehicle. The French regime is elaborated further in section 4.3.3. The system in the Netherlands, as elaborated in section 4.3.2, is a little less strict than the French, in the sense that owners or keepers of motor vehicles are obliged to remunerate at least 50% of non-motorized victims (over the age of 14), and that for the other 50% apportionment of damages may depend on *inter alia* contributory negligence of the victim. The English regime, illustrated in section 4.3.4, is of another nature: whether or not a driver of a motor vehicle has to compensate a traffic accident victim, is a matter of *negligence* at the side of the driver. Although there is a rather high *standard of care*, there is no risk liability for such cases in England. As stated, that has changed for (at least some future) *automated vehicles*, as the AEVA 2018 has entered into force. The AEVA 2018 entails a strict liability mechanism for insurers or (non-insured) owners of such vehicles.

Before exploring into more detail the regimes of the three systems indicated above, some observations must be made regarding the part of motor vehicle accident law that *has* been harmonised in the EU. While every of the three jurisdictions studied in the following sections (The Netherlands, England and France) have varying insurance mechanisms related to motor vehicles, EU harmonisation took place by means of the Motor Vehicles Insurance Directive.[861] The MVID contains rules regarding *inter alia* high standards of protection for motor vehicle accident victims, irrespective of the place (in Europe) where it happened; it sets minimum rules on mandatory civil liability insurance;[862] holds minimum amounts of compensation for damages to be covered by such insurance;[863] harmonises exclusion clauses;[864] and guarantees 'easy access' for cross-border

[861] Directive 2009/103/EC of the European Parliament and of the Council relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability, 2009, *OJ* L 263 (Motor Vehicles Insurance Directive, MVID). This is officially the fifth EU directive; the predecessors (Directives 72/166/EEC, 84/5/EEC, 90/232/EEC, 2000/26/EC and 2005/14/EC) have been repealed in art. 29 MVID. A proposal for a revised Directive has been published in 2018: EC COM(2018) 336 final, 2018/0168 (COD), available via https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1407-REFIT-review-of-the-Motor-Insurance-Directive (last accessed 29 April 2020).
[862] Article 3, 5 MVID.
[863] Article 9 MVID.
[864] Article 13 MVID.

accident victims to file for compensation.[865] In practice, victims of motor vehicle related accidents, will not have to 'go beyond' the insurance companies to receive compensation for their losses, and will, in many cases, not have to claim damages themselves based on the underlying liability rules. These rules are however often used by insurers in order to seek redress from the insurers of actual tortfeasors.[866]

Besides (mandatory) motor vehicle insurance, there are several other forms of insurance that can be used to compensate victims of motor vehicle accidents.

> Such systems, recently illustrated by Karner, include *inter alia*: voluntary loss (first party) insurance, where for instance vehicle owners can take out insurance in order to compensate their own losses,[867] regardless of the accident cause, whereby the costs are spread between the participants of the insurance scheme; social insurance systems, which compensate – often to a limited extent - personal injuries by accident victims, regardless of the accident cause,[868] whereby the costs are borne by society as a whole, and whereby in some jurisdictions recourse can be sought from the tortfeasor; and no-fault compensation systems, that result therein that victims are compensated to a limited extent and scope (often personal injuries only), regardless of who was at fault – which systems have in fact replaced the possibility to seek compensation based on tort law in some common law jurisdictions such as New Zealand.[869]

Insurance mechanisms may thus also cover for losses that are not compensable under the applicable liability regimes. It must be noted although that the scope and amount of damages to remunerated under (voluntary) insurance are often limited (for instance to personal damages caps are placed on the sums to be awarded).[870] In the following sections, the focus will be on the liability regimes, rather than on the insurance mechanisms, of The Netherlands (section 4.3.2), France (section 4.3.3) and England (section 4.3.4). The reason for this focus is that the norms for determining liability in AV-related accidents are encompassed in the liability regimes rather than in the rules concerning liability insurance.

[865] Articles 20-26 MVID.
[866] In most cases redress from tortfeasors is only possible to a very limited extent, and applies for instance only when the tortfeasor was drunk when driving, see Karner 2018, p. 372.
[867] See Karner 2018, p. 374-376. See also on potential benefits of first party insurance schemes Schijns 2019.
[868] ibidem p. 376-377.
[869]ibidem p. 378-381.
[870] See Engelhard & De Bruin 2018, p. 31-32.

4.3.2 THE NETHERLANDS

In The Netherlands, "traffic liability", i.e. liability for accidents in which motorised vehicles are involved, is addressed in article 185 Wegenverkeerswet (WVW). That provision stipulates, as will be elaborated in the following sections, a risk-liability of the owner or the keeper of a motor vehicle towards non-motorised victims (pedestrians and cyclists). Liability towards other victims, such as the passengers of the vehicle itself or those of another vehicle, can be based on general liability provisions, for example fault-based liability as addressed in article 6:162 BW, or liability for dangerous equipment as addressed in article 6:173 BW. As the objective of this part of the study is to focus on specific traffic liability rules, the provisions of article 185 WVW will be further illustrated here. Furthermore, reference is made to article 6:162 BW, to the extent that case law provides specific rules for accidents with motor vehicles, where damage compensation is not covered under article 185 WVW. As article 6:173 BW is currently seldomly applied in traffic liability cases, but that might change given the advent of AVs,[871] attention is also paid to that regime, which addresses liability for movable goods.

The next sections are structured as follows. The text of article 185 WVW and the purposes of the legislator are introduced in section 4.3.2.1. Section 4.3.2.2 focuses on the risk liability nature regarding the allocation of liability, and the most important defence of "overmacht" (*force majeure*). Section 4.3.2.3 is about the apportionment of damages upon a successful liability claim. Special attention is paid to the role that contributory negligence can play. The regime of article 6:162 BW as applicable in traffic liability cases is sketched in section 4.3.2.4.1, and in section 4.3.2.4.2, an overview is given of the rules that applies to defective movable goods.

4.3.2.1 Article 185 WVW: introduction and purpose

Article 185 WVW was introduced in 1994. It succeeded article 25 (later 31) of the Motor- en Rijwielwet (Motor Vehicles and Cyclists Act) as introduced in 1924, which was to a large extent comparable to the current provision.[872] It created a strict liability for keepers of motor vehicles to remunerate damages to cyclists and pedestrians, unless *force majeure* was plausible.[873]

By creating the regime, the legislator sought to resolve issues that traffic-accident victims had in successfully claiming damages under the general fault-based liability provisions. It was observed that it was (too) difficult for victims of traffic accidents in which motor vehicles were involved, to prove drivers' faults and causality, in a period in which such accidents dramatically increased.[874]

---

[871] See Tjong Tjin Tai & Boesten, p. 657, who indicate that the regime of art. 6:173 BW can be applied in AV cases (since 2005).
[872] See Van Dam & Van Maanen 2010, p. 132-136 for a historical overview of the development of the provision which now is article 185 WVW.
[873] See Van Dam & Van Maanen 2010, p. 123-133.
[874] See Hartkamp & Sieburgh 2019, nr. 273; Van Dam & Van Maanen 2010, p. 132-133.

Proof-issues for victims would be minimised by a 'default' liability for keepers of motor vehicles, whereas there still remained the possibility to prove *force majeure* for motor vehicle keepers to reduce liability. These principles still underly the current version of article 18S5 WVW, which stipulates the following in paragraph 1:

> *"If a motor vehicle, which is being driven on a road is involved in a traffic accident which causes damage to persons or goods not carried by that motor vehicle [...] the owner of the motor vehicle or, if there is a keeper of the motor vehicle, the keeper is obliged to compensate that loss, unless it is plausible that the accident is due to force majeure, even where it is caused by someone for whom the owner or keeper is not liable"*[875]

The second paragraph regulates that the owner or keeper is (furthermore) liable for the behaviour of the person who is instructed or allowed by the owner or keeper to drive the vehicle. The third paragraph clarifies that the first two paragraphs do not apply to damage caused by the motor vehicle to animals running loose, to other moving motor vehicles and/or to persons or goods carried by that other motor vehicle. Article 185 concludes with the fourth paragraph, which states that its provisions are without prejudice to liability that may follow from other statutory provisions.

It follows from the wordings of article 185(1), (3) and (4) WVW, that for instance damage to persons or goods inside the damage-causing motor vehicle; damage to unleashed animals and people or goods in another moving motor vehicle, must be based on other liability rules. The most likely basis for a liability claim is in such cases article 6:162 BW, which is further illustrated in section 4.3.2.4.1.[876] In claims based on 6:162 BW, the burden of proof regarding *inter alia* the unlawful act, the attributability, the damage and the causal relationship between the act and the damage, is on the victim, while article 185 WVW reverses the burden of proof to the owner or keeper of a motor vehicle, which is illustrated in the following section.

[875] This translation is incorporated in Ernst, W. (ed.), *The Development of Traffic Liability*, Cambridge: Cambridge University Press 2010, p. 236. In footnote 6, reference is made to Van Boom 2004, p. 129 as the source of the translation. However, I (*RWdB*), have not been able to identify the text in the said source (which *does* however contain a translation of article 6:101 BW). Therefore, I cannot verify that the translation is from W.H. van Boom, and I cannot identify another source of it either. Nonetheless it is, to my best knowledge and in the absence of another (official) translation, a quite accurate translation. Should the reader be able to identify the (true) author of the translation, please report it to me.

[876] In traffic liability cases, the outcomes of the application of the norms of article 6:162 BW is rather similar to that of article 185 WVW.

4.3.2.2 Allocation of liability

Article 185 WVW is a risk liability regime.[877] It holds that the owner or keeper of a motor vehicle is by default liable towards non-motorised victims (under the aforementioned conditions), who suffered damage from a traffic accident, because of the *Betriebsgefahr* (operational risk) that motorised vehicles impose for non-motorised traffic participants.[878]

Liability is bestowed on the "owner *or* keeper" of a motor vehicle. Ownership is defined in article 5:1 BW as *the most comprehensive (property) right that an owner can have to a thing*. Someone who keeps something either for himself, or for another person, by means of *de facto* exercising power over that thing, is a *keeper* in sense of articles 3:107(4)-3:111 BW. When one rents a car for example from its owner, he is qualified as *keeper.* Article 1(2) WVW clarifies that the holder of the license plate registration is deemed owner or holder of the vehicle. "Motor vehicles" are defined in article 1 WVW as *vehicles, intended to be moved wholly or partly by mechanical force on or connected to the vehicle, or by electric traction with a power source elsewhere, although not via rails.* In practice, cars, motor cycles and mopeds thus qualify as "motor vehicles" in sense of the WVW. The notion of "traffic accident" is explained broadly: a collision between a driver and a pedestrian or cyclist is not even necessary, it is also a "traffic accident" when for instance an unexpected move by a driver frightens a non-motorized person in such way that he falls.[879] Article 185 does however only apply to accidents in which a *moving* motorized vehicle was involved, and does therefore not apply to parked cars for example.[880] It is furthermore necessary that the accident took place on a public road.[881]

> Taking into account that AVs fall under the scope of the definition of article 1 WVW, and the "technology-neutral" formulation of article 185 WVW it is highly likely that the regime is also applicable in case an AV (irrespective of the level of autonomy) gets involved in an accident with a non-motorised victim.[882] Victims can thus address a claim at the owner or keeper of the vehicle. It must be noted that only non-motorized victims can issue a claim under the WVW.

[877] See differently: Giesen 2019, p. 3, who argues (against what he indicates to be the prevailing doctrine) that the 185 WVW regime can better be qualified as "very heavy" fault liability regime, as there is a (theoretical) possibility for the owner or keeper of a motor vehicle who is sought to remunerate damage of a non-motorised victim, to invoke a *force majeure* defence.
[878] See Tjong Tjin Tai & Boesten 2016, p. 657; Hartkamp & Sieburgh 2019, no. 279, who illustrate: "Hoewel bij het regelen van deze aansprakelijkheid de wetgever mede een vermoeden van fout voor ogen heeft gehad, berust de wet toch in hoofdzaak op de gedachte dat degene die door het gebruik van een motorrijtuig de gevaren op de weg in aanzienlijke mate verhoogt, het risico daarvan behoort te dragen".
[879] Hartkamp & Sieburgh 2019, no. 276.
[880] Ibidem, no. 277.
[881] Ibidem, no, 276.
[882] See also Tjong Tjin Tai & Besten 2016, p. 658-659; Vellinga 2014, no. 5.

In most traffic accidents in which both a motor vehicle and a non-motorized accident are involved, the owner or keeper of the vehicle is liable. There is however one escape possible: liability cannot be allocated when the owner or keeper can make a plausible case for *overmacht* (*force majeure*).[883] The main rule, is that a successful *overmacht* claim is only possible, (i) if the driver could not 'legally' be blamed for his conduct, a standard of reference that allows for a comparison with the 'perfect driver'; and (ii) that the accident was (thus) solely due to another person's fault (including the victim's own fault),[884] that was so improbable that the driver could not reasonably have taken them into account whilst driving".[885] It must be noted that a successful claim on the *overmacht* defence is virtually impossible when the victim is younger than 14 years old (see further below).

Which circumstances that can be qualified as *overmacht*, have been addressed in case law. The Hoge Raad decided in 1942 that technical defects (for example: refusing brakes and a broken control rod)[886] of the vehicle do not constitute *overmacht*.[887] Also in other cases, a claim on the *overmacht* defence is seldomly awarded, however in 1996, the Hoge Raad decided that bus driver Ketelaar could rely on the defence. His bus crashed, whilst driving at low speed, with bicyclist Plomp. The Hoge Raad held that Ketelaar was not to blame at all, as he did not have to expect that bicyclist Plomp ignored the red traffic light, while crossing the street just behind another, parked, bus. Therefore Ketelaar's *overmacht* defence was justified.[888]

> Autonomous vehicles can be hacked, allowing a malevolent third party to take over control of the vehicle.[889] It is questionable whether or not hacking could constitute *overmacht*. The actual concept of *overmacht* in the WVW might suggest so, as it may be possible that it can be proven that: i) the owner or keeper took all necessary measures to update the cars' software (wherefore he cannot be blamed for the behaviour of the car); ii) that the hacker is a third party (implicating that another person is solely to blame for the accident); and iii) that the

[883] *Overmacht* as such does not have to be proven: it is sufficient that the *plausibility* of *overmacht* can be proven. See Hartkamp & Sieburgh 2019, no. 288; also: Van Dam & Van Maanen 2010, p. 150.
[884] In traffic liability cases, the *overmacht* concept is intertwined with the *own fault* concept, which is not entirely correct from a dogmatic point of view, as *overmacht* is intended as a defence in the phase of establishment of liability, while *own fault* can be used as a defence in the damage apportionment phase. That second phase is only 'reached' when the first phase results in actual allocation of liability. See furthermore section 4.3.2.3.
[885] See Hijma, J., & Olthof, M.M., "433b Aansprakelijkheid voor motorrijtuigen", *Compendium Nederlands vermogensrecht,* Deventer: Wolters Kluwer 2017/433b; Hartkamp & Sieburgh 2019, no. 283-284. See also Van Dam & Van Maanen 2010, p. 138, 139. The refer to Hoge Raad 22 May 1922, *NJ* 1992/527 (ABP/Winterthur); and furthermore *inter* alia to Hoge Raad 24 December 1982, *NJ* 1983/443, *Verkeersrecht*1983/40 (Wijman/Corten); Hoge Raad 23 May 1986 *NJ*1987/482 (Frank van Holsteijn).
[886] These examples are given in Hartkamp & Sieburgh 2019, no. 282.
[887] Hoge Raad 16 april 1942, *NJ*1942/394 (Torenbout).
[888] Hoge Raad 16 February 1996, *NJ* 1996/343, *Verkeersrecht* 1996/195, and the elaboration by Van Dam & van Maanen 2010, p. 139. See also Engelhard, E.F.D. & Van Maanen, G.E., *Aansprakelijkheid voor verkeersongevallen*, Nijmegen 1998, p. 18.
[889] See for instance section 4.2.2.

> specific vulnerability in the software was unknown at the time the hacking took place (in order to underpin the "improbability" of the accident.[890]

The criteria for *overmacht* are even stricter when it concerns young non-motorised victims. The Hoge Raad held that *overmacht* cannot be successfully invoked when the victim is under 14 years old, *unless* the child acted intentionally (*opzet*), or with recklessness approaching intent/wilful recklessness (*aan opzet grenzende roekeloosheid*),[891] even when the behaviour of the child significantly contributed to the accident.[892] Again unless the existence of *opzet* and *aan opzet grenzende roekeloosheid*, faults of the victim cannot be attributed to a child under fourteen as *own-fault* (contributory negligence) under article 6:101 BW.[893] This entails that in practice, the *overmacht*-defence cannot be successfully relied on in cases were the non-motorised victim is under fourteen years of age,[894] and that contributory negligence of the victim can in principle not lead to a reduction of the amount of damages to be remunerated. Taken together, this is referred to as the *100%-rule,*[895] since this means that the owner/keeper is 100% liable. The 100%-rule does not apply to other categories of vulnerable non-motorised traffic participants.[896] However, there is another rule which has been developed in case law, the *50%-rule*, according to which liable owners or keepers (who cannot prove *overmacht*) have to remunerate at least 50% of the damage suffered by the victim, even if there was contributory negligence at the side of the victim. As the 50%-rule technically relates to *contributory negligence* (which plays a role in determining the legal causation and the apportionment of damages to be remunerated),[897] and not to *overmacht* (which relates to factual causation, and the establishment of liability), the 50%-rule is further elaborated in the next section.

> Also in AV-related traffic accidents, an owner or keeper could try to invoke the *overmacht* defence. Tjong Tjin Tai & Boesten have posed the question whether the defence may have to be extended or limited regarding AV-accidents. I share their observation that the scope of the defence should rather be limited further than extended, as AVs are (at least potentially) better equipped to detect dangerous situations and to prevent accidents than human drivers can.[898]

---

[890] See also Lavrijssen & Weitering 2019, who reach the same conclusion that the *overmacht* defence can in principle be relied on, when the criteria that apply to 'human' drivers are fulfilled (p. 4).
[891] Hoge Raad 31 mei 1991, *NJ*1991/721 (Marbeth van Uitregt).
[892] Hoge Raad 2 June 1995, *NJ*1997/700 (Marloes de Vos).
[893] Hoge Raad 1 June 1990, *NJ* 1991/720 (Ingrid Kolkman).
[894] See also: Hartkamp & Sieburgh 2019, no. 285; Van Dam & Van Maanen 2010, p. 139.
[895] Ibidem.
[896] Hoge Raad 28 February 1992, *NJ*1993/566 (IZA/Vrerink).
[897] See for more on legal and factual causation section 4.2.3.4.
[898] Tjong Tjin Tai & Boesten 2016, p. 659. See somewhat differently Lavrijssen & Weitering 2019 (p. 4), who consider that the criteria are already very strict, and that raising the bar for AVs would require legislative action.

For instance radar, lidar, camera and infrared technology contribute to that potential of better-than-human perception of (non-motorised) danger. In theory, AV-technology could (and should) result in less situations that are "so improbable that the driver could not reasonably have taken them into account whilst driving", i.e. the condition that could trigger applicability of the *overmacht* defence.

4.3.2.3 Damage apportionment

When *overmacht* is not proven, and an owner or keeper of a motor vehicle is held liable towards a victim, in principle damages of the victim (that is: any of those remunerable under Dutch Law),[899] which can be reasonably attributed to tortfeasor as a consequence of the accident for which he is liable, must be compensated.[900] There are however some exceptions to that rule. In cases based on an article 185 WVW claim, the most likely defence that can be brought up against the victim is *contributory negligence*, addressed in article 6:101 BW. The first paragraph holds the following:

> *When the damage is caused as well by circumstances which are attributable to the injured person himself, then the obligation to compensate damages is reduced by imputing the total damage to the injured person and to the liable person in proportion to the degree in which the circumstances which have contributed to the damage can be attributed to them individually, on the understanding that another imputation occurs or the obligation to compensate damages extinguishes or stays in force totally, if this is required by fairness in view of the significance of the various faults or of other circumstances in the prevailing situation.*[901]

The *contributory negligence* defence consists of two steps:[902] first, it must be established to what extent the circumstances that can be attributed to the claimant and the defendant respectively, contributed to the damage. Then, this "causal apportionment" can be adjusted, insofar as principles of fairness require so.

---

[899] There are no limitations as to the types of damages that may qualify for remuneration (which is thus different from for example the product liability regime, where some types of damage are explicitly excluded). See section 4.2.3.3 for some general observations concerning types of damage that may be remunerable under the laws of The Netherlands, and furthermore Section 6.1.10 of the BW.
[900] See article 6:98 BW. Giesen 2019, p. 4-5 illustrates that the burden of proof regarding the causal relationship between the traffic accident and the damage can be reversed, based on case law of the Hoge Raad (including Hoge Raad 16 November 1991, *NJ* 1991, 55 (*Kinderbescherming/Engelen*); and Hoge Raad 24 December 1999, *NJ* 2000/428 (*Gouda/Lutz*).
[901] See for the source of this non-official translation of article 6:106 BW: http://www.dutchcivillaw.com/legislation/dcctitle6611bb.htm (last accessed 5 February 2020).
[902] Van Boom 2004 however distinguishes three steps (p. 134): "(1) imputable occurrence, (2) primary apportionment, and (3) equitable adjustment", although in most case law and also by for example Van Dam & Van Maanen, a two-step-test is used. In a similar vein: Hartlief, T., "Aansprakelijkheid voor motorrijtuigen", in Spier, J. et al., *Verbintenissen uit de wet en Schadevergoeding*", Deventer: Kluwer 2000, p. 146.

In the causal apportionment-phase, both the "factual" degrees of contribution to the damage of both claimant and defendant, and *Betriebsgefahr* play a role. The inherent risk that a motor vehicle poses (in terms of weight and speed of the vehicle) to non-motorized victims, is always observed to form a significant factor in the causation of the damage.[903]

It follows from case law that principles of fairness require that the owner or keeper of the vehicle always has to remunerate a minimum of 50% of the victim's damages, even when the victim's own contribution to the origination of the accident amounted to more than 50%,[904] *unless* there was intent or wilful recklessness from the side of the victim.[905] For the "other" 50%, it must be established a) to what extent the circumstances can be factually attributed to the victim (above the first 50%); and b) it would be fair to attribute these circumstances to the victim.[906]

> When an AV collides with two bicyclists, a 13 year old boy and a 45 year old woman, who did not have appropriate lighting on their bicycles whilst riding the dark, the following may apply. Liability will be allocated to the owner or keeper of the AV, as the cyclists' failure of attaching appropriate lighting equipment to their bikes will likely not constitute *overmacht*, as this is not regarded as a situation "so improbable that the driver could not reasonably have taken them into account whilst driving". Furthermore, it follows from the *100%-rule*, that *overmacht* cannot be invoked towards the 13 year old victim even when the behaviour of the child significantly contributed to the accident (which could be the case here), unless intent or wilful recklessness can be proven (not likely in this case).
>
> The fact that the bicyclists were not equipped with appropriate lighting may constitute *contributory negligence* regarding the 45 year old victim. However at least 50% of her damage will still have to remunerated by the AV owner or keeper. Should it be established that the absence of appropriate lighting contributed for 70% to the accident, the victim should bear (70% - 50%=) 20% of her own damages, *unless* that would be deemed unfair. It follows again from the *100%-rule* that, despite factual "contributory negligence" regarding the cause of the accident by the respective victims, principles of fairness require that 100% of the damage suffered by the 13 year old victim have to be remunerated by the AV's owner or keeper.

[903] See Tjong Tjin Tai & Boesten 2016, p. 657; Van Dam & Van Maanen 2010, p. 142
[904] See Van Boom 2004, p. 142; Van Dam & Van Maanen 2010, p. 143-144; Hartkamp & Sieburgh 2019, nrs. 285-286; and Hoge Raad IZA/Vrerink; and Hoge Raad 24 December 1993, *NJ* 1995/236 (Anja Kellenaers).
[905] See for example Hoge Raad 30 maart 2007, *NJ* 2008/64. The Hoge Raad held that a drunk pedestrian, who was wearing dark clothes, and walked in a motor-traffic lane acted with recklessness approaching intent, as he must have known that his behaviour led to severe chances of an accident. Note again that there is a special "100%-regime" regime for children under 14, as elaborated in section 4.3.2.
[906] See Hartkamp & Sieburgh 2019, no. 286.

4.3.2.4 Other sources of traffic liability allocation

As stated in section 4.3.2.1, article 185 WVW only applies in cases of traffic accidents between a motorized vehicle, and a non-motorized victim. When the motor vehicle caused for instance damage to persons or goods inside the damage-causing motor vehicle; or to unleashed animals and people or goods in another moving motor vehicle, a claim for damages must be based on other liability rules. Such claims can be based on the general "unlawful act" (*onrechtmatige daad*) rule of article 6:162 BW, which is elaborated in section 4.3.2.4.1. Under some circumstances, itis also possible to base a claim on the risk-liability regime of article 6:173 BW that applies to defective movable goods, which is elaborated in section 4.3.2.4.2, which can in some cases be applicable when the product liability regime does not apply.

4.3.2.4.1 Unlawful act, article 6:162 BW

Article 6:162(1) BW states that:

> "*One who commits an unlawful act against another person, which can be attributed to him, is obliged to remunerate the damage that the other person suffered as a result thereof.*"[907]

Section 2 explains that an *unlawful act* can consist of:

> "*a violation of someone else's right, and an act or omission in violation of a legal obligation or in violation of what is appropriate in society under unwritten law, insofar as there is no justification for that behaviour*".[908]

Article 6:162(3) concludes with a rule regarding *attributability* of an *unlawful act*:

> "*An unlawful act can be attributed to a tortfeasor, when it can be imputed to him as his fault, or when he can be held accountable for its cause by virtue of law or generally accepted opinions*".[909]

Regarding road traffic accidents, the victim thus has to prove that an *unlawful act* was committed. That may for example consist of the violation of a statutory rule, such as a specific rule of traffic law.[910] Furthermore, a violation of the right to bodily integrity of the victim,[911] and 'careless'

[907] My own translation. See for another (non-official) translation: http://www.dutchcivillaw.com/civilcodebook066.htm (last accessed on 6 May 2020).
[908] Ibidem.
[909] Ibidem.
[910] See Van Dam & Van Maanen 2010, p. 141; Van Wijk 2014, p. 55, indicating that a violation of article 6 WVW (regarding attributable *fault* resulting in serious personal injury; see further below fn. 916). constitutes violation of a legal obligation. Violation of article 5 (general prohibition to behave as such that it causes "danger" or "hindrance" on the road) or 5a (which lists more specific prohibited conducts) can also qualify as such.
[911] Ibidem.

driving contrary to "what is appropriate in society",[912] can also constitute an *unlawful act*. In traffic liability cases, most claims are based on 'societal carelessness' (*maatschappelijke onzorgvuldigheid*, i.e. contrary to what is appropriate in society).[913] It follows from case law, that a high standard of care applies, and that failure to behave in accordance with that standard of care, constitutes societal carelessness.[914] That standard of care entails *inter alia* that drivers have to take possible faults of other traffic participants into account, unless such faults were so improbable that the driver could not reasonably have taken them into account.[915] This standard of care reflects the *overmacht* criterion of 185 WVW.

Attribution can be based on either fault (*schuld*) of a driver, or on a cause for which he is accountable, by virtue of statutory provisions, or by virtue of common opinion in society. The *schuld* criterion in traffic accidents is *inter alia* incorporated in article 6 WVW. This provision holds that it is prohibited for traffic participants to behave in such a way that traffic accidents occur due to their fault (*schuld*), causing death, serious injuries or injuries leading to illness or hinder a victim to perform his normal activities.[916] It follows from case law of the Hoge Raad, that the mere violation of a traffic rule is not enough to establish *schuld* in such cases. Factors including the behaviour of the (suspected) norm-violator, the nature of his behaviour, the seriousness of the violation and/or all other circumstances must be taken in to account.[917] Driving in the wrong lane;[918] opening the doors of a parked vehicle without taking due notice of the other traffic;[919] and colliding with a traffic participant in the blind spot of a vehicle,[920] all constitute fault. A relatively mild violation of the maximum speed by 7 km/hour is not "sufficiently" severe to bring about

[912] See Tjong Tjin Tai & Boesten 2016, p. 657. When principles (rather than concrete rules) of traffic law are violated, this might constitute careless behaviour which is not appropriate in society. See also Van Wijk 2014, p. 55.
[913] See Giesen 2019, p. 3-4.
[914] *Inter alia*: Hoge Raad 15 January 1993, *NJ* 1993, 568 (*Puts/Ceha*); HR 14 July 2000, C99/128HR, (X/Haagsche Tramweg Maatschappij); as cited in Giesen 2019, p. 4; also Tjong Tjin Tai & Boesten 2016, p. 658.
[915] See for instance HR X/Haagsche Tramweg Maatschappij, no. 4.1.
[916] My paraphrasing and translation of the provision: "Het is een ieder die aan het verkeer deelneemt verboden zich zodanig te gedragen dat een aan zijn schuld te wijten verkeersongeval plaatsvindt waardoor een ander wordt gedood of waardoor een ander zwaar lichamelijk letsel wordt toegebracht of zodanig lichamelijk letsel dat daaruit tijdelijke ziekte of verhindering in de uitoefening van de normale bezigheden ontstaat.".
[917] Hoge Raad 1 June 2004, *NJ* 2005, 252, annotated by Knigge, *VR* 2005, annotated by Simmelink, and elaborated by Van Wijk 2014, p. 40-50. Although in this case a criminal liability claim was made, the Hoge Raad decision is also relevant for civil liability in sense of article 6:162 BW jo. 6 WVW, as Van Wijk indicates at p. 40.
[918] Ibidem HR 1 June 2004.
[919] Hoge Raad 21 October 2003, *VR* 2003, 36; Rechtbank (court of first instance) 's-Gravenhage 6 august 2004, LJN AQ6513 (cited by Van Wijk 2014, fn. 91).
[920] Hoge Raad 17 January 2006, *NJ* 2006, 3030, annotated by Buruma (cited by Van Wijk 2014, fn. 92).

schuld ,[921] without other relevant circumstances such as road- and weather conditions and the drivers' consumption of alcohol.[922]

The standard of attributability is in traffic liability cases generally rather low.[923] This follows from case law of the Hoge Raad, who held that in traffic liability cases human blameworthiness (*menselijk verwijtbaar*) is not necessary, and that legal blameworthiness (*rechtens verwijtbaar*) suffices.[924] In the *Meppelse ree*-case,[925] a deer suddenly turned up in front of a car. The driver swerved around it, onto the other lane, and into traffic – with a collision with another car as a consequence. Both the driver and the two passengers of that other car, as well as the wrongdoer, were killed in the accident. The Hoge Raad decided that the reaction of the driver was legally blameworthy (rather than humanly blameworthy), as he should have chosen another, less dangerous reaction, such as a swerve into the other side of the road, or a collision with the deer, although the reaction of the driver was considered to be understandable and perhaps even unavoidable. When assessing whether or not the damage-causing behaviour of a driver is legally blameworthy, the standard is set by what can be expected from a "perfect driver". As Van Dam & Van Maanen put it: "This is not a normal objective standard, but rather one of a 'perfect driver' who knows and foresees almost everything and is able to avoid almost all possible risks: it is the robot type of comparison".[926]

> The regime of article 6:162 BW may also be applied to traffic accidents involving AVs. However, the autonomous nature of AVs could entail difficulties for victims, which also illustrates possible flaws in the current system of article 6:162 BW. Where human drivers gradually release their reins as autonomy in AVs increases, eventually leading to SAE level 5 where no human control over the vehicle remains, it will be harder to establish unlawful *conduct* of AV drivers. Then, the *de facto* norm violators will be the vehicles themselves, rather than their 'drivers'.[927] From a more theoretical than practical perspective, as not many accidents with AVs have occurred yet, and even less have been taken to court, norm violation could however be attributable to AV-'drivers' (or other entities such as owners) due to their blameworthy

[921] Rechtbank 's-Granvenhage 12 November 2004, *VR* 2005, 69 (cited by Van Wijk 2014, fn. 95.
[922] See Van Wijk 204, p. 45-46.
[923] See Tjong Tjin Tai & Boesten 2016, p. 658; Van Dam & Van Maanen 2020, p. 141-142; Van Dam, C.C., "De Hoge Raad op zoek naar de perfekte automobilist. Drie recente arresten", *VR*, 1985, p. 261-264.
[924] See Hoge Raad 11 November 1983, *NJ* 1984, 331, *VR*, 1984, 56 (*Meppelse ree*), as elaborated in Van Dam & Van Maanen 2010, p. 141-142; Van Wijk 2014, p. 85-88. See also Hoge Raad 26 March 1982, ECLI:NL:HR:1982:AG4351, *NJ*1982, 292 (*Wenmaker/Smeets*), in which case it was decided that the same (high) level of care must be observed between drivers and passengers; see Van Dam & Van Maanen 2010, p. 142; Tjong Tjin Tai & Boesten 2016, p. 658.
[925] Ibidem.
[926] Van Dam & Van Maanen 2020, p. 242.
[927] See De Vey Mestdagh & Lubbers 2015, p. 274; also Vellinga 2014, no. 7.

omissions,[928] which is attributable by virtue of common opinion in society. Tjong Tjin Tai & Boesten indicate two possible categories of such omissions attributable to a driver (or owner): 1) wrongfully allowing an AV to be set in motion without taking due (safety) measures; and 2) wrongfully not taking (back) control of an AV where he could, and should have done so.[929] It must be noted that the second category only applies to AVs that can be categorized as SAE-levels 0-4, and cannot be applied to fully autonomous (level 5) vehicles. For non-fully autonomous vehicles, it can be held *unlawful* and *attributable* when a driver does nothing upon a request of the system to take back the steering wheel – to the extent possible for a driver to do so.[930] That could however also be the case when a driver takes over control, or intervenes in the automatic decisions of an AV which causes an accident (that would not have occurred when no human intervention was made). It can furthermore be an *attributable unlawful act* when an AV is allowed on the road when this was actually inappropriate. That could be the case for instance when a vehicle was not properly mechanically maintained; when a critical safety update had not been installed (perhaps even allowing a hacker to take over control of the vehicle); when a driver has been tempering with the soft- or hardware;[931] or when an AV is driven in dangerous conditions, such as extreme weather or in dense crowds.[932] It must be noted, that it will require extensive data-analysis (to be carried out by a claimant) to establish whether or not the AV – and therefore the driver or owner – was at fault. For *category 1* accidents it must for instance be proven that a) a request was directed at the driver to reclaim control of the vehicle; b) that such request was neglected; while c) it had been possible for a driver to successfully do so. In *category 2* accidents, it can only be proven after thorough data analysis that for instance a certain software-update was missed, or that the soft- and/or hardware was altered by (or under responsibility of) the defendant, or that the AV was in any other way 'unfit' to be driven.

The general principle is that a victim who seeks remuneration on the basis of a 6:162 BW-claim, has to prove (*inter alia*) a causal relationship between an unlawful act and damage. However, the Hoge Raad developed a rule which reverses the burden of proof in cases where unlawful

[928] See De Vey Mestdagh & Lubbers 2015, p. 273-274, referring *inter alia* to Van Wees, K.A.P.C., "Over intelligente voertuigen, slimme wegen en aansprakelijkheid", *VR* 2010, no. 2, pp. 33-44; and Tjong Tjin Tai & Boesten 2016, p. 659-660.
[929] "1) de bestuurder had niet de zelfrijdende auto in gang mogen zetten, althans niet zonder nadere maatregelen, die hij achterwege heeft gelaten; 2) de bestuurder heeft in de concrete situatie nagelaten in te grijpen terwijl hij dat wel kon en moest doen", Tjong Tjin Tai & Boesten 2016, p. 659. This seems to be in line with the findings and recommendations in European Commission 2020, p. 54.
[930] Ibidem.
[931] De Vey Mestdagh & Lubbers 2015, p. 274
[932] Tjong Tjin Tai & Boesten 2016, p. 660.

behaviour results in increased danger. When such increased danger manifests and results in damage, the causal relationship is deemed to be established, unless the opposite is proven by the tortfeasor.[933] Over the years, this rule has been further developed and nuanced by the Hoge Raad.[934] Currently, judges may presume a causal relationship between a norm violation and damage, in cases where one behaves contrary to a norm which sees to the prevention of a specific damage-inflicting danger, and where that specific danger has in fact materialised. The presumption of causation is rebuttable by the defendant, who may refute (*ontzenuwen*) the assumption. Mere invalidation of the causal relationship (*tegenbewijs*) suffices proof of the opposite (*tegendeelbewijs*) is not (longer) necessary. The burden of proof remains with the victim, who is however aided by the respective presumption of causation.[935]

This *omkeringsregel* was for instance applied in a case where a bicyclist neglected the prohibition to drive in the wrong cycling lane and crashed onto another bicyclist;[936] in a case where a moped driver drank too much alcohol, contrary to the specific rule on allowed blood alcohol levels;[937] and in a case where a driver failed to adapt, in conformity with the norms, his speed to match the actual circumstances on the road.[938]

Regarding damage apportionment and defences, generally the same rules apply as to article 185 WVW, which have been illustrated in section 4.3.2.3. Also where a justification for the unlawful act can be established, [939] such as self-defence, an emergency, the execution of a legal requirement or the execution of a duly issued official order.[940]

Thus, in traffic accident cases where article 185 WVW does not apply, a liability claim can be based on article 6:162 BW. Although it will be (at least in theory) less 'easy' for a victim to be awarded damages than under article 185 WVW, since he has to prove *inter alia* unlawfulness, attributability, damage and causation, there are ample rules that can aid a claimant. The standard of care that has to be taken into account by drivers is very high, 'legal blameworthiness' will suffice, and where a specific traffic rule has been violated, it is often enough to establish that

[933] See HR *Kinderbescherming/Engelen* and *Gouda/Lutz* (fn. 900 supra), as elaborated in Giesen 2019, p. 5-6.
[934] As cited by Giesen 2019, p. 5: Hoge Raad 26 January 1996, *NJ* 1996, 607 (*Dicky Trading II*); Hoge Raad 16 June 2000, *NJ* 2000, 248 (*Sint Willibrord/V*); Hoge Raad 5 June 2009*, NJ* 2009, 257 (*X/AXA*).
[935] See Giesen 2019, p. 5; Van Wijk 2014, p. 99-111.
[936] Hoge Raad *Gouda/Lutz* (fn. 900 supra).
[937] Hoge Raad 24 December 2005, *NJ* 2005, 284 (*Aydin/Wintherthur*).
[938] Hoge Raad 24 September 2004, *NJ* 2005, 466 (*Stad Rotterdam/Groene Land*). These three examples are illustrated in Giesen 2019, p. 5-6.
[939] See furthermore the 'relativity defence' article 6:163 BW; as explained by Van Maanen, G.E. & Lindenbergh, S.D., in Hartlief et al., *Verbintenissen uit de wet en Schadevergoeding*, Deventer: Wolters Kluwer 2018, p. 27-28.
[940] 6:162(2) BW. See furthermore Van Maanen, G.E. & Lindenbergh, S.D., in Hartlief et al., *Verbintenissen uit de wet en Schadevergoeding*, Deventer: Wolters Kluwer 2018, p. 59-76

violation, after which the causal relationship between that violation and the damage will be presumed.

4.3.2.4.2 Liability of possessors of defective movable goods: 6:173 BW

Besides article 185 WVW or 6:162 BW, victims of road traffic accidents may, since 2005,[941] direct a claim against the possessor (often the owner)[942] of a vehicle on the basis of article 6:173 BW. 6:173 BW is seldomly used in 'traditional' traffic liability cases,[943] although that might change when vehicles become more autonomous.[944] Article 6:173 (1) BW regulates strict liability for defective movable goods, as follows:[945]

> *The possessor of a movable good of which it is known that it presents a special hazard to people or goods when it does not comply with the requirements that one may have regarding that movable good, taking account of the given circumstances, is liable when such hazard realizes, unless liability ex art. 6:162-168 BW would not have existed if he would have known the danger at the time it occurred.*

One is thus liable for goods he possesses which are "defective". Goods can be held defective, if these are "intrinsically defective", or have "abnormal characteristics" or have "properties which such goods ought not to have".[946] Regarding vehicles, it might be expected that these comply with all safety standards.[947] If for instance the brakes do not function properly, a vehicle can be defective in the sense of article 6:173 BW. It is furthermore necessary that the movable good in question poses a *specific danger* to people or goods. A general danger, which is inherent in virtually any good (for instance when something is thrown from a ten-story building), is not sufficient. A specific danger is for example posed by a beer bottle, which explodes or fractures upon opening.[948] Regarding AVs, a specific danger will exist when the steering software can crash while the vehicle is in action, rendering the AV uncontrollable. It is not necessary that the respective defect was subjectively known by the possessor at the time of its manifestation. General, objective knowledge is to be assessed. Such general, objective knowledge exists for

---

[941] See Bauw 2015, nr. 10; Tjong Tjin Tai & Boesten 2016, p. 657; Van Dam & Van Maanen 2010, p. 142-143.
[942] See article 3:119 BW.
[943] Searching the register of published cases on www.rechtspraak.nl with the keywords "6:173 BW, ongeval (*accident*), verkeer (*traffic*), returned on 12 May 2020 only 1 relevant case: Rechtbank Rotterdam 25 April 2014, ECLI:NL:RBROT:2014:3097 in which it was held that a tractor that lost its trailer was defective in sense of 6:173 BW.
[944] See for instance Tjong Tjin Tai & Boesten 2016, p. 661-664; De Vey Mestdagh & Lubbers 2015, p. 274.
[945] My translation, see for another, unofficial, translation: http://dutchcivillaw.com/civilcodebook066.htm (last accessed 11 May 2020).
[946] See Keirse 2018, p. 103, and her references in footnote 69.
[947] See De Vey Mestdagh & Lubbers 2015, p. 274.
[948] Keirse 2018, p. 104.

example when one has, or ought to have, knowledge of the fact that a car with defective brakes should not be driven (rather than that one has knowledge that the brakes of a specific car were unreliable). Unknown, general risks – or risks that could not reasonably be known by the possessor, do not have to be taken into account. Keirse illustrates this as follows: should it become known in the future that mobile phones may have a bad influence on the health of certain people, those people cannot claim damages on the basis of 6:173 BW, as this defect could not have reasonably known at the time such phones were used in the past.[949]

A claim based on 6:173 BW cannot successfully be invoked insofar "liability ex art. 6:162-168 BW would not have existed if he would have known the danger at the time it occurred". This entails that when liability could not be established on the basis of article 6:162 and following, article 6:173 does not apply.[950] Contrarily, the applicability of article 6:173 BW is limited to those cases in which one would be liable on the basis of article 6:162 BW *should* one have had knowledge of the defect in question, and should one have had time and opportunity to prevent the hazard from causing damage.[951] Case law implicates another limitation of the applicability of article 6:173 BW. It follows from the Hoge Raad-decisions in the matters *Wilnis,*[952] and *Paalrot*,[953] that when a possessor of a defective good (or in those cases: a structure) could not have had objective knowledge of the respective hazard, a defect in sense of article 6:173 (or, as in those cases 6:174) BW cannot as such be construed.[954]

The generic defences that are incorporated in articles 6:162-168 BW may furthermore limit or prevent liability in the sense of 6:173 BW.[955] More concretely, defences such as *force majeure*, *relativity* and the *existence of a justification ground*[956] can be invoked by the defendant. Besides the generic defences, article 6:173(2) BW stipulates a specific defence. When a movable good is a *defective product* in sense of article 6:185 BW (which implements the PLD, see section 4.2.3), its possessor cannot be held liable under article 6:173 BW, unless the damage is "property damage" below the threshold of €500,-,[957] or when it is likely that the defect came into existence after it had been entered into circulation.[958] Thus, liability is "channelled" towards the producer, if the product is defective (when damages amount more than the threshold, and when the defect existed

[949] Keirse 2018, p. 105-106 – my paraphrasing.
[950] See Sieburgh 2019, no. 223.
[951] Ibidem, no. 225; Oldenhuis, F.T., "5.13 De 'tenzij-formulie' in art 6:173 BW", in: Stolker, C.J.J.M. (ed.), *Groene Serie Onrechtmatige Daad*, Deventer: Wolters Kluwer 2020 (online edition), no. 5.13.
[952] Hoge Raad 17 December 2010, ECLI:NL:HR:2010:BN6236 (*Wilnis*), no. 4.4.6.
[953] Hoge Raad, 30 November 2012, ECLI:NL:HR:2012: BX7487 (*Paalrot*), no. 4.4.
[954] Ibidem Oldenhuis, no. 5.13.2; see also the *Wilnis*-case note by Hollander, P.W. den, "Hoe gebrekkig is een verschoven veendijk"?, *AV&S* 2011, no. 10.
[955] Keirse 2018, p. 106.
[956] See section 4.3.2.4.1.
[957] Article 6:173(2)(b) jo. 6:185 jo 6:190(1)(b) BW.
[958] Article 6:173(2)(a) BW.

when it was put into circulation by the producer). When the producer is able to invoke a defence (such as the development risk defence, see section 4.2.2.8.6), the victim cannot seek remuneration from the possessor under 6:173 BW.[959]

Furthermore, regarding the apportionment of damages, it must be noted that the regime of article 6:98 and 6:101 BW also applies in cases based on 6:173 BW.[960]

In academic literature, there is discussion concerning the level of safety that might be expected from AVs.[961] Schreuder,[962] and Van Wees,[963] argue that the safety level in the sense of 6:173 BW can be compared to the (rather low) safety level under the PLD implementation in article 6:185 ff. BW. Thus, the objective "reasonable expectations of the public at a large",[964] including "the intended purpose, the objective characteristics and properties of the product […] and the specific requirements of the group of users for whom the product is intended"[965] would therefore have to be taken into account. De Vey Mestdagh & Lubbers indicate that the safety expectations regarding AVs are high (higher than the norm incorporated under 6:185), and that when AVs indeed are safer than non-AVs, the expectations may be in conformity with the actual (higher) safety levels.[966] Taking notice of the fact that AVs can act themselves, and the *Betriebsgefahr* that will still exist in AVs, Tjong Tjin Tai & Boesten argue that a very high level of safety expectations should be applied.[967] The safety standard should relate to what may be expected from a human driver. As elaborated in sections 4.3.2.1 and 4.3.2.4.1, the expectations regarding human drivers are already high. In my opinion, the bar should be set at least at the level of safety that what can be expected of the best human driver.

In damage claims based on 6:173 BW, the onus of proof regarding defectiveness is on the victims. A possessor of an allegedly defective movable good, may defend himself by stating (and proving) that liability would not have existed on the basis of article 6:162 ff BW (for instance by stating that the defect could not have been discovered on the basis of objective knowledge), or that for instance the *overmacht* defence applies. Furthermore, victims will have to establish that

[959] See Sieburg 2019, no. 228; Keirse 2018, p. 106.
[960] See *inter alia* supra section 4.3.2.3, footnote 899, and section 4.2.4.3.
[961] See for instance De Vey Mestdagh 2015, p. 274; Tjong Tjin Tai & Boesten 2016, p. 661-662; Schreuder 2014, no. 2.2; Van Wees 2015, no. 4.4.
[962] Schreuder 2014, no. 2.2., referring to Bauw 2008, p. 15.
[963] Van Wees 2015, np. 4.4., also referring to Bauw 2008, p. 15.
[964] CJEU 5 March 2015, joined cases C-503/14 and C-504/14 (Boston Scientific Medizintechnik GMBH), para. 37; see furthermore section 4.2.2.3
[965] CJEU Boston Scientific Medizintechnik GMBH, para. 38.
[966] De Vey Mestdagh & Lubber 2015, p. 274.
[967] Tjong Tjin Tai & Boesten 2016, p. 661-662.

a defect did not exist at the time a vehicle was put on the market by its producer.[968] It is indicated that this could seriously hinder victims in effectuating liability claims against possessors,[969] as victims will be required to indicate when a certain defect came into existence, which cannot be done without extensive technical analysis of the vehicle at hand.

4.3.3 FRANCE

4.3.3.1 Introduction and purpose

In France, rules regarding damage compensation of victims of road traffic accidents evolved in the 20th century. Along with the increasing appearance of cars on the French roads during the first two decades of that century, the general rule of article 1240 CC,[970] regarding *fault*-liability was soon considered to be "too restrictive in comparison to what fairness seemed to require in terms of compensation for victims – especially non-drivers",[971] as it was often impossible for victims to prove that the driver was at fault, leaving victims empty-handed. It was observed that "automobiles created a specific and serious risk of accidents, which, as a matter of principle, should be borne by those who chose to run this risk by using these machines".[972] A solution to this problem was found in case law, by applying the rules regarding *responsabilité du fait des choses* (responsibility for things into one's keeping) to motor vehicle accidents.[973] In the Jand'heur decision of the *Cour de Cassation*, it was held that keepers of cars are strictly liable, whether the car was driven or not at the time of the accident, irrespective of their defectiveness and irrespective of these cars being particularly dangerous.[974] Furthermore, it was held that "liability could not be lifted except by proof of an external, unforeseeable and unstoppable cause".[975] The fact that defences such as *force majeure, cause étrangère*,[976] and *contributory negligence* could

[968] See Keirse 2018, p. 109; Tjong Tjin Tai & Boesten 2016, p. 663.
[969] In general terms: Keirse 2018, p. 109; Regarding AVs: Tjong Tjin Tai & Boesten 2016, p. 633; Van Wees 2015, no. 4.4.
[970] This was article 1382 CC *before* the reform of 2016, see supra fn. 687.
[971] Borghetti 2018, p. 267; Viney & Guégan-Lécuyer 2010, p. 50, 61.
[972] Borhgetti 2018, p. 267 and his reference to Viney, G., Jourdain, P., & Carval, S., *Les régimes spéciaux et l'assurance de responsabilité*, Paris: LGDJ 2017, p. 79.
[973] See Viney & Guégan-Lécuyer 2010, p. 52; 60-67; Borghetti 2018, p. 268-269. The relevant provision of art. 1242 (formerly art. 1384) CC reads in official translation: "One is liable not only for the harm which one causes by one's own action, but also for that which is caused by the action of persons for whom one is responsible, or of things which one has in one's keeping". For these sections, I have used the English translation of the provisions in the CC which is made by J. Cartwright, J., Fauvarque-Cosson, B., and Whittaker, S., commissioned by the *Direction des affaires civiles et du sceau, Ministère de la Justice, République française*. It is available online, via http://www.textes.justice.gouv.fr/art_pix/THE-LAW-OF-CONTRACT-2-5-16.pdf (last accessed 11 March 2020).
[974] Cour de Cassation, ch. Réunies, 13 February 1930, DP 1930, I, 57, as cited in Borghetti 2018, p. 270.
[975] Ibidem, as cited in Viney & Guégan-Lécuyer 2010, p. 61.
[976] Cause étrangère was successfully invoked in cases of "ice or a patch of oil on the road, game animals crossing the road or a storm" (Viney & Guégan-Lécuyer 2010, p. 64).

however easily be invoked, led to dissatisfaction among victims and in society as a whole.[977] In academia, an alternative to the existing rules was proposed by prof. André Tunc, which was endorsed in case law,[978] and eventually by minister of justice Robert Badinter, which in turn led to the adoption in 1985 of the *Loi 85-677 du 5 juillet 1985 tendant à l'amélioration des victims d'accidents de la circulation et à l'acceleration des procedures d'indemnisation* (*Loi Badinter*).[979]

4.3.3.2 Allocation of liability: Loi Badinter

Victims of road traffic accidents in which a motor vehicle (trains and trams which run on their own tracks excepted) is involved can base a liability claim on the provisions of the *Loi Badinter*, even when those victims were transported by virtue of a contract,[980] as long as the damage was not intentionally caused.[981] Motor vehicles are not defined in the *Loi Badinter*, although it is held that the definition of the French insurance code (*code des assurances*) applies here, which defines motor vehicles in line with the MVID as "any motor vehicle intended for travel on land and propelled by mechanical power, but not running on rails and any trailer, whether or not coupled".[982] Road traffic accidents are not defined either, but "any unforeseen and potentially harmful event arising in connection with the circulation of motor vehicles" can be seen as such.[983]

The very strict nature of the liability regime is expressed *inter alia* by the absence of the regular causality requirement; for allocation of liability, involvement (*implication*) of a motor vehicle suffices.[984] The notion of *involvement* has been developed in case law. Involvement occurs anytime a motor vehicle "intervenes" in a traffic accident.[985] It is not required that there has been any

[977] Borghetti 2018, p. 271. Viney & Guégan-Lécuyer 2010 furthermore point out that the obligatory insurance and a *Fonds de garantie*, which were installed to guarantee remuneration of victims, also of insolvent tortfeasors, were seen to be inadequate, as it was possible to exclude family members of victims from remuneration (p. 63-64).
[978] The *Cour de Cassation* held in its *Desmare* decision that contributory negligence could no longer be successfully invoked by a defendant, unless that constituted *force majeure*. Cass. Civ. (2) 21 July 1982, D. 1982, 449, concl. Charbonnier, note C. Larroumet; JCP 1982, II, 19861, note F. Chabas, as cited in Viney & Guégan-Lécuyer 2010, p. 66.
[979] Ibidem.
[980] Article 1 *Loi Badinter:* Les dispositions du présent chapitre s'appliquent, même lorsqu'elles sont transportées en vertu d'un contrat, aux victimes d'un accident de la circulation dans lequel est impliqué un véhicule terrestre à moteur ainsi que ses remorques ou semi-remorques, à l'exception des chemins de fer et des tramways circulant sur des voies qui leur sont propres – the paraphrased translation is mine.
[981] Van Gerven 2001, p. 592/2; Van Dam 2013, p. 410; Borghetti 2018, p. 273, referring to *inter alia Cour de cassation* 2e civ. 22 January 2004, No. 01-11665, Bull. civ. II, and its decision of 21 July 1992, No. 91-13186, Bull. civ. II.
[982] Borghetti 2018, p. 272, paraphrasing article 1 MVID.
[983] Ibidem; this follows from various court decisions. See Furthermore Van Gerven 2001, p. 592/2.
[984] See Van Dam 2013, p. 409; Borghetti 2018, p. 278. See also *Cour de cassation* 2e civ. 19 October 2006, no. 05-14338, Bull. Civ. II.
[985] See Borghetti 2018, p. 278 and his reference to *Cour de cassation* 2e civ. 17 June 2010, No. 09-67338, Bull. civ. II.

physical contact between the motor vehicle and the victim,[986] *involvement* is also accepted whenever a motor vehicle had a "disturbing effect" resulting in damage.[987] *Involvement* was for instance upheld in the case where a traffic participant got scared by an (approaching) vehicle, leading to a collision between the traffic participant and an obstacle on the road.[988] Also the road-sweeping vehicle that sprinkled grit on the road, on which someone slipped (at a later moment) was held to be *involved* in a traffic accident.[989]

Whether an accident occurred on private property or on a public road, is indecisive for the applicability of the *Loi Badinter*, and it is furthermore not (always) necessary that the motor vehicle was actually in motion at the time of the accident.[990] The *Loi Badinter* does however not apply to motor racers.[991]

Victims of road traffic accidents can claim compensation from a driver (*conducteur*) and/or keeper (*guardien*) of any of the involved motor vehicles. This follows from article 2 *Loi Badinter,*[992] and case law of the *Cour de cassation*.[993] A keeper is defined as the one who has "use, control and direction" (*usage, contrôle, et direction*) of the motor vehicle.[994] Car owners are deemed "keepers" in sense of the *Loi Badinter*, although that presumption can be rebutted.[995]

> AVs fall under the scope of the *Loi Badinter*, which can be used in its current form by victims of accidents in which autonomous motor vehicles are involved. Even in states of progressed autonomy (for example SAE levels 3 – 5), where the role of *drivers* is gradually phased-out,

[986] However, it follows from *Cour de cassation* 2e civ. 20 January 1993, Bull. civ. 1993.II.19, that the victim needs to show that the "presence of the motor vehicle a necessary condition for the occurrence of the accident in order for that vehicle to be "involved" (impliqué) in the accident" (Van Gerven 2001, p. 592/3.
[987] See Borghetti 2018, p. 277; Van Dam 2013, p. 409.
[988] *Cour de cassation* 2e civ. 8 June 1994, Bull. civ. II, and *Cour de cassation* 2e civ. 13 January 1997, Bull. civ. II, both referred to by Van Dam 2013, p. 409, and *Cour de cassation* 2e civ. 23 March 1994, Bul. Civ. II., as cited by Borghetti 2018, p. 277.
[989] *Cour de cassation* Civ. 2e. 24 april 2003, referred to by Van Dam 2013, p. 409 (footnote 31).
[990] A fire in a parked car is considered as an accident (*Cour de cassation* 2e civ. 18 March 2004, No. 02-15190, Bull. Civ. II), however an exploding fuel truck is *not* considered an accident, as this truck was performing a "tool function" rather than a "travelling function" (*Cour de cassation* 2e civ. 19 October 2006, No. 05-14338), as both cited in Borghetti 2018, p. 273. The shredder, attached to a moving vehicle, which spits out a piece of wood, injuring a pedestrian *would* consititute a road traffic accident, according to the *Cour de cassation* 5 January 1994, 2e civ. Bull. civ. 1994.II.1, as cited in Van Gerwen 2001, p. 592/2.
[991] *Cour de cassation* 2e civ. 28 February 1996, No. 93-17457, Bull. civ. II, as cited by Borghetti 2018, p. 274.
[992] *Les victimes, y compris les conducteurs, ne peuvent se voir opposer la force majeure ou le fait d'un tiers par le conducteur ou le gardien d'un véhicule mentionné à l'article 1er*.
[993] *Cour de cassation* ch. Réuns 2 December 1941, Bull. civ. No 292, cited by Borghetti 2018, p. 274.
[994] Ibidem.
[995] See *Cour de cassation* 2e civ., 19 June 2003, Bull. civ. No. 00-18991, cited by Borghetti 2018, p. 274.

> victims may direct their claims at the *keepers*, or, when it is held that in SAE level 5 one does not any longer have "control and direction" over a car, at the owners.[996]

A claimant may thus choose who to sue (driver or keeper), which may be practical in case a driver cannot be identified. Should, for example, more than one motor vehicle be involved in a traffic accident, or when driver and keeper are two different persons, all these actors are jointly liable towards the victim(s).[997] Under the *Loi Badinter*, it is not excluded that a driver and/or a keeper can claim damages from other drivers or keepers of motor vehicles,[998] and it is also possible that an owner of a vehicle seeks compensation from the driver.[999] The *Loi Badinter* does however not apply to one-sided accidents.

4.3.3.3 Damage apportionment and defences

The main rule is that *any* person who suffered damage caused by a traffic accident in which a motor vehicle is involved, can claim damages. That includes *victimes par ricochet* (indirect victims).[1000] Although it is stipulated in the *Loi Badinter* that personal injuries and property damage qualify for remuneration, it is held that also other forms of damage are compensable, including pure economic loss, as long as the damage is "sufficiently closely connected to the initial harm".[1001] When those damages are sufficiently closely connected, 100% must be remunerated by a liable owner or keeper of a motor vehicle, unless a defence can be invoked. The (level of) applicability of those defences depend on the nature of the damage, and on the type of claimant, which will be elaborated hereafter.[1002] It must be noted first, that a defendant cannot rely on the *force majeure* defence, and the *act of a third party-defence* is also excluded.[1003]

> Differently from the situation in The Netherlands for example, also the passengers of the motor vehicle (including AVs) that was involved in the traffic accident can claim damages from the driver or keeper of the respective vehicle (or actually: from the insurance company).

---

[996] See Borghetti 2018, p. 290
[997] See Borghetti 2018, p. 275, referring to *Cour de cassation* 2e civ. 6 June 2002, No. 00-10187, Bull. civ. II.
[998] Ibidem, referring to *Cour de cassation* 1e Civ 29 February 200, No. 96-22884, Bull. civ. II.
[999] This follows from artivle 5, second paragraph *Loi Badinter*: *Lorsque le conducteur d'un véhicule terrestre à moteur n'en est pas le propriétaire, la faute de ce conducteur peut être opposée au propriétaire pour l'indemnisation des dommages causés à son véhicule. Le propriétaire dispose d'un recours contre le conducteur* (underlining added).
[1000] See Borghetti 2018, p. 278, 282; and also section 4.2.3.3. *Victimes par ricochet* are treated under the rules of the *Loi Badinter* the same way as direct victims, this follows from article 6.
[1001] Borghetti 2018, p. 278.
[1002] See Karner 2018, p. 371; Borghetti 2018, p. 279-282; Van Dam 2013, p. 408.
[1003] Article 2 *Loi Badinter*, which stipulates: Les victimes, y compris les conducteurs, ne peuvent se voir opposer la force majeure ou le fait d'un tiers par le conducteur ou le gardien d'un véhicule mentionné à l'article 1er. See also: Van Dam 2013, p. 409; Borghetti 2018, p. 279; Viney & Guégan-Lécuyer 2010, p. 68.

Article 3(1) *Loi Badinter* stipulates that the liability of drivers or keepers of motor vehicles can only be reduced, or in some cases, annulled, if they can prove an inexcusable fault (*faute inexcusable*) at the side of the victim.[1004] The extent to which a *faute inexcusable* may lead to a reduction of liability may depend on the nature of the damage and the type of defendant.

When a non-motorized victim suffered personal injuries, *faute inexcusable* can only be invoked when that inexcusable fault was the exclusive cause of the accident.[1005] Would that be proven, the victim will receive no compensation at all. However, this hardly ever happens, as this requires a "voluntary fault of an exceptional seriousness, exposing, without any reason, the person committing the fault, to a danger of which he should have been aware".[1006] This holds a double test: 1) the defendant should have been grossly negligent; and 2) a reasonable person would never have behaved as such.[1007] Van Dam notes that this could be the case if someone for instance intents to commits suicide, or behaves extremely recklessly.[1008] As Borghetti illustrates, it follows from case law that behaviour of a "passenger jumping from a car in motion",[1009] and "a pedestrian crossing an unlit motorway by night after having jumped over a safety barrier"[1010] qualify as such. Behaviour of drunken pedestrians who "crossed the road at a blind and dark bend", or who are "lying in the middle of the street in the middle of the night", [1011] do not.

> Whereas in The Netherlands, or in England, it could be argued that a hack of AV software may under certain conditions be construed as *force majeure*, it is unlikely that such circumstances would qualify as *faute inexcusable* under the *Loi Badinter.* The only exception could be when the victim hacked into the specific vehicle, while either accepting the risk of getting injured, or with the intention to harm himself by it.

[1004] *Les victimes, hormis les conducteurs de véhicules terrestres à moteur, sont indemnisées des dommages résultant des atteintes à leur personne qu'elles ont subis, sans que puisse leur être opposée leur propre faute à l'exception de leur faute inexcusable si elle a été la cause exclusive de l'accident.*
[1005] See art. 3(1) *Loi Badinter*; Karner 2018, p. 371; Borghetti 2018, p. 279.
[1006] See Borghetti 2018, p. 280, paraphrasing *Cour de cassation* 2e civ. 20 July 1987, No. 86-11275, Bull. civ II: "*une faute volontaire d'une exceptionelle gravité exposant sans raison valable son auteur à un danger don't il aurait dû avoir conscience*".
[1007] See Borghetti 2018, p. 280.
[1008] Van Dam 2013, p. 409
[1009] Borghetti 2018, p. 280, referring to *Cour de cassation* crim. 28 June 1990, No. 88-86996, Bull. crim.
[1010] Ibidem, referring to *Cour de cassation* 2e civ. 6 December 1995, No. 94-11481, Bull. civ. II.
[1011] Van Dam 2013, p. 409, referring to *Cour de cassation, assemblée plénière* 10 November 1995, D. 1995, 633, *JCP* 1996, II. 22564, comm. Viney, RTD Civ. 1996, 183, obs. Jourdain; *Cour de cassation* 2e civ. 23 January 2003, ETL 2003, 174 (Lafay, Morétau and Pellerin-Rugliano).

Non-motorized victims who are either younger than 16, older than 70, or for more than 80% disabled, are so called *victimes superprivilégiées*, and will always receive full compensation, unless they voluntarily sought the damage.[1012]

Motorized victims who suffer personal injuries are less protected than the non-motorized. It follows from article 4 *Loi Badinter* that the drivers' own fault may limit or exclude the damages he is to receive from the driver or keeper of a motor vehicle involved in a traffic accident.[1013] It must be noted however, that this "own fault" only relates to the origination of the damage, rather than the accident as such.[1014] As Van Dam illustrates: "[t]his implied for example, that when a victim driver is under the influence of alcohol but this does not contribute to the accident or his damage, the amount of damage will not be reduced".[1015]

> A situation of *own fault* might occur, when for example an AV-driver fails to install a safety-critical software-update of his vehicle, albeit being reminded to do so several times by the system, and the driver is notified of the (specific) damage that might result from not updating the software.

A victim's *own fault* is always a defence that can be invoked against claims from motorized and non-motorized victims regarding property damage, as follows from article 5(1) *Loi Badinter*.[1016] The "seriousness" of that *own fault* is decisive for the determination of the reduction of the damages to be compensated by the driver or keeper of the involved motor vehicle.

Furthermore, when the owner (not the driver) of vehicle A has suffered damage, as a result of a traffic accident in which vehicle B was involved, seeks remuneration from the driver or owner of vehicle B, his compensation may be reduced depending on the *own fault* of the driver of vehicle A,

---

[1012] Article 3(2) and (3) *Loi Badinter: Les victimes désignées à l'alinéa précédent, lorsqu'elles sont âgées de moins de seize ans ou de plus de soixante-dix ans, ou lorsque, quel que soit leur âge, elles sont titulaires, au moment de l'accident, d'un titre leur reconnaissant un taux d'incapacité permanente ou d'invalidité au moins égal à 80 p. 100, sont, dans tous les cas, indemnisées des dommages résultant des atteintes à leur personne qu'elles ont subis.*
Toutefois, dans les cas visés aux deux alinéas précédents, la victime n'est pas indemnisée par l'auteur de l'accident des dommages résultant des atteintes à sa personne lorsqu'elle a volontairement recherché le dommage qu'elle a subi. See also Borghetti 2018, p. 280; Van Dam 2013, p. 410.
[1013] *La faute commise par le conducteur du véhicule terrestre à moteur a pour effet de limiter ou d'exclure l'indemnisation des dommages qu'il a subis.*
[1014] See Borghetti 2018, p. 281, also referring to *Cour de cassation* 2e civ. 7 February 1990, No. 88-18441, Bull. civ. II.
[1015] *Cour de cassation, assamblée plénière* 6 April 2007, D. 2007, 1839, note Groutel, JCP 2007, II. 10078, note Jourdain; JCP 2007, I. 185, obs. Stoffel-Munck.
[1016] *La faute, commise par la victime a pour effet de limiter ou d'exclure l'indemnisation des dommages aux biens qu'elle a subis. Toutefois, les fournitures et appareils délivrés sur prescription médicale donnent lieu à indemnisation selon les règles applicables à la réparation des atteintes à la personne*.

notwithstanding the right of the owner of vehicle A to seek compensation from the driver.[1017] Article 3(3) *Loi Badinter* holds that when it can be proved that the victim voluntarily sought the damage, liability of the owner or keeper can be exonerated.

To conclude, it must be noted that a Reform Bill to the *Loi Badinter* has been proposed in 2017.[1018] In the Reform Bill,[1019] it is *inter alia* proposed that the *faute inexcusable* defence is limited further than in the current regime, i.e. that only a defence may be invoked in case a victim "voluntarily sought the harm which he suffered".[1020] Furthermore, all victims (thus including victim-drivers) shall have a right to compensation for personal injuries, unless there was an *faute inexcusable* which can be opposed to the victim-driver.[1021] This goes beyond the current situation, in which the drivers' *own fault* can be used as a defence.[1022] The regime currently applicable to *victimes superprivilégiées*, shall however not apply to victim-drivers. Regarding property damage, the Reform Bill proposes that the victims *own fault* remains as a defence, but where this *own fault* would lead to a total exclusion of compensation, this "must be specially justified by a court by reference to the seriousness of the fault".[1023]

> It is generally observed that the Reform Bill does not address AI and new technologies, [1024] but more importantly, that the current regime of the *Loi Badinter* is already sufficiently applicable to AVs.[1025] This would be true, I think, if the definition of *keepers* who can be held liable, would extend to those who use and control the vehicle, where "control" should be broadly interpreted, [1026] and that the requirement of "direction" is no longer made, as it can be questionable if one can still "direct" a fully autonomous vehicle[1027]

[1017] This follows from article 5(2) *Loi Badinter: Lorsque le conducteur d'un véhicule terrestre à moteur n'en est pas le propriétaire, la faute de ce conducteur peut être opposée au propriétaire pour l'indemnisation des dommages causés à son véhicule. Le propriétaire dispose d'un recours contre le conducteur.,* as paraphrased by Borghetti 2018, p. 282.
[1018] Ministère de la Justice, "Projet de Réforme de la Responsabilité Civile, CHAPITRE VI - LES PRINCIPAUX REGIMES SPECIAUX DE RESPONSABILITE SECTION 1 Le fait des véhicules terrestres à moteur," via http://www.justice.gouv.fr/publication/Projet_de_reforme_de_la_responsabilite_civile_13032017.pdf (last accessed 26 march 2020), and the official translation thereof by S. Whittaker and J.S. Borghetti, available via http://www.textes.justice.gouv.fr/art_pix/reform_bill_on_civil_liability_march_2017.pdf (last accessed 26 March 2020), hereafter: Reform Bill.
[1019] See for a more detailed elaboration Borghetti 2018, p. 289-290.
[1020] Article 1286 Reform Bill.
[1021] Article 1287 Reform Bill.
[1022] See for this interpretation also Borghetti 2018, p. 289.
[1023] Article 1288 Reform Bill.
[1024] See also: Borghetti 2018, p. 290.
[1025] Ibidem.
[1026] Holding *inter alia* that also the instruction by a person to drive the AV from point A to point B, would qualify as "control".
[1027] Especially with high-level (SAE 4-5) AVs, "human" direction of a car will no longer be required.

4.3.4 ENGLAND

4.3.4.1 Introduction

In England (and Wales), questions regarding liability for accidents in which motor vehicles are involved, are traditionally answered on the basis of negligence rules.[1028] Until recently, there was no strict liability regime in place such as the *Wegenverkeerswet* in the Netherlands, or the *Loi Badinter* in France. Victims of traffic accidents may hold the *driver* of a motor vehicle liable, when that driver was in breach of a "duty of care" towards the victim, in the sense that he was careless i.e. failed to comply with a standard of care, resulting in damage suffered by the victim, for which the driver can be held responsible.[1029]

> As the *driver* will be of decreasing importance as AV technology develops because AVs will increasingly be able to drive themselves (resulting therein that eventually one cannot speak of a driver any longer), the traditional negligence regime will become less significant. This is even more so, since the AV-specific strict liability regime of the Automated and Electric Vehicles Act has been introduced in 2018, which has entered into force as of 21 April 2021.[1030]

The AEVA does *inter alia* not apply to situations in which autonomous driving mode has not been engaged, it is still relevant to illustrate the traditional negligence rules, which will be done in section 4.3.4.1. The contributory negligence defence is addressed in section 4.3.4.2. Section 4.3.4.4 highlights the new rules of the AEVA, insofar as these have not been addressed in section 4.2.5.7.[1031]

4.3.4.2 Allocation of liability: (stricter) negligence

In order to be successful in a negligence claim, a claimant has to prove that the defendant was in *breach* of a *duty of care* (i.e. acting carelessly); that he had suffered *damage* which can be attributed to the defendant as a result of rules on *causation*.[1032] As there are specific rules regarding the *duty of care* to be observed by drivers of motor vehicles, these will be elaborated further in this section.

In order to establish whether or not a defendant acted carelessly, his conduct is usually compared to the conduct of "a reasonable man of ordinary prudence", which constitutes the *standard of care*.[1033] Regarding traffic accidents, the concept of the "reasonable man" has developed in case

---

[1028] There are however also other causes of action that may apply, such as the *tort of trespass* or *public nuisance*, as illustrated in Bagshaw 2010, p. 38-39. Negligence is however the most 'common' cause of action in traffic accidents in which motor vehicles are involved. Strict liability has – until the AEVA – been rejected by the courts. See Baghsaw 2010, p. 39-41.
[1029] See Deakin, Johnston & Markesinis 2007, p. 99.
[1030] See section 4.2.5.7.
[1031] See furthermore De Bruin 2020.
[1032] Deakin, Johnston & Markesinis 2007, p. 99; Van Dam 2013, p. 230-231.
[1033] *Blyth v Birmingham Waterworks* [1856] 156 R 1047, 1049, as cited in Van Dam 2013, p. 230; Sappideen & Vines 2011, p. 123.

law in (mainly) the 20th century. Although the standard of care does not enshrine that one has to drive "in as safe a way as is technically possible",[1034] it is higher than what would be regularly required from a "reasonable man", and is stricter than the standard of care to be observed by those operating in less risky environments than drivers of motor vehicles.[1035] This stricter-than-average standard of care, resulting therein that victims of car accidents are better protected than victims of other negligent behaviour ,must be observed against the backdrop (also in England and Wales) of an increase in traffic accidents since the second world war, and the fact "that motor vehicles, more than any other item of technology, exposed a large proportion of the population to the risk of becoming a tortfeasor".[1036]

This high *standard of care* follows *inter alia* from the decision in *Roberts v Ramsbottom*,[1037] in which it was held that even driver Ramsbottom who lost consciousness due to a minor stroke, for which he could not be blamed as there were no earlier occasions or symptoms indicating that he was unfit to drive, acted negligently by driving into Roberts. Furthermore, in *Ng Chun Pui v Lee Chuen Tat*, it was established, based on *res ipsa loquitur,*[1038] that the driver of a coach who crossed the grass central reservation between the carriageways and eventually collided with a passenger bus heading in the opposite direction, was acting negligently.[1039] It was inferred that a well-maintained bus that was driven properly, would not get involved in such an accident unless it was not being driven in conformity with the due *standard of care*.[1040] The *standard of care* is the same for experienced and non-experienced drivers, as follows from *Nettleship v Weston*.[1041]

There are also indications however, that the *standard of care* is not always interpreted strictly by the courts. For example, the defendant whose brakes failed, saw the negligence claim against him dismissed because he could adduce evidence to counter the court's assumption (again based on *res ipsa loquitur*) that the vehicle must have been poorly maintained, by showing that his minibus was recently serviced and passed its MOT-test (the mandatory yearly test to check whether or not a car is still safeto drive).[1042] Furthermore, the Court of Appeal held in *Moore v Poyner*, that the driver of a bus, who drove in conformity with the speed limit 30 miles/hour in a residential area on a (dry) Sunday afternoon, and collided into a kid who appeared from behind another (parked) bus, was not acting negligently as he could not have reasonably anticipated that the kid emerged

[1034] Bagshaw 2010, p. 41. See differently: Van Dam 2013, p. 303.
[1035] Van Dam 2013, p. 303.
[1036] Bagshaw 2010, p. 37.
[1037] *Roberts v Ramsbottom* [1980] 1 WLR 823.
[1038] I.e. it was assumed by the court that negligence logically follow from the facts of the case. See for more on *res ipsa loquitur* as a "rule of proof" in civil procedure section 4.2.3.5.
[1039] *Ng Chun Pui v Lee Chuen Tat* [1988] RTR 298.
[1040] Ibidem.
[1041] *Nettleship v Weston* [1971] 2 QB 691, CA.; Bragshaw 2010, p. 41-42; Van Dam 2013, p. 413.
[1042] *Worsley v Hollins* [1991] RTR 252, CA

on the road from behind the bus, considering the fact that the driver did slow down when approaching the parked bus, and the fact that he was aware of children playing in that area.[1043] The *standard of care* defined in *Roberts v Ramsbottom* was nuanced in *Mansfield v Weetabix*.[1044] The Court of Appeal held in that case, that driver Tarleton, who crashed a car as a result of a low blood sugar caused by a disease that was not known and could not have been known by him, was *not* acting below the *standard of care*. In a similar vein, a bus driver who suddenly breaked to avoid collision with a dog,[1045] and a policeman who made an error of judgment in the pursuit of a driver of a stolen car, were not acting negligently.[1046]

The foregoing shows that, while a 'stricter' form of negligence[1047] seems to result from case law regarding accidents with motor vehicles in England and Wales in the form of a rather high *standard of care*, there are several – case specific – exceptions to this rule. Furthermore, courts tend to aid victims of motor vehicle related accidents by for instance assuming negligence on the basis of *res ipsa loquitur*.[1048] However, the burden of proof (regarding the *duty of care*, *damage*, and *causation*)[1049] remains at the victim.[1050]

4.3.4.3 Contributory negligence defence: damage apportionment

Once *negligence* has been established – and liability is thus allocated, damage can be apportioned. The most common defence that can be invoked by the liable party in order to reduce the obligation to remunerate damages is *contributory negligence*.[1051] This is a "partial defence" since the introduction of the Law Reform (Contributory Negligence) Act 1945. Before that act, the defence led to a complete reduction of liability. Since then, courts are allowed to distribute losses between claimant and defendant, varying from 0% to 100% to be borne by either the claimant or the defendant.[1052] For a successful *contributory negligence* defence, it is necessary that the defendant can prove *fault* of the claimant,[1053] which is defined as "negligence, breach of statutory duty or other act or omission that gives rise to liability in tort, or would, apart from this Act, give rise to the defence of contributory negligence".[1054] The test that is used in order to assess the claimants'

[1043] *Moore v Poyner* [1975] RTR 127, CA, as referred to in Bagshaw 2010, p. 41-42.
[1044] *Mansfield v Weetabix Ltd* [1998] 1 WLR 1263, CA.
[1045] *Parkinson v Liverpool Corporation* [1950] All ER, 367, CA.
[1046] *Marshall v Osmond* [1983] QB 1034, CA.
[1047] Van Dam 2013 identifies this as "stricter liability" (p. 302-304; 413).
[1048] See also Bagshaw 2010, p. 42.
[1049] Causation and damages are not addressed in these sections, as I have chosen to focus on the material rules that are most specific for motor vehicle accidents . See for causation and damages in product liability cases and some general principles under English law: section 4.2.5.3 (damage) and 4.2.5.4 (causation).
[1050] Van Dam 2013, p. 413-414
[1051] See Markesinis, Deakin & Johnston 2013, p. 749-750.
[1052] Ibidem, p. 753-754, referring to *inter alia McKew v Holland and Hannen and Cubitts (Scotland) Ltd.* [1969] all ER 1621.
[1053] Section 1 jo. 4 Contributory Negligence Act (CNA).
[1054] Section 4 CNA; see Deakin Johnston & Markesinis 2013, p. 754.

fault, is "whether the claimant acted reasonably, that is to say, with the amount of self-care that a normal person would have exercised in the circumstances".[1055] When *fault* has been established, a court can reduce the amount of damages to be paid "to such extent as the court thinks just and equitable having regard to the claimant's share in the responsibility for the damage".[1056]

Differently from the traffic liability applicable in for example France and The Netherlands, liability may be reduced up to 100% when *contributory negligence* can be proven by a liable motorist. Although this defence can hardly be relied on when a victim is 5 years of age or younger,[1057] it may successfully be invoked against any 'older' victims. For example in *Morales v Eccleston*,[1058] the 11 year old Morales was held to be 75% to blame himself for chasing after a football onto the public road, without checking for oncoming traffic. In *Gough v Thorne*, a 13 year old girl waited for a lorry, which stopped to let her pass. Unfortunately, she was hit by a car that overtook the lorry. In appeal, the *contributory negligence* defence was dismissed as she was not of such an age to be "reasonably expected to take precautions for her own safety".[1059] The *contributory negligence* defence was succesfully invoked against an uncautious adult crossing roads in *Fitzgerald v Lane*.[1060] It was held that the victim was to blame 50%, as he had ignored a red traffic light and was hit by two cars successively, and suffered tetraplegia. Also, a motorist who did not like seatbelts (and did not put them on), and suffered injuries was held to be blamed himself for 20% - as wearing seatbelts could have prevented some parts of the damage, and whereas normal self-caring persons would have chosen to wear them.[1061] Furthermore it is observed that, even on short trips and when the chances of an accident are low, the impact and harm that might result when – against the odds – an accident would happen is very large compared to the effort and costs of taking the precautionary measure of using seatbelts. Failure to wear a crash helmet by motor cyclists has led to a comparable outcome.[1062] However, Deakin, Johnston and Markesinis point out that not wearing seatbelts by women in advanced stages of pregnancy, or not wearing helmets by Sikhs wearing turbans might be exempted from the rule to either wear helmets or seatbelts;[1063] a *contributory negligence* defence might not be invoked in such cases. Driving in a vehicle that is

[1055] Ibidem, p. 755.
[1056] Section 1 CNA.
[1057] *Barnes v Flucker* [1985] SLT 142, OH, see: Lunney, Nolan & Oliphant 2017, p. 317.
[1058] *Morales v Eccleston* [1991] RTR 151.
[1059] *Gough v Thorne* [1966] 3 All ER 398, [1966] 1 WLR 1387 (quote by Lord Denning); see Van Dam 2013, p. 415.
[1060] *Fitzgerald v Lane* [1989] 1 AC 328.
[1061] *Froom v Butcher*[1976] AC 286, CA. See also Deakin, Johnston & Markesinis 2013, p. 755.
[1062] *O'Connel v Jackson* [1972] 1 QB 270; and *Capps v Miller* [1989] 1 WLR 839.
[1063] Deakin, Johnstin & Markesinis 2013, p. 755.

known to be defective,[1064] or embarking on a vehicle with the knowledge that the driver is drunk and therefore unfit to drive,[1065] may however constitute *contributory negligence*.

4.3.4.4 AEVA 2018

The AEVA 2018 is, to a certain extent, applicable to accidents in which autonomous vehicles are involved. As introduced in section 4.2.5.7, the AEVA 2018 makes either the insurer or the owner of an "automated vehicle" strictly liable for damage caused by the automated vehicle. One of the purposes of the AEVA is to better protect victims of AV-related accidents, as the current liability- and insurance rules are considered insufficient in that respect, as victims would have to seek remuneration from AV producers under the current rules.[1066] However, there are several situations in which the AEVA-rules will not apply. As the AEVA 2018 leaves the 'old' liability rules untouched, the aforementioned regimes on product liability and negligence will in those situations still be applicable. In the following sections, the boundaries of the AEVA 2018 and the possible interfaces with the traditional negligence rules are explored.

4.3.4.4.1 Scope

It follows from article 1 AEVA 2018 that *automated vehicles* fall under its scope, that are "designed or adapted to be capable, in at least some circumstances or situations, of safely driving themselves". Such vehicles must be listed by the Secretary of State. This entails that probably only AVs that are on the SAE-list identified as level 4 or 5 are covered by the regime,[1067] provided that they are on the list. Vehicles containing some driver assistance systems (such as lane change assistance and/or adaptive cruise control), that require the driver to take back control when requested, will likely be out of scope of the AEVA 2018.[1068] Furthermore, the AEVA 2018-regime only applies to *automated vehicles* when driving themselves,[1069] which is the case "if it is operating in a mode in which it is not being controlled, and does not need to be monitored, by an individual".[1070] Only SAE-level 4 and 5 vehicles may not have to be monitored by human drivers for large parts (level 4) or all of the driving modes (level 5). This implicates that – at least until level 4 and 5-vehicles are widely deployed, the AEVA 2018-regime will often not apply.

[1064] *Gregory v Kelly* [1978] RTR 426.
[1065] As referred to in Deakin, Johnston and Markesinis 2013, p. 755, fn. 49: *Owens v Brimmel*, [1977] QB 859; *Ashton v Turner* [1981] QB 137; *Meah v McCreamer (No. 1)* [1985] 1 All ER 637; *Gleeson v Court* [2007] EWCA Civ 2397.
[1066] See Burcher & Edmonds 2018.
[1067] See section 2.3.
[1068] See Channon 2019, p. 19; also J. Marson, K. Ferris & J. Dickinson, "The Automated and Electric Vehicles Act Part I and Beyond: A Critical Review", *Statute Law Review* 2019, Vol XX, no XX, 1-22, doi:10.1093/slr/hmz021 (hierna: Marson, Ferris & Dickinson 2019), p. 17-19.
[1069] Section 2(1)(a) and 2(2)(a) AEVA 2018.
[1070] Section 8(1)(a) AEVA 2018.

4.3.4.4.2 Causation and damage

The AEVA-regime is only applicable where an accident is (wholly or partly)[1071] *caused by* an automated vehicle when driving itself,[1072] and a person suffers damage *as a result* of the accident.[1073] The absence of a specific rule of proof in the AEVA 2018, implicates that the burden to prove that the accident was caused by an AV and that damage resulted therefrom, rests on the victim.

> The fact that victims need to prove causation implies uncertainty, and that it is (still) necessary for them to establish that a vehicle was in self-driving mode, and that self-driving caused their damage, which cannot be done without proper access to and (likely expensive) means to interpret vehicle data.[1074] It will be up to the courts to decide whether or not to help victims in their position through, for example, using assumptions (to be rebutted by the AV-owners or insurers), while the legislator could have made another choice in this regard, for instance through not legislating a *causation* requirement. However, absence thereof may in turn result in a high number of (illegitimate) claims.[1075] Another option would have been to reverse the burden of proof, i.e. that *causation* is automatically assumed, unless the opposite can be proven by the defendant.
>
> As it seems, insurers in the UK are actually open for a solution to ensure "adequate and open access to crash data",[1076] which may be of aid in establishing proof of the self-driving mode, and causation between that self-driving mode and the damage. Keeping and providing access to such data to underpin an AEVA 2018-claim, will constitute processing of personal data in the sense of the General Data Protection Regulation.[1077] That data processing would have been less necessary when another path had been chosen by the legislator, for example if AV

[1071] Section 8(3)(b) AEVA 2018.
[1072] This applies whenever either if the vehicle is insured (section 2(1)(c) AEVA 2018), or when it does not have to be insured as a result of section 143 Road Traffic Act 1988 (RTA), when either the exemption for public bodies etc. applies (144(2) RTA), or because the vehicle is in public service of the crown (section 2(2)(c) AEVA 2018). A vehicle is furthermore *driving itself* when it is not controlled, and does not need to be monitored by an individual (8(1)(a) AEVA 2018).
[1073] See sections 2(1)(c) and 2(2)(c) AEVA 2018.
[1074] Channon 2019 (p. 25) indicates that it "could be a significant challenge" to prove "that the accident was caused when the vehicle was driving itself at the time".
[1075] See also Engelhard & De Bruin 2018, p. 90-91.
[1076] See Cbannon 2019, p. 25 and his reference (fn. 97 and 78) to Association of British Insurers and Thatcham Research, "Pathway to Driverless Cars: Proposals to support advanced driver assistance systems and automated vehicle technologies: Response of the Association of British Insurers and Thatcham Research" of June 2016, p. 19, available via https://www.abi.org.uk/globalassets/sitecore/files/documents/consultation-papers/2016/09/090916_abi_thatcham_response_ccav_automated_driving_consultation.pdf, last accessed 2 March 2020.
[1077] See 0.

involvement in a crash would have been enough to establish (risk) liability for the insurer or owner of the vehicle.

Should it not be possible to prove *causation*, making a claim based on the AEVA 2018 unsuccessful, the negligence regime may serve as an alternative. The victim must then prove that the driver was acting below the required *standard of care*. That can be problematic, especially when considering that it has been impossible for the victim to establish a causal relationship between the self-driving mode and the accident, and/or a causal relationship between the accident and the damage.

Damage to be remunerated under the AEVA 2018, is limited to "death or personal injury and any property other than (a) the automated vehicle; goods carried for hire or reward in or on that vehicle or in or on any trailer (whether or not coupled) drawn by it, or (c) property in custody, or under the control of"[1078] either the insured person, or the person in charge of the vehicle (when the vehicle does not have to be insured).

Although the implications for victims in terms of proof-issues may be less significant for victims in this regard than regarding causation (as aforementioned), the "usefulness" and "equitability" of these damage-provisions are also questioned.[1079] The fact that automated vehicles and their load are to a large extent exempted from the recovery obligations, and that it is likely that many objects carried by an AV are in the custody of "the person in charge of the vehicle" implies that most of the property damage is to be carried by the victims themselves.

4.3.4.4.3 Exclusions and limitations

There are several limitations regarding the obligation to remunerate damages for the liable insurer or vehicle owner. First of all, it must be noted that *contributory negligence* may be invoked. Section 3(1) AEVA 2018 stipulates that the liability of the owner/insurer may be reduced insofar that follows from application of the Law Reform (Contributory Negligence) Act 1945. It follows from section 3(2) that owners/insurers may even be entirely exempt from liability (only) to the person in charge of the vehicle "where the accident that it caused was wholly due to the person's negligence in allowing the vehicle to begin driving itself when it was not appropriate to do so". When such negligence will occur has not been clarified in the AEVA 2018. Although it is stated that "[t]he term 'wholly' is likely to impose a significant burden upon the insurer to ensure that

[1078] Section 2(3) AEVA 2018.
[1079] See Channon 2019, p. 24

there were no other causes of the accident or contributing factors, however minor",[1080] the absence of clarification leaves uncertainty for drivers.

> What this exception also entails, is – if anything – a duty of care for drivers to verify whether or not it is appropriate to engage a self-driving mode. That could perhaps result in an extensive checklist that must be used upon engaging autopilot functions. Questions that might arise, could include:
>
> - Would it be appropriate to use self-driving modes in case of frosty weather, heavy rain or mist?
> - Is it appropriate to use self-driving modes within urban areas, or with heavy traffic?
> - Would it be appropriate to beta-test new functions of an AV?
>
> Such questions should in my opinion not be of concern for drivers of *automated vehicles* in sense of the AEVA 2018, as it might discourage people to use the technology.

Furthermore, insurance policies may contain certain exclusions or limitations of the insurers' liability to remunerate damages to the insured person (i.e. a vehicle owner for example) if an accident is the direct result of software alterations made or permitted by the insured person, when such alterations are prohibited in the insurance policy. When software alterations are made with the knowledge of an insured person (for example by a driver that is not the same person as the vehicle owner), despite a known[1081] prohibition in the policy, and an accident is the direct result of that software alteration, an insurer (or owner) who has paid damages to a victim, may seek redress from the person who made, or had knowledge or, the software alterations.[1082]

The same mechanism applies to failures "to install safety-critical software updates that the insured person knows, or ought reasonably to know, are safety-critical".[1083] Thus: an insurance policy may provide that the insurers' liability can be limited if the insured person fails to install safety-critical software updates, and the insurer (or owner) may seek redress from that person after having compensated victims who claimed damages under the AEVA 2018. Software updates are deemed "safety-critical", if "it would be unsafe to use the vehicle in question without the updates being installed.[1084]

[1080] Channon 2019, p. 31.
[1081] Section 4(2) AEVA 2018.
[1082] Section 4(3) jo. (4)(a) AEVA 2018.
[1083] Section 4(1)(b) jo. 4(3) jo. (4)(b) AEVA 2018.
[1084] Section 4(6)(b) AEVA 2018.

It makes sense that an insurer might want to prevent unauthorize software alterations to be made. Whether or not 'auto-updates' by a self-learning algorithm incorporated in an AV could also qualify as a prohibited software alteration, exempting the insurers' liability, is also a relevant question. Such 'auto-updates' can be agreed with in general terms by a vehicle owner or user, but might result at the same time in a potential liability reduction.

Another uncertainty lies in the definition of what might constitute "safety-critical" software-updates. Given the wordings of section 4(6)(b) AEVA 2018, it is for the insured person to judge whether or not skipping the update would render a vehicle unsafe, which may require (extensive) research into the safety problems that not installing an update might cause. It is questionable if such enquiries can be made by 'normal' AV users.[1085] Another option would have been to require manufactures to 'push' safety critical updates to AVs.[1086] However, perhaps because the AEVA 2018 did not intend to address AV-producers, the current solution was enacted.

4.3.5 Conclusion

Having examined the legal frameworks of The Netherlands, France and England that may apply to road traffic accidents in which AVs are involved, some observations can be made regarding similarities and differences between those three systems. Furthermore, I will make several assumptions as to how the characteristics of the current traffic liability regimes might interact with innovation and acceptance (taking account of the factors identified in section 3.4) thereof in the field of AVs, given the increasing autonomy of such vehicles, as further examined in Chapter 6.

4.3.5.1 Allocation of liability

Under the French *Loi Badinter* all victims of road traffic accidents, other motorists, passengers and indirect victims included, can claim compensation from a driver or keeper of a motor vehicle. The *Loi Badinter* provides a very strict risk liability regime, the sheer *involvement* of a motor vehicle (even when parked, and an actual collision is not necessary) suffices to establish liability. Victims have to prove such involvement. It is very likely that the French rules will apply to road traffic accidents in which AVs are involved; victims may thus seek compensation from keepers (those who use, control and direct a motor vehicle) when drivers will be gradually phased out as vehicles become more autonomous.

[1085] See also Channon 2019, p. 24-26.

[1086] See R. Jones, "The Automated and Electric Vehicles Act 2018 – six months on, is it fit for purpose?", *Roydswithyking.com*, 13 februari 2019, via https://www.roydswithyking.com/the-automated-and-electric-vehicles-act-2018-six-months-on-is-it-fit-for-purpose/ (last accessed 23 januari 2020).

The rules applicable in England and Wales are of a different nature. Traditionally, negligence rules are to be applied in order to establish liability. Drivers are liable towards victims of traffic accidents to the extent that they acted contrary to their *duty of care*. The standard of care to be obeyed by drivers is rather high (vehicles must be properly maintained, health problems of drivers are often taken to be their own risk, and even improbable actions of other road users must be anticipated), and is the same for experienced and not-so-experienced drivers. Be that as it may, victims do have to prove negligence of the driver. There are certain mechanisms in place that tend to aid claimants: judges often assume negligence based on the facts of the case (*res ipsa loquitur*). Application of these negligence rules in AV-related accidents can be problematic, but the British legislator anticipated the advent of self-driving technology in the AEVA 2018. The AEVA 2018 introduces a risk-liability regime for AV-accidents, and leaves other liability frameworks intact. Insurers, or owners who do not have to take out vehicle insurance, will be liable for damage caused by an automated vehicle when driving itself. Victims have to prove that a vehicle was in self-driving mode, the damage and causality between the AV-accident and the damage. Thus, the level of protection of AV-related accidents will likely improve.

The legal framework in the Netherlands combines some of the characteristics of the French and the English rules. Article 185 WVW is a risk-liability system, although its scope is more limited than the *Loi Badinter*. It applies to traffic accidents in which motor vehicles are involved. Non-motorised victims (not: passengers, or motorised victims) can seek compensation from the owner or keeper of the vehicle. This regime applies to motor vehicles in motion, and is not applicable to parked cars for example. Victims have to prove the involvement of a motor vehicle. It is very likely that article 185 WVW equally applies to traffic accidents involving AVs. In situations where article 185 WVW does *not* apply, for instance in cases where the victim is a passenger of the involved vehicle, or where the victim is the driver or passenger of another motor vehicle, a compensation claim can be based on the general fault liability rule of article 6:162 BW. In 6:162-claims, victims have to prove fault (an *attributable unlawful act*) of the defendant. Such *unlawful act* may exist when a driver for instance acted carelessly (cf. negligently), or violated statutory (traffic) rules. The standard of care to be taken into account by drivers is high, and entails *inter alia* that faults of other traffic participants must be anticipated, unless so improbable that the driver could not reasonably have taken such faults into account. *Unlawful acts* can often easily be attributed to drivers, *legal blameworthiness* suffices here. AVs are not anticipated upon in these rules, so when autonomy increases it will become harder to establish unlawful conduct of drivers. It is argued however (yet this is for the courts to decide and until then uncertain), that carelessness of AV-drivers or -owners can consist of wrongfully allowing an AV to be set in motion, or wrongfully not taking back control, when the AV requires so, or when or intervening in the self-driving mode *without* being instructed to do so. The *causal relationship* between the *unlawful act* and *damage*

must be proven by the victim as well, although certain mechanisms have been developed in case law that can aid victims in their position. Alternatively, a liability claim for damage caused by an AV might be based on article 6:173 BW, a strict liability regime for possessors of defective movable goods. It is however uncertain when an AV can be held *defective* (which is for a victim to prove), and the fact that victims also have to prove that *defects did not exist* when movable goods were entered into circulation, are considered to be problematic. Proof of defects, (the moment of) their origination, and causality between defects and damage requires extensive analysis and interpretation of technical data, which can also be very challenging, time- and money consuming for victims.

4.3.5.2 Defences and damage apportionment

Under the *Loi Badinter*, the only invokable defence is *faute inexcusable* at the side of the victim (*force majeure* and the *act-of-a-third-party defence* are excluded). *Faute inexcusable* is seldomly accepted, as it requires that the victim was grossly negligent, and that a reasonable person would never have acted as such. Only extreme behaviour, such as jumping in front of a moving vehicle, or crossing an unlit motorway in the middle of night qualify as *faute inexcusable*.

When liability has been established, 100% of the suffered damages have to be remunerated in principle. Compensation of *motorized* victims (including vehicle owners who did not drive the vehicle), or *property damage* of *non-motorized* victims can be reduced to the extent that the damage results from the *own fault* of those victims. It is generally assumed that the *Loi Badinter* is sufficiently equipped to deal with AV-related accidents.

The most important defence under the English negligence system, is the *contributory negligence* defence. Fault at the side of the victim must then be proven. It is tested to what extent the "claimant acted reasonably, that is to say, with the amount of self-care that a normal person would have exercised in the circumstances".[1087] Failure to take precautionary measures such as wearing seatbelts or crash helmets, chasing a football on the public road, ignoring red traffic lights, driving in defective vehicles and embarking on a vehicle with the knowledge that its driver is drunk, all constitute (to varying extents) contributory negligence. When contributory negligence is proven, it is up to the court to reduce damages "to the extent as the court thinks just and equitable having regard to the claimant's share in the responsibility for the damage[…]".[1088] Differently from the French and Dutch legal systems, contributory negligence of all "kinds of" victims can be invoked, even from children (above the age of 5). Contributory negligence is also allowed as a defence under the AEVA 2018. It is indicated that it can be negligent towards insurers, when an AV is

[1087] See Deakin, Johnston & Markesinis 2013, p. 754.
[1088] Section 1(1) CNA.

allowed to drive itself when it was not appropriate to do so. This entails uncertainty for AV drivers, or at least a duty of care to verify whether or not enabling a self-driving mode is appropriate. Furthermore, it can constitute contributory negligence towards insurers when, contrary to insurance policies, software alterations are (allowed to be) made, and when safety-critical updates are not installed.

In the Netherlands, the most important defence to an article 185 WVW-claim is *overmacht* (force majeure). *Overmacht* can be a valid defence when the driver cannot legally be blamed for his conduct, and the accident was completely due to another person's fault, which was so improbable that the driver could not reasonably have taken that fault into account. An *overmacht*-defence is seldomly awarded. When victims of traffic accidents are younger than 14 years of age, the criteria are even stricter. In those cases *overmacht* cannot be successfully invoked unless the child acted intentionally or wilfully recklessly, even when the child's behaviour significantly contributed to the accident. As an *overmacht* defence is never successful in cases of victims younger than 14, and contributory negligence is practically never applied in these cases, this situation is described as the 100%-rule. It is questionable whether or not accidents caused by an AV that was hacked into by a third party can qualify as *overmacht*, when all necessary precautions have been taken by the vehicle owner (or keeper). When *overmacht* cannot be proven, in principle all damages have to be remunerated. The amount of damages can be reduced to the extent that the victim (when he was at least 14 years old) was at fault himself. This contributory negligence defence (based in article 6:101 BW) consists of two steps. First, causal apportionment must be established. Second, this causal apportionment can be corrected by a judge, to the extent that fairness requires him to do so. It follows from case law that at least 50% of the damages have to be borne by the liable owner or keeper of a vehicle. *Overmacht* and *contributory negligence* can also be invoked by defendants facing claims based on article 6:162 BW. Furthermore, in such cases a *justification ground* can be established by the defendant. These defences can also be invoked by a defendant under a 6:173 BW-claim. Moreover, when defendants state that the defect already existed at the time that the respective movable good was entered into circulation, it is up to the claimant to prove the opposite.

It can be concluded that, from a formal point of view, the Dutch system is the most complex of the three regimes illustrated above for victims of road traffic accidents in terms of finding the right basis to file a claim for remuneration of traffic accidents involving AVs. A 'one-stop-shop' does currently not exist. Non-motorised victims can seek damage compensation on the basis of article

185 WVW, while non-motorised victims must base their claim on 6:162 BW.[1089] Under the French Loi Badinter, no distinction is made between motorised and non-motorised victims. The AEVA 2018 also creates a one-stop-shop for victims, of highly or fully autonomous vehicles, irrespective of their means of transportation, to claim damages from insurers or (uninsured) vehicle owners. When the AEVA is not applicable, and a claim must be based on negligence, the nature of the claimant does not matter either.

4.4 RECENT EU-BASED REGULATORY DEVELOPMENTS AND RECOMMENDATIONS

4.4.1 INTRODUCTION

As indicated above, several recommendations have been made for and by the European institutions regarding the adaptation of liability regulation in order to properly address the new risks that (mainly) AI may pose to consumers. As I will refer to some of these (i.e. the most recent and therefore relevant recommendations) below, especially in my recommendations (Chapter 8 and Chapter 9), it is relevant to briefly illustrate the following three: 1) The recommendations done by the Expert Group (EG) on Liability for New Technologies for the European Commission in 2020;[1090] 2) the subsequent Juri-committee response authored by Bertolini for the European Parliament;[1091] and 3) the (most recent)[1092] EP proposal with recommendations to the EC on "a civil liability regime for artificial intelligence" (EP Proposal).[1093]

4.4.2 THE EXPERT GROUP REPORT

The Expert Group reviewed the extra-contractual liability frameworks that might apply to AI and other "emerging technologies". They found *inter alia* that the studied liability frameworks offer basic protection for victims of damage induced by the operation of such emerging digital technologies, but that successful compensation will become increasingly difficult as technology becomes *inter alia* more complex; can be modified during it lifetime as a result of self-learning technology or updates; operates in less predictable ways; and is prone to cybersecurity risks.[1094] Several changes to both the harmonised and the non-harmonised liability regimes are suggested. Operators (who can exercise more control that regular users) of for instance AI-driven robots which implicate high risks for citizens, for instance as a result of their application in public spaces, should amongst other things be strictly liable towards victims; Fault-based liability should be

[1089] Furthermore, when confronted with a defective vehicle, a victim requiring remuneration from its possessor, first has to establish whether or not the defect existed when it was put into circulation in order to ascertain whether to sue its possessor on the basis of 6:173 BW or instead its producer under 6:185 BW.
[1090] See European Commission 2020.
[1091] European Parliament 2020.
[1092] I.e. until September 1st 2021.
[1093] European Parliament 2020a.
[1094] European Commission 2020, p. 3.

bestowed on operators of less risky AI-driven applications, in cases of improper selection, operation, monitoring and maintaining the respective technology.[1095] Thus, the Expert Group distinguishes between strict liability for operators of "high-risk" AI, and fault liability for "low-risk" AI. Furthermore, the Expert Group suggests that "manufacturers of products or digital content incorporating digital technology" must be considered as producers in sense of the PLD, and producers should be liable for damages that result from defective products, even after putting those products on the market.[1096] Compulsory insurance is suggested for situations in which third parties could be confronted with harmful new technology. Also, procedural aids are to be provided to victims who are confronted with increased "difficulties of proving the existence of an element of liability beyond what can be reasonably expected".[1097] Emerging technologies would furthermore, where appropriate, have to be equipped with features to log their activities. Non-compliance with logging-obligations, or the obligation to provide access to the logged information, should lead to reversed proof-burdens for operators in order to better facilitate the proof position of victims. While awarding emerging technologies legal personality is considered unnecessary, the Expert Group sees it fit to regulate that "destruction of the victim's data should be regarded as damage" which must be remunerable in some cases.[1098]

4.4.3 EP's Juri Committee Response

Under the authorship of Bertolini, the Juri Committee of the European Parliament has responded that a consolidated approach such as the one the Expert Group suggested, in order to adapt extra-contractual liability rules might not be necessary. Regulatory intervention should occur through dedicated acts, and only where necessary. Thus, according to Bertolini, regulatory intervention should not be over-generalised.[1099] He criticises *inter alia* the distinction made by the Expert Group between high- and low-risk AI on the basis of the significance of the (potential harm), arguing that it will be hard to predict the "tipping point" between these, also because there are no relevant data yet regarding the damages to be expected.[1100] Bertolini furthermore finds that in practice it will be very hard to define "AI-systems" in order to trigger the applicability of the recommended specific liability rules. He advocates to continue the sector-specific (although Union-wide) approach that has been followed so far, in order to remain able to provide tailored

[1095] Ibidem.
[1096] Ibidem, p. 3-4. Furthermore, it is suggested that these producers should not be able to rely on the *development risks-defence* (p. 6.)
[1097] Ibidem, p. 4.
[1098] Ibidem.
[1099] Bertolini 2020, p. 12.
[1100] Ibidem, p. 63.

liability rules. Furthermore, it is argued that generic regulatory intervention might not be in line with principles of proportionality, subsidiarity and better regulation.[1101]

At the same time, Bertolini seems to agree mainly with the material deficits of the current liability regimes summarised by the Expert Group. He observes *inter alia* that fault-based (and contractual) liability rules may become too burdensome for claimants, and may decrease access to justice, due to increased complexity of (AI-) technology. In turn, this could negatively impact trust in technology, and societal uptake thereof.[1102] Also the functioning of the PLD is criticized (to a large extent in line with the Expert Group's vision). The current *product* notion may be problematic as software may not always be covered under its scope.[1103] The notion of *defect* is problematic as it is uncertain which level of *safety* may be expected. Also according to Bertolini, it will be burdensome for victims to demonstrate defectiveness, as this would require access to data, and (expensive) technical expertise to interpret these. Similarly, establishing causality would also become too burdensome for victims.[1104] Establishing causality will furthermore be increasingly complicated as many different factors from different sources might contribute to the origination of damage.[1105]

Furthermore, it is argued that compensation obligations should not be limited to material damages, which do not see to the defective product itself, and excluding immaterial damages.[1106] Also, the development risks defence should be excluded.[1107] Bertolini advises to reform the PLD,[1108] although he also suggests that "policy makers and legislators shall avoid technology neutral regulatory regimes, even with respect to civil liability rules".[1109] Instead, he recommends a thus bottom-up regulation on a case-by-case basis, in conformity with principles that are indicated as "risk management approach".[1110] According to Bertolini, strict or absolute liability is to be preferred over fault liability, which is to be bestowed on the party that is best position to identify; control; and minimize risks.[1111] There should be a one-stop-shop for victims, and the actor who had been held liable should have recourse rights on other potential tortfeasors.[1112] Insurance mechanisms and compensation funds should not be precluded (although compulsory

[1101] Ibidem.
[1102] Ibidem, p. 10.
[1103] Ibidem, p. 57.
[1104] Ibidem, p. 58.
[1105] Ibidem, p. 11.
[1106] Ibidem, p. 59-60.
[1107] Ibidem, p. 58.
[1108] Ibidem, p. 68.
[1109] Ibidem, p. 122.
[1110] Ibidem.
[1111] Ibidem, p. 123.
[1112] Ibidem.

insurance is not considered ideal),[1113] and other types of solutions, such as the "creation of a legal or electronic person",[1114] should not be precluded lightly either.

4.4.4 Proposed Regulation for a Civil Liability Regime by the European Parliament

The European Parliament took account, among many other things, of the EG- and Bertolini's recommendations in its resolution "with recommendations to the Commission on a civil liability regime". The EP acknowledges that there are deficits in the current extra-contractual liability regimes, and states that changes are necessary. Those changes should on the one hand see to creating citizen's trust that digital (AI) technology is safe and reliable, amongst other things through "efficiently and fairly protecting potential victims of harm and damage", [1115] while on the other hand stimulating (investments in) innovation, by leaving enough leeway for especially smaller and medium size enterprises to develop new products and services. The ultimate goal of new civil liability rules, should be to "provide legal certainty for all parties, whether it be the producer, the operator, the affecter person or any other third party".[1116]

In line with the Expert Group's findings (acknowledged by Bertolini), the EP holds that the application of AI-technology could make it very hard, if not impossible, to identify AI-related risks, and eventually causes of accidents, and who was – or should be – in control thereof.[1117] Although the EP considers that a complete revision of the existing (well-functioning) regimes is not needed per se, developments in the realm of AI necessitate a "new, principle-based EU regulation".[1118] Before outlining which principles should be taken into account, the EP also suggests that the PLD must be adapted "to the digital world",[1119] and urges the EC to revise the PLD. In that, the EP suggests that the PLD might best be transformed in a regulation. Also, it is stated that the *products* definition should be clarified "by determining whether digital content and digital services fall under its scope".[1120] The EP advises that the notion of *producer* should cover "manufacturers, developers, programmers, service providers as well as backend operators". The concepts of *damage* and *defectiveness* would need to be updated too (but the EP does not provide further

[1113] Ibidem, p. 123, p. 14.
[1114] Ibidem, p. 14.
[1115] European Parliament 2020a, consideration B.
[1116] Ibidem.
[1117] Ibidem, consideration H.
[1118] Ibidem, consideration 6.
[1119] "… and to address the challenges posed by emerging digital technologies, ensuring, thereby, a high level of effective consumer protection, as well as legal certainty for consumers and businesses, while avoiding high costs and risks for SMEs and start-ups", consideration 8.
[1120] Ibidem.

guidelines on how to do so). Furthermore, the EC should "consider reversing the rules governing the burden of proof for harm caused by emerging digital technologies in clearly defined cases".[1121]

The EP Proposal repeatedly states the importance of striking a balance between the interests of the public in terms of creating trust and allowing for effective damage remuneration possibilities, and incentives for innovation,[1122] and holds that not only legal certainty should be maximised, but also that "over-regulation and red tape must be prevented, as that would hamper innovation in AI".[1123] That being stated, the EP Proposal underscores the principle that citizens who suffer harm caused by an AI-system, should enjoy the same level of protection as citizens who suffer harm caused by a non-AI-system, which is stated to be beneficial for citizen's confidence in the technology,[1124] whilst both material and immaterial damages should be remunerable in principle under a new Regulation.[1125]

The proposal addresses AI-systems. An AI-system is defined in Article 3 (a) as

> *"system that is either software-based or embedded in hardware, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals".*

Autonomy is defined (sub (b)) as

> *"an AI-system that operates by interpreting certain input and by using a set of pre-determined instructions, without being limited to such instructions, despite the system's behaviour being constrained by, and targeted at, fulfilling the goal it was given and other relevant design choices made by its developer".*

Thus, distinctive features of an AI-system compared to a non-AI-system seem to be a capacity to extract data from its environment and to analyse and interpret those data (intelligence), and the fact that they can operate, although within certain design-constraints, without being limited to pre-determined instructions (autonomy). The Proposal furthermore distinguishes between "high-risk" and "non high-risk" AI-systems. AI-systems are to be determined "high-risk" when there is

> *"a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can be reasonably*

[1121] Ibidem.
[1122] Ibidem, principle 4.
[1123] Ibidem, principle 3.
[1124] Ibidem, principle 7.
[1125] Ibidem, principle 8, and principle 1.

expected; the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision making, the likelihood that risk materialises and the manner and the context in which the AI-system is being used".[1126]

High-risk AI-systems must be listed in an Annex.[1127] All other AI-systems qualify as non-high-risk. The addressees of the obligations of the EP proposal are "operators", who might either be "frontend-" or "backend-operators. A frontend-operator is the one who

"exercises a degree of control over a risk connected with the operation and functioning of the AI-system and benefits from its operation",[1128]

comparable with the level of control a "traditional" car-owner has over his vehicle.[1129] A backend-operator is the one

"who, on a continuous basis, defines the features of the technology, and provides data and an essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system".

Thus, the entity who can exercise remote-control over a system, whose database is used, or who provides maintenance, updates or support, must be qualified as backend-operator. Article 4(1) regulates that an operator

"of a high-risk AI-system shall be liable for any harm or damage[1130] *that was caused by a physical or virtual activity, device or process driven by that AI-system".*

The EP Proposal does not stipulate how causation should be established, or on whom the onus of proof rests. However, article 4(3) implicates that operators cannot exonerate liability on the basis of illustrating their due diligence, or that the damage came into existence as a result of the autonomous operation of the system. The only possibility for operators of high-risk AI-systems is to prove that damage was caused by force majeure. Frontend operators need to insure the operations of their high-risk AI-systems, and backend operators should also take out insurance

[1126] Article 3(c) EP Proposal. The EC is to keep this list, and update this by means of delegated act.
[1127] Article 4(2) EP Proposal. In a previous version (European Parliament 2020), a concept-annex has been attached, which included *inter alia* "Vehicles with automation levels 4 and 5 according to SAE J3016", as well as unmanned aircraft, Autonomous Traffic Management Systems, Autonomous robots and Autonomous public places cleaning services.
[1128] Article 3(e) EP Proposal.
[1129] Consideration (10) to the EP Proposal; "control is defined in 3(f) as "any action of an operator that influences the operation of an AI-system and thus the extent to which the operator exposes third parties to the potential risks associated with the operation and functioning of the AI-system"
[1130] This may include anything with an "adverse impact affecting the life, health, physical integrity of a natural person, the property of a natural or legal person or causing significant immaterial harm that results in verifiable economic loss", as follows from article 3(i). The extent of damage compensation is specified in article 5.

covering its services, on the basis of article 4(4). The amount of compensable damages is capped on € 2 million in case of death or harm caused to "the health or physical integrity of an affected person", [1131] and on € 1 million in case of "significant immaterial harm that results in a verifiable economic loss or of damage caused to property".[1132]

Operators of non-high-risk AI-systems should be liable on the basis of "fault" towards affected persons "for any harm or damage that was caused by a physical or virtual activity, device or process driven by the AI-system".[1133] The operator can invoke a defence if he can prove that damage is not attributable to him on the basis of fault. He can do so through proving that the AI-system was activated without his knowledge, and beyond his control, or by showing he acted with "due diligence" regarding the selection, operation, monitoring and maintaining the system – including the provisioning of available updates.[1134]

Operators cannot escape liability stating by that the harm was caused by an autonomous decision, although a force majeure defence may be relied on. An operator is furthermore liable for damage as a consequence of activity of a "third party that interfered with the AI-system by modifying its functioning or its effects […] if such third party is untraceable or impecunious".[1135]

The operator's liability can be reduced (or avoided) if he can prove contributory negligence at the side of the affected person.[1136] In order to substantiate a contributory negligence defence, an operator may "use the data generated by the AI-system" in accordance with the GDPR or other relevant data protection laws.[1137] Also the affected person may "use such data as a means of proof or clarification in the liability claim".[1138] Operators are jointly and severally liable, and if a frontend operator also is the producer in sense of the PLD, the proposed Regulation is to prevail over the PLD-provisions.[1139] The PLD does however apply (in full) to backend providers who qualify as producers in sense of the PLD. When there is only one operator, and that operator is also the producer in sense of the PLD, the provisions of the EP proposal apply, prevailing over the PLD.[1140]

[1131] Article 5(1)(a) EP Proposal.
[1132] Article 5(1)(b) EP Proposal. Article 6 proposes limitation periods, of 30 years regarding physical harm (including death), and of 10 years regarding property damage or immaterial harm.
[1133] Article 8(1) EP Proposal.
[1134] Article 8(2) EP Proposal.
[1135] Article 8(4) EP Proposal.
[1136] Article 10(1) EP Proposal.
[1137] Article 10(2) EP Proposal.
[1138] Ibidem.
[1139] Article 11 EP Proposal.
[1140] Ibidem. Recourse rights are addressed in article 12.

4.5 CONCLUSION

In this Chapter, I illustrated the outlines of the regulatory regimes regarding extra-contractual liability for defective products, and traffic accidents as apply in the Europe, and more specifically The Netherlands, France and England – with a focus on accidents in which (defective) AVs can be involved.

It showed that both the product liability framework and the fault-based traffic liability rules (of The Netherlands, and to some extent England) may implicate several uncertainties and problems for victims who would seek compensation from a producer, or an owner, a keeper or a "driver" of an AV. Many of these issues relate to establishing a norm-violation, i.e. a *defect* or *fault* respectively, and *causality* between the norm violation and inflicted damage. It was observed that this requires access to AV- and accident related data, and specific expertise of the technology in order to successfully claim compensation. At the same time, producers under the PLD have ample defence opportunities, as they can invoke for example the *development risk* and *later existence* defences in order to limit their liability risks.

This Chapter concluded with a view into the potential future, illustrating the contours of the European Parliament's Proposal regarding a Civil Liability Regulation for AI. This proposal holds a risk-liability regime for operators of high-risk AI-systems, likely including AVs. The most prominent issues for victims that would result from the PLD, or the fault-based liability regimes would be diminished under the proposed regime. However, this *sui generis* regime, which is to operate alongside the PLD, may implicate several other problems for innovators.

It must be noted that the EP-proposal must still be regarded as a "recommendation" to take further regulatory steps. However, the position of the EP regarding the necessity to change the currently liability rules in view of the development and deployment of AI-systems has become clear with its proposal. Also clear is that the EP is in favour of creating more legal certainty through the instalment of strict liability rules for operators of high-risk AI-systems, and stricter rules for producers of (any) AI-system, as well as stricter fault-liability rules for operators of "regular" AI-systems. According to the EP, this can be motivated from the citizen's perspective that their losses which can be correlated with the application of risky AI-systems should be compensable, (at least) to similar extents as victims of non-AI-related damage are currently protected. I further reflect on the ways in which civil liability rules might need to be adapted – also in relation to the EP recommendations, in Chapter 8 and Chapter 9, in terms of the *factors* indicated in section 3.4.2 and 3.4.3.

Chapter 5. PERSONAL DATA PROTECTION REGULATION IN THE EU

5.1 INTRODUCTION

5.1.1 GENERAL OVERVIEW

The subject of this chapter is the regulatory framework regarding personal data protection in the European Union. The concept of personal data protection is relatively new, especially when compared to the liability concepts that have been studied in the foregoing chapter. This subject gained broad societal attention in the second half of the 20th century.[1141] The regulatory framework in the EU substantially grew from the 1950's onwards. Personal data protection has *inter alia* been included in the Charter of Fundamental Rights of the EU in 2012,[1142] and was eventually codified in the General Data Protection Regulation,[1143] which came into force Unionwide on 25 May 2018. The extension of the regulatory framework, which comprises many more sources than those mentioned above,[1144] was – at least partly – fuelled by technological developments leading to increasing possibilities of large scale processing of personal data,[1145] which will be illustrated in section 5.1.4.

The GDPR holds the most important body of rules regarding personal data processing in the EU, and applies *inter alia* to the development and deployment of AVs.

> The operation of AVs will involve processing of personal data processing on a massive scale. As further illustrated in section 5.2.2, the operation of AVs requires for instance the processing of *location data* of vehicles (especially when AVs are to communicate with other AVs on the road, or other parts of road infrastructure for optimal operation of these vehicles), and information regarding *vehicle use* for maintenance purposes, as well as *sensor*- and sometimes *camera* data, which are all personal data in sense of the GDPR, as individuals can be identified on the basis of such information. Furthermore, personal data will likely be processed for commercial purposes, such as car-rental, or pay-as-you-drive models for AVs, and AV-behaviour data are likely to be stored in event data recorders or comparable mechanisms, for *inter alia* engineering- and perhaps even insurance purposes. Also processing data regarding

[1141] See Kranenborg & Verhey 2018, p. 4.
[1142] Charter of Fundamental Rights of the European Union, *OJ C*236, 26.10.2012, p. 391-407 (Charter).
[1143] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJ* 119, 4.5.2016, p. 1-88 (GDPR).
[1144] See section 5.1.4.
[1145] See Kranenborg & Verhey 2018, p. 5-7; Blok 2002, p. 118.

the personal preferences of an AV-user in order to accommodate personalised climate, or infotainment settings involves personal data processing triggers applicability of the GDPR.[1146]

Therefore, I will explain under which circumstances the GDPR applies in section 5.2.2 and 5.2.3, and I will sketch the most important obligations under the GDPR for the entities determining means and purposes of AV-related personal data processing (*controllers* in terms of the GDPR, see section 5.2.4, 5.2.5 and 5.2.7), and entities processing personal data on behalf of those controllers (*processors*, see section 5.2.8), as well as the rights of the persons to whom such personal data relate (*data subjects,* section 5.2.6). Special attention is paid to responsibility and liability for compliance with the rules, which can be enforced through both public (section 5.2.10) and private enforcement-mechanisms (section 5.2.11) that have been created under the GDPR. In order to illustrate my review of the applicable GDPR-rules, I will use examples that relate to (existing and future) AV appliances, such as personal data processing through black boxes in AVs, and vehicle-to-vehicle and vehicle-to-infrastructure communication technologies as introduced in section 2.3. I have chosen to focus on such appliances, as these can *inter alia* be used to prevent accidents as much as possible, and also to aid in establishing the causes of accidents when these have happened, which is often necessary in order to claim (or defend against a claim) damages resulting from AV accidents, as was stated in the previous Chapter, and will be further elaborated in section 5.2.11. Also other AV-related examples are given, in order to illustrate the more generic compliance-obligations for entities processing personal data, or when this follows from (the scarcely available) guidance given by the data protection authorities or judiciary on these or related subjects.

As stated above, and further explained in section 5.1.4, the main object of my research in this chapter is formed by the GDPR, the case law of the CJEU and policy rules of the European Data Protection Board in section 5.2. Where the GDPR rules contain open norms that can be relevant for my case study, national laws of The Netherlands, England and France, as well as policy guidelines of local supervisory authorities and case law are occasionally illustrated.

Before diving into the material contents of the regulatory framework under review, attention is given to the concepts of privacy- and personal data protection in section 5.1.2. Some understanding of general concepts of privacy is necessary on order to review the functioning of the current data protection framework as applicable to AVs, in terms of factors *legal certainty, stringency, flexibility*, *risk* and *trust*. Rules regarding personal data protection are seen to be derived from, and forming part of, the protection of the fundamental right to privacy.

[1146] See also Glancy 2012, who gives a useful overview of potential forms of personal data processing through AVs, om p. 1175-1176.

Privacy protection relates to the classic idea that the rights of individuals should be shielded from public interference, and has close ties with other fundamental rights that oppose a 'private sphere' to a 'public sphere', such as the freedom of communication, freedom of religion,[1147] as well as intellectual property.[1148] It is held that within a private sphere (opposed to a public sphere), one does in principle (notwithstanding certain justified exceptions – see further section 5.1.3) not have to tolerate interferences from third parties,[1149] and is (again to a certain extent) free to do what he wants.[1150] Such a private sphere can be of a physical nature (for instance the body or a home are examples of physical private spheres), or of a 'virtual' nature, including for example thought, religion, ideas and information or data relating to a person. Traditionally, the fundamental freedoms *(inter alia* communication freedom and freedom of religion) saw to the protection of citizens from interference by the state. However, facilitated by the technological developments from the past three decades onwards, the possibilities for private entities to enter into the private spheres of other private entities also increased. This is reflected *inter alia* in article 8 of the Charter and the GDPR, which provide data-protection rules that are applicable to any entity, allowing citizens to enforce their rights against either governmental or civil entities. It needs to be mentioned in this respect, that the GDPR provides that infringement of the GDPR-rules can lead to civil, extra-contractual liability (thus: tort) of the non-complying entity towards the individual whose rights are infringed.[1151]

This chapter ends with an interim conclusion in section 5.3, summarizing the key fundaments and provisions that have been reviewed.

5.1.2 PRIVACY AND PERSONAL DATA PROTECTION

In order to understand the functions and purposes of privacy- and personal data protection, it is necessary to explore the meanings of these two concepts. Furthermore, understanding these concepts is also necessary for providing answers to the question how the regulatory framework on personal data protection can potentially be optimised to better facilitate innovation in the field of AVs, and acceptance thereof by EU-citizens. Privacy and personal data protection are often used

[1147] See Blok 2002, p. 11.
[1148] Intellectual property is enshrined in article 17(2) the Charter of Fundamental Rights of the European Union, and in article 1, First Protocol to the ECHR; see furthermore Geerts P.G.F.A., & Verschuur, A.M.E. (eds.), *Kort begrip van het intellectuele eigendomsrecht*, Deventer: Wolters Kluwer 2018, p. 24-26, who conclude on p. 26: "Dus ook IE-rechten zijn grondrechten!" (translated as "so also IP-rights are fundamental rights!").
[1149] See Blok 2002, p. 11, 17, 25.
[1150] See also Glancy 2012, p. 1192, who clarifies that "autonomy privacy" (which I assume to be compatible with the "private sphere" introduced above) has a positive side and a negative side. The positive side holds that one is free "to take action and affirmatively do something, such as [to] make choices". The negative side holds that an individual has "freedom from external interferences".
[1151] Article 82 GDPR, see 5.2.11.2.

as similar notions, although they are not the same. Both notions are debated in literature.[1152] The works by Blok (2002) and Solove (2009) contain thorough overviews and analyses regarding the different lines of reasoning in the academic literature on privacy – and personal data protection. In the following section, *inter alia* their analyses are used to illustrate the diversity of opinions regarding the definition of privacy, and their respective re-conceptualisations thereof, also in order to introduce some similarities and differences between *privacy* and *personal data protection*.[1153]

Solove distinguishes six different categories of interpretations of the notion of privacy.[1154] First, he mentions one of the most "famous" concepts coined by Warren & Brandeis, in 1890:[1155] "the right to be let alone". [1156] They found that the then new technology of "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life"; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[1157] According to them, privacy is an individual right, "like the right not be assaulted or beaten, the right not be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed".[1158] Privacy must be seen as forming part of "the more general right to immunity of the person, -- the right to one's personality".[1159] Whereas Solove recognizes the importance of the Warren & Brandeis' concept, he observes that their take on privacy is too broad, and that it contains a "vague conception of privacy".[1160] It is furthermore argued that although the concept by Warren & Brandeis recognized that technological developments increased the importance of the right to be let alone, it cannot be easily applied to "modern-day intrusions of privacy". [1161] Solove then expresses the similar criticism regarding the second concept he mentions, that of "limited access to the self" as an explanation of privacy.[1162] That concept entails that there is an individual right to exclude others

[1152] It is even stated that privacy cannot be defined at all. See for instance Berlee 2018, p. 135 and her references there. See also Glancy 2012, p. 1187 ff.
[1153] See furthermore Glancy 2012, who illustrates that AVs may be relevant both in terms of personal data protection, and the more general notion of privacy, as the deployment of AVs interferes with the 'personal sphere' of citizens, and it reduces 'human' autonomy in operating a car (see for example p. 1186-1188).
[1154] Solove 2009, p. 12-13. See for another, chronological, overview Berlee 2018, p. 136-150.
[1155] Ibidem, p. 15-18. Another conceptualization is illustrated in Allen 2011. She distinguishes "physical privacies", comprising "seclusion and concealment" (p. 29-96), from "information privacies", comprising "confidentiality and data protection" (p. 99-194).
[1156] Warren, S., and Brandeis, L., "The Right to Privacy", Harvard Law Review 15 December 1890, Vol. IV no. 5, available via https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (last accessed 3 June 2020, Warren & Brandeis 1890).
[1157] Warren & Brandeis 1890, 4th paragraph.
[1158] Ibidem, 14th paragraph.
[1159] Ibidem, 16th paragraph.
[1160] Solove 2009, p. 18.
[1161] Berlee 2018, p. 139.
[1162] Ibidem, p. 20.

from access to the private realm.[1163] Solove interprets this concept as comparable to the right to be "let alone", and holds that "[w]hitout a notion of what matters are private, limited-access conceptions do not tell us the substantive matters for which access would implicate privacy".[1164] A more demarcated (third) concept is "privacy as secrecy". Under that concept, privacy is infringed when information is published which had been concealed before, against the will of the person to which the information relates.[1165] This is closely related to the (fourth) concept of "control over personal information", which according to Westin holds that "Privacy is the claim of individuals, groups, or institutions to determine for themselves how, and to what extent information about them is communicated to others".[1166] Privacy-as-control is also referred to as *informational privacy* in literature.[1167] Solove comments that this is too narrow, as it excludes non-informational aspects of privacy, and often is too vague, as it is not always clear which types of information are to be protected, and what 'control' entails.[1168] Fifthly, Solove mentions that privacy is sometimes seen as the protection of "personhood". In line with Warren and Brandeis' "inviolate personality", this personhood is seen to relate to "those attributes of an individual which are irreducible in his selfhood",[1169] and holds that integrity of personality, or individuality, must be protected. Another related term is "identity", according to build identity, it is held that autonomy, or privacy, is necessary.[1170] Again, it is observed that "personality" and "individuality" are often not satisfactorily defined and remain very vague.[1171] Solove concludes with the concept of privacy as a form of intimacy, in which privacy is seen as "essential not just for individual self-creation, but also for human relationships".[1172] This concept, he comments, is both to broad as "intimacy" is often not adequately defined, and it fails to appreciate that there are other aspects to privacy that have nothing to do with intimate relationships.

[1163] He refers *inter alia* to Godkin (Godkin, E.L., "Libel and Its Legal Remedy", *Journal of Social Science*, 1880, vol. 69, no. 80); Bok (Bok, S., *On the Ethics of Concealment and Revelation*, New York: Knopf Doubleday 1983, p. 10-11); and Gross (Gross, H., "The Concept of Privacy", *New York University Law Review* 1967, vol. 43, no. 34, p. 35-36); as advocates of the "limited-access concept".
[1164] Ibidem.
[1165] See Posner, R.A., *The Economics of Justice*, Cambridge (US): Harvard University Press 1981, p. 272-273, cited by Solove 2009, p. 21.
[1166] Solove, 2008, p. 24, citing Westin, A., *Privacy and Freedom*, New York: Athenum 1967, p. 7. He further refers *inter alia* to Miller, A.R., *The Assault on Privacy*, Michigan: University of Michigan Press 1971, p. 25; and Fried, Ch., "Privacy", *Yale Law Yournal*, 1968, vol. 77, no. 465, p. 483-483. See also Berlee 2018, p. 139-142.
[1167] See Berlee 2018, p. 139, 151.
[1168] Ibidem, p. 25-26.
[1169] Solove 2009, p. 30, referring to Freund, P., Address at the American Law Institute, 52nd annual meeting 1975, p. 42-43.
[1170] See Berlee 2018, p. 144, referring *inter alia* to Hildebrandt, M., "Profiling and the identity of the European citizen", in Hildebrandt, M., and Gutwirth, S., *Profiling the European Citizen*, Dordrecht: Springer 2018, p. 303-344.
[1171] Ibidem; see also Berlee 2018, p. 145.
[1172] Ibidem, p. 34. He refers *inter alia* to Inness, J., *Privacy, Intimacy and Isolation*, Oxford: Oxford University Press 1996.

All in all, Solove concludes that there are many conceptions of privacy, but that they all fail to address a common denominator. Furthermore, the concepts he identified are often too broad, as notions of "intimacy", "personhood", "private realm" or "personality" are not adequately defined, or too narrow, when these for instance only relate to "secrecy" or "personal information".

Solove then provides us a new approach, which aims to characterize privacy through an identification of a web of different, yet related privacy problems. These problems are different from each other as they do not share a common denominator, but bear some (or more) "family resemblances", i.e. that these problems share certain elements with other problems.[1173] The problems he indicates, "impede valuable activities that society wants to protect, and therefore society devises ways to protect [us from] these problems".[1174] The protections against the problems Solove identified, must be seen as "privacy". These problems (situations that create "harm to individuals and society")[1175], can be comprised in four categories.[1176] The four categories relate to three forms of activities that may pose privacy issues in terms of data processing (information collection, processing and dissemination), and "invasion", which does not (always) involve data processing, but rather sees to physical and psychological intrusion. Privacy problems regarding information collection include for example surveillance, or interrogation of people.[1177] Information processing can be problematic when decisions are made on the basis of aggregated data concerning a person, when identification is required (but not always necessary) to take part in certain aspects of social life, when personal data are insecurely processed or stored, when data are processed without consent, or beyond the control of a person they relate to.[1178] Information dissemination could detriment privacy when for example confidentiality is breached or threatened to be breached, or when personal data are disclosed without due authorization, or when the disclosed information is false.[1179] Such privacy problems can cause several forms of harms, including (less likely) physical injuries; financial or property loss; and (more likely) reputational harms; emotional and psychological harms; relationship harms; vulnerability harms (i.e. a risk that someone gets harmed in the future); chilling effects (i.e. the likeliness that people refrain from being engaged in certain activities); and power imbalances.

[1173] Solove 2009, p. 171, 174. Solove uses the family-resemblance concept developed by Wittgenstein, in Wittgenstein, L., *Philosophical Investigations*, Basil Blackwell 1958.
[1174] Ibidem, p. 174.
[1175] Ibidem.
[1176] Solove 2009, p. 10-11.
[1177] Ibidem, p. 104.
[1178] Ibidem.
[1179] Ibidem, p. 105.

The idea that privacy is hard to conceptualize and must be dynamically approached in for instance a problem-based way, is generally acknowledged in literature.[1180] Critique to problem-based approaches such as provided by Solove is also given, i.e. that "these scholars' focus on the ways in which privacy can be infringed and the legal problem which must be solved is largely reactive. They focus on specific harms which are already occurring and which must be stopped, rather than over-arching protections that should be instituted to prevent harms".[1181]

Blok also acknowledges that many authors struggle with the vagueness of the concept of privacy and the associated notions.[1182] However, he does provide a top-down definition of the kind that Solove criticizes but that in my opinion provides – at least for a large part – enough clarity and precision to be meaningful and workable in terms of this study, which also sees to protection of privacy and thus to *prevent* harms indicated by *inter alia* Solove. Thus, while the problem-based approach sketched by Solove is usable to identify different problems that can be associated with privacy, and to identify (types of) harms that could result from such problems, the approach by Blok is usable to understand what privacy protection through law and policy should entail, in order to prevent (Solove's) privacy problems as much as possible, and to repair damage should privacy problems have occurred.

Blok provides a classification of privacy that consists of four elements. First, he observes that privacy can be seen as a *subjective right*. It is a right that every individual has, which equips the right holder to exercise control over the protection of his private sphere ("persoonlijke levenssfeer").[1183] In that, privacy can be compared to other rights that see to the protection of a *private sphere* of citizens (which can be opposed to a *public sphere*), such as communication freedom, and the freedom of religion.[1184] On the basis of the subjective right of privacy, anyone may decide in principle whether or not to allow someone else (including government) to access the protected personal sphere. Second, Blok illustrates that privacy is a right *in rem* (rather than a right *in personam*).[1185] This entails that rights can be enforced towards anyone. The object of the privacy right is, according to Blok, as stated, the personal sphere of citizens. In principle, all outsiders – including government and other people – have to refrain from intrusion in the personal sphere, and the privacy right offers a means of protection. Third, privacy rights must be seen as *personality rights* ("persoonlijkheidsrechten").[1186] A characteristic of personality rights, is

[1180] See Berlee 2018, p. 145-146; see also Hildebrandt, M., "Privacy & Identity", in Claes, E., Duff, A, & Gutwirth, S., *Privacy and the criminal law*, Antwerp/Oxford: Intersentia 2006, p. 61-104; and Finn, e.a. 2013, p. 4-7.
[1181] Finn e.a. 2013, p. 6.
[1182] Blok 2002, p. 9.
[1183] Ibidem, p. 16
[1184] Ibidem, p. 11.
[1185] Ibidem, p. 24.
[1186] Ibidem, p. 26-32.

that they are inherent to the personality, and that they can therefore not be assigned (or passed on) to others. Fourth, Blok observes that privacy is a *negative right*, i.e. a right to non-interference, rather than for instance an obligation.[1187]

As stated, Blok recognizes that the object of privacy protection, the *private sphere*, is observed as rather vague and open.[1188] However, Blok argues that the constitutions of the jurisdictions that he reviewed in his dissertation (the United States and The Netherlands) as well as international human rights treaties, do provide the necessary guidance to illustrate what the private sphere encompasses – which is to be protected by the right to privacy. The elements that are classically comprised within the *private sphere* in terms of the right to privacy, are the home, the body, family life, correspondence and the intimate life.[1189] Furthermore, personal data protection is often included within these elements – also in legislation. Blok contends that this is a problem: "the foremost exception to the relatively strict delineation of the private sphere is the use of the concept of privacy in the field of data protection".[1190] As personal data protection sees not only to the 'classic' elements, but rather to all aspects of information that may (in)directly relate to an individual, the scope of the concept is massively extended by including personal data protection as an element. Another point of critique, is that personal data protection is not as "strict" right as the protection of the home, family life, intimacy and correspondence. In fact, rules on personal data protection by default *allow* interference with the private sphere by others, as long as certain formalities are taken into account by default,[1191] whereas the more classic privacy rights *disallow* such interference by default.

From a conceptual point of view, it can be argued that 'classic' privacy rights, i.e. subjective rights regarding non-interference of home, body, family life, correspondence and intimate life, that can be enforced against anyone in principle, and cannot be assigned to others, must be distinguished from informational privacy, i.e. personal data protection. I share the observations by Blok and Solove, that personal data protection is of another – yet related – nature than protection of the classic privacy rights. It is related in the sense that the storage, collection and dissemination of personal data form a potential risk for the protection of the personal sphere of citizens. It is different in the sense that personal data protection rights are not as strict as the classic privacy rights, and see to the creation of a form of control over, and insight in the access to personal data by others than the data subject, rather than a right of "non-interference".

[1187] Ibidem., p. 36.
[1188] Ibidem, p. 321.
[1189] Ibidem, p. 323-324.
[1190] Ibidem, p. 326.
[1191] Ibidem; see also section 5.1.4.

In the following sections, the informational privacy aspects of AV technology as regulated in the EU framework on personal data protection, more concretely the GDPR, will form the starting point of my research. This is necessary to assess the potential influence of the regulatory framework regarding personal data protection on innovation and acceptance in the field of AV-technology, in terms of the factors identified in section 3.4, and to make potential improvement-recommendations. As will be shown, my review hereunder includes at some points also references to 'larger' concepts of privacy, which are occasionally elaborated as well. As the focus will be on informational privacy, I will first review the meaning and functions of personal data protection in the next section.

5.1.3 FUNCTIONS OF PERSONAL DATA PROTECTION

As highlighted in the foregoing section, there are many different conceptions on the notion of privacy. The identification of the values and functions of privacy are almost equally diverse. However, some observations can be made regarding the general functions that the 'different-yet-related' concepts of privacy may serve.

Some authors highlight individual values that underly privacy. It is for instance argued that privacy serves the psychological, physical, social and moral well-being of citizens.[1192] This can be related to the approach of 'liberty' described by Mill, Locke and Rawls, regarding the importance of self-determination and self-realisation for individuals.[1193] As DeCew illustrates, "loss of privacy can diminish freedom" of an individual.[1194] Westin also underscores the importance of privacy for self-realization, and in similar vein, Freund illustrates that "privacy offers a shelter for the loosening of inhibitions, for self-discovery and self-awareness, self-direction, innovation, groping, nourishment for a feeling of uniqueness and a release from the oppression of commonness".[1195] Thus, it is held that a certain amount of protection of a private sphere is necessary for people to be free in the sense that they are not disturbed by others, which can in turn foster *inter alia* self-realisation, creativity and innovation. This idea is underscored by the potential *chilling effect* that might occur when privacy is not adequately protected. Solove for instance points out that people

[1192] Solove 2009, p. 79, referring *inter alia* to a report by the US Department of Health, Education & Welfare, "records, Computers and the Rights of Citizens", 1973, p. 33.
[1193] See for instance Rössler 2005, p. 27-34, 83-86 and 216-217.
[1194] DeCew 1997, p. 58.
[1195] Freund, P.A., "Privacy: One Concept of Many", in: Pennock, J.R., & Chapman J.W., *Privacy, Nomos XIII: Yearbook of the American Society for Political and Legal Philosophy,* New York: Atherthon 1971, cited in Solove 2009, p. 79.

may refrain from engaging in certain activities when they know that their behaviour is, or – even worse – can be monitored by government.[1196]

Besides individual values, privacy is said to serve societal and democratic goals.[1197] A protected private sphere is seen to be essential for the exercise of other democratic rights such as communication freedom. As Gavison underscores,

> "[p]rivacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy. […] Thus, to the extent that privacy is important for autonomy, it is important for democracy as well".[1198]

Furthermore, privacy enables people to engage in debates in which they can hold and express, even anonymously, opinions that differ from the common and popular views. Again, it might have a chilling effect on such debates, and thus the 'free marketplace of ideas',[1199] and therefore democracy, when people do not a certain protection of their private spheres.[1200] In this line of reasoning, it can also be argued that too little privacy protection may negatively impact communication freedom in general, i.e. the freedom to gather, to hold and to express ideas and information. Where limited communication freedom leads to limited availability of information

[1196] See Van der Sloot 2018, p. 422-426, who refers to Bentham J., *Panopticon: or The inspection-house*, Dublin, 1971 and Foucault, M., *Surveiller et punir: naissance de la prison*, Paris Gallimard 1975; and who points out that the ECtHR seems to accept "this doctrine in certain cases relating to Article 8 ECHR, primarily when they regard surveillance measures, but also in relation to laws that discriminate or stigmatize certain society" (p. 422-423); Solove 2009, p. 178, who inter alia shows that the chilling effect notion is also recognized in US law. He refers to the interesting article by Schauer, F., "Fear, Risk and the First Amendment: Unravelling the 'Chilling Effect'", *Boston University Law Review* 1978, Vol. 58:685, p. 685-732. Schauer also recognizes that courts assume chilling effects. Much empirical evidence on chilling effects in relation to (informational) privacy protection cannot be easily found in literature Solove and Van der Sloot cited. However, hints of such evidence are shown by Penney, J.W., "Internet surveillance, regulation and chilling effects online: a comparative case study", *Internet Policy Review – Journal on internet regulation* 26 May 2017, vol. 6, issue 2. Penney conducted a survey under a "relatively representative" pool of US based internet users, and suggests repeating and upscaling the conducted research. It is observed in the study that "at state and non-state action, such as laws, regulations, or state actions like surveillance, can, and do, have a chilling effect on people's activities online". Furthermore, it is observed that "greater chilling effects arise when individually targeted by legal threat […] while government surveillance […] was consistently associated with the second highest level of chilling effects". Also, it is stated that ", findings suggest a range of other factors, likeeducation, legal training, and knowledge of the US National Security Agency's online activitiesalso influence the nature and extent of regulatory chilling effect" (all citations from the conclusions by Penny, on p. 22).
[1197] See for instance Solove 2009, p. 91-93; Berlee 2018, p. 142.
[1198] Gavison, R., "Privacy and the Limits of Law", *The Yale Law Journal* 1980, vol. 89, no. 3, p. 455.
[1199] Mill, J.S., *On liberty and other essays*, Oxford: Oxford paperbacks 1998 (republishing the 1859-edition).
[1200] See also Berlee 2018, p. 145.

and ideas within the public domain,[1201] this in turn could lead to limited 'fuel' for creativity and innovation on both the individual and the societal level.[1202]

At the same time, it must be observed that the value of privacy protection is not absolute. Unrestrained protection of private spheres may for instance lead to a "retreat from society",[1203] and may cloak unwanted and even criminal behaviour. Furthermore, it must be acknowledged that privacy may collide with other fundamental rights, such as communication freedom, and that when privacy is to prevail 'by default' over other fundamental rights, this could lead to disbalance with a negative impact on the functioning of democracy. Moving slightly away from the more abstract general values and functions of privacy described above, it is illustrative to refer again to potential problems and 'harms' when (informational) privacy is *not* adequately protected as described by Solove and introduced in section 5.1.2. An important function of privacy protection is, or should be, the prevention of problems related to unlimited data collection, uncontrolled processing and unrestrained dissemination, which could for instance lead to data breaches resulting in public accessibility of highly sensitive personal information, which in turn could cause for example financial, psychological and even physical harm.

> Some examples: Financial harm may for instance occur when someone's credit card details are leaked from a database used by an AV-rental company to charge money for pay-as-you-drive concepts. Psychological, or even physical harm could be inflicted upon people, when for example their opinions, which are generally qualified as unpopular, subversive or even undermining, are made publicly known. Stalkers may misuse inappropriately protected location data of certain AV-users.[1204] The reputation of a public figure may be harmed, when certain details of his or her intimate relationships are revealed to the public. Burglars can take advantage of a data breach providing insight in the personal diaries of home owners. Employers may discipline their employees when it shows from insufficiently protected GPS-data that their lease-vehicles are used for other purposes than those desired by the company. Social media-users may be prevented from reading information that the platform algorithm deems 'irrelevant' based on the profiles that were automatically created on the basis of their 'search and like'-behaviour on or outside the platform in the past. Someone may be denied a

[1201] See Belder, De Cock Buning & De Bruin 2015, p. 106-107.
[1202] See for instance P. Uhlir, *Draft Policy Guidelines for the Development and Promotion of Public Domain Information*, Unesco doc. CI-2003/WS/2, 1.1, 2003, cited in G. Davies, "The public interest in the public domain", in Ch. Waelde & MacQueen (eds.), *Intellectual Property – The Many Faces of the Public Domain*, Cheltenham: Edward Elgar Publishing 2007; and Frosio, G., "1. Communia and the European Public Domain Project: A Politics of the Public Domain", in Dulong de Rosnay, M., and De Martin, J.C. (eds.)., *The Digital Public Domain – Foundations for an Open Culture,* Cambridge: Open Book Publishers 2012.
[1203] Solove 2009, p. 80.
[1204] See Glancy 2012, p. 1196.

loan, when it shows from his online behaviour that he has recently visited an online gambling website. Identity-theft may occur when biometric details used to authenticate AV-users and to 'unlock' those vehicles, are stolen from a database in which such data are centrally stored.[1205]

In anticipation of section 5.1.4 and 5.2, it can be stated that the GDPR for instance does *inter alia* indeed see to the prevention of problems regarding personal data processing (encompassing the collection, storage and dissemination stages,[1206] indicated by Solove) and the reparation of damage that results from non-observance of the norms.[1207]

Thus, from the myriad of privacy values indicated in literature, four main threads can be derived. The first is that privacy serves individual goals aimed at psychological, physical, social and moral well-being of citizens, and regard *inter alia self*-realisation, autonomy and creativity. Secondly, privacy is necessary for the well-functioning of democracy. Thirdly, absence of adequate privacy protection could result in *chilling effects* and may have a negative impact on innovation. Fourthly and more concretely regarding informational privacy, its value is to prevent problems related to collection, storage and dissemination of personal data.

5.1.4 Regulatory Framework in the EU

5.1.4.1 Introduction

The regulatory framework regarding personal data protection in the European Union consists of several layers and stems from multiple sources. The 'top layer' is formed by the two human rights catalogues that apply in the EU.[1208] These are Charter of Fundamental Rights (illustrated in section 5.1.4.2) and the European Convention on Human Rights (addressed in section 5.1.4.3). The second layer is formed by secondary union legislation, of which the General Data Protection Regulation (addressed in section 5.1.4.4 and elaborated in more detail in section 5.2) is most important in terms of this study. One of the other important sources of secondary EU legislation in terms of AV-

[1205] See also Glancy 2012, p. 1196.
[1206] See *inter alia* the 39th recital to the GDPR, and article 5.
[1207] GDPR, recital 146 and article 82.
[1208] Of course, there are more human rights frameworks that apply in the Member States of the European Union which address privacy protection, such as the Universal Declaration of Human Rights of 1948 (article 12) and the UN International Convenant on Civil and Political Rights of 196 (article 17). Specifically regarding personal data protection, the Strasbourg Treaty of 28 January 1981 must be mentioned, which is currently ratified by 51 countries including all EU Member States. Also the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 must be noted. All these instruments are important, although the instruments elaborated in the main text of these sections are of more actual and practical value, as these are nowadays most used by legislators and judiciary in the EU Member States. See for example Berlee 2018, p. 169 on the OECD Guidelines; p. 169-170 on the Universal Declaration of Human Rights; p. 170-171 on the ICPR; and p. 179-182 on Convention 108; and Kranenborg & Verhey 2018, p. 22 on the Strasbourg Treaty.

data processing, is *inter alia* the ePrivacy Directive (to be replaced by a regulation),[1209] mentioned in 5.1.4.5. Under the GDPR, certain regulatory aspects are delegated to the Member States. This is the third layer. Furthermore, as a fourth layer, the GDPR contains many open norms, which are to be filled in by *inter alia* respective stake holders and to be accredited by supervisory authorities (addressed in section 5.1.4.4).

5.1.4.2 CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

The Charter of Fundamental Rights of the European Union (CFR)[1210] was adopted in 2000, and entered into force in 2009 by the Lisbon Treaty.[1211] It has the same legal value as the Treaty on European Union, [1212] (TEU) and the Treaty on the Functioning of the European Union, [1213] (TFEU),[1214] and is therefore primary EU law, applicable in all 27 EU Member States. The CFR addresses the right to respect for "private and family life, home and communications" in article 7. Article 8 CFR, which addresses the right to personal data protection explicitly apart from the more general provision on privacy protection in article 7, is seen as a *lex specialis* of article 16 of the TFEU,[1215] and "personal data protection" is held to form part of the protected "private and family life, home and communications" enshrined in article 7. Article 8 CFR stipulates that everyone has the right to protection of personal data concerning him, and that the Union shall draft legislation for personal data processing by institutions of the Union and Member states, as well as prescriptions regarding the free movement of personal data.

Article 8 CFR is specially dedicated to personal data protection, and states the following:

> 1. *Everyone has the right to the protection of personal data concerning him or her.*
> 2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> 3. *Compliance with these rules shall be subject to control by an independent authority.*

[1209] See also Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, *OJ* L 295, 21.11.2018, p. 39–98
[1210] Charter of Fundamental Rights of the European Union, *OJ* C 326, 26-10-2012, p. 391-407.
[1211] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *OJ* C 306, 17-12-2007, p. 1–271 (Lisbon Treaty).
[1212] Treaty on European Union, *OJ* C 326, 26-10-2012, p. 13–390.
[1213] Treaty on the Functioning of the European Union, *OJ* C 326, 26-10-2012, p. 47–390.
[1214] Article 6 Lisbon Treaty.
[1215] See Kranenborg & Verhey 2018, p. 48-49; Berlee 2018, p. 183.

This provision has proven to be of major importance for the interpretation by the Court of Justice of the European Union (CJEU) of provisions of the Data Protection Directive, which has now been replaced by the GDPR.[1216] Insofar as case law of the CJEU addressing article 8 CFR is relevant in the sense of this study, this is further elaborated in section 5.2.

5.1.4.3 EUROPEAN CONVENTION ON HUMAN RIGHTS

The CFR exists alongside the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which is applicable in all 47 member states of the Council of Europe, including the EU Member States. Insofar the rights incorporated in the CFR correspond with the rights guaranteed by the ECHR, article 52(3) CFR states that "the meaning and scope of those rights shall be the same", albeit that Union law may provide more extensive protection.

The ECHR entered into force in 1953, and prescribes minimum protection for fundamental rights encompassed therein. Privacy is addressed in article 8.[1217] It must be noted that article 8 ECHR does not explicitly addresses personal data protection. However, it follows from the case law of the European Court of Human Rights (ECtHR), that personal data protection is encompassed in the scope of protection. The ECtHR has declared that under the protection of article 8 fall *inter alia* "personal data", [1218] "aspects relating to personal identity, such as a person's name and picture", [1219] information regarding someone's (historical) political activities, [1220] information regarding someone's intimate (business) relationships, [1221] phone, [1222] and email correspondence"[1223] – also in employment spheres. Sheer "business information" is not included in the scope of article 8 ECHR.[1224] Kranenborg and Verhey observe that "personal data" under 8 ECHR and the concept of personal data under the CFR (and the GDPR) are similar, although not

[1216] See Berlee 2018, p. 183, footnote 220. She refers inter alia to the annulment of the Data Retention Directive in the CJEU decision of 8 April 2014, ECLI:EU:C:2014:238, C-293/12 and C-594/12 (*Digital Rights Ireland*) and the (pre-GDPR) introduction of the 'right to be forgotten' in CJEU 13 May 2014, ECLI:EU:C:2014:317, C-131/12 (*Google Spain/Mario Costeja González*). Also the 'Safe harbor decision' of the European Commission, which was used as a basis to 'legalise' transfer of personal data of EU citizens to the United States, was annulled regarding the rights acknowledged in the CFR. See CJEU 6 October 2015, ECLI:EU:2015:C:650, C-362/14 (*Max Schrems/Data Protection Commissioner*).
[1217] 1: Everyone has the right to respect for his private and family life, his home and his correspondence. 2: There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
[1218] ECtHR 25 February 2997, 22009/93 (*Z/Finland*).
[1219] ECtHR 5 October 2010, 420/07 (*Köpke/Germany*); ECtHR 24 June 2004, 59320/00, (*Caroline von Hannover/Germany*).
[1220] ECtHR 4 May 2000, 28341/95, (*Rotaru/Romania*).
[1221] ECtHR 16 December 1992, 13710/88 (*Niemietz/Germany*).
[1222] ECtHR 25 June 1997, 20605/92 (*Halford/UK*).
[1223] ECtHR 26 June 2007, 62617/00 (*Copland/UK*).
[1224] ECtHR 4 January 2007, 39658/05 (*Smith/UK).*

the same.[1225] The concept of personal data under the CFR and the GDPR is wider than the concept under 8 ECHR, as the right to respect of a person's private life is not always at stake when personal data in sense of the CFR and GDPR are being processed,[1226] which follows inter alia form the *Smith* case.[1227]

As indicated above, there is certain overlap between article 8 ECHR, as interpreted by the Court, and the provisions of the CFR. This is acknowledged in article 52 CFR. That states in its third section:

> *In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.*

One can thus assume that the provisions of the ECHR are seen as a form of 'minimum protection' by the Union, and that the EU reserves the right to make arrangements that further protect the fundamental rights of citizens.

The current more extensive take on the scope of personal data by the CFR and secondary union law, compared to that of article 8 ECHR, is in line with this provision. Furthermore, it must be observed that article 6(1) TEU stipulates that the EU is to accede to the ECHR. If that were to happen, the ECtHR could directly assess whether or not the EU data protection legislation (as interpreted by the CJEU) is in conformity with article 8 ECHR.[1228] However, the concept agreement drafted by the EC on accession to the ECHR has been turned down by the CJEU in its advice of 18 December 2014,[1229] and it is foreseeable that both the concept agreement and the TEU need to be changed in order to make accession possible.[1230] Until that moment, the ECtHR jurisprudence remains of important, yet indirect, influence on the (interpretation of) the CFR and related legislation.

[1225] Kranenborg & Verhey 2018, p. 31.
[1226] Ibidem: "Niet bij elke verwerking van een persoonsgegeven is het recht op privéleven (privacy) in het geding.
[1227] ECtHR 4 January 2007, 39658/05 (*Smith/UK*). Smith required access to files in which his name was mentioned. Under GDPR rules (lex specialis of the CFR), he should in principle be allowed access thereto, for instance in order to correct the data incorporated in the files, as the sheer existence of personal data in a file constitutes personal data processing in the sense of the GDPR. The ECtHR held however that 8 ECHR was not applicable in this situation, as the respective files contained "business information", and as the contents were already known to Smith.
[1228] See Kranenborg & Verhey 2018, p. 49-50.
[1229] CJEU Advice 2/13, 18 December 2014, ECLI:EU:C:2014:2454
[1230] Ibidem, p. 50.

5.1.4.4 General Data Protection Regulation

The most important source of rules regarding the protection of personal data in the European Union is currently formed by the GDPR. The GDPR provisions directly apply in the Member States, and regulates almost every aspect of personal data protection. There is little room for Member States to legislate themselves, apart from *inter alia* open norms that are to be filled in by national legislators, or sector-specific rules that are not regulated by the GDPR. The GDPR has replaced the 1995 Data Protection Directive (DPD). Many of the material norms under the GDPR are the same or similar to those under the DPD, but the GDPR-rules are directly binding for the regulated citizens, companies and government institutions under its scope, and the enforcement mechanisms have been strongly increased.[1231] To the extent relevant for this study, section 5.2 provides further elaboration on the GDPR. It must be noted here that the judiciaries of (in any case) the Member States will have to hear conflicts that may arise out of the application of the GDPR; these courts can file prejudicial questions at the Court of Justice of the European Union regarding the interpretation of GDPR-norms. Alongside the courts, enforcement of the GDPR provisions within the Member States also takes place through local Data Protection Authorities (DPAs) and the European Data Protection Board (EDPB), in which all local DPAs and the European Data Protection Supervisor (EDPS) are represented.

The DPAs, which are independent supervisory authorities,[1232] have several competences and tasks besides monitoring and enforcing the GDPR-rules,[1233] including *inter alia* the duty to inform the public and those to whom the GDPR-rules apply,[1234] the obligation to advise the national legislators on (proposed) legislative and administrative measures and high-risk personal data protection operations,[1235] the obligation to handle complaints by data subjects and to investigate the subject matter at hand,[1236] and the tasks to encourage the drafting of codes of conduct and data protection certification mechanisms.[1237] DPAs should furthermore cooperate, *inter alia* through the EDPB and through bi- or multilateral ad hoc collaboration.[1238]

The tasks of the EDPB, which is like the DPAs an independent supervisory authority,[1239] include the monitoring and enforcement of the correct (and coherent) application of the GDPR within the EU Member States and the institutions of the Union.[1240] Another important task of the EDPB is to

[1231] See for example Custers e.a. 2019, p. 2.
[1232] See artt. 51 and 52 GDPR.
[1233] Art. 57(1)(a, h, i, u) GDPR.
[1234] Art. 57(1)(b, d, e) GDPR.
[1235] Art. 57(1)(c, l) GDPR.
[1236] Art. 57(1)(f) GDPR.
[1237] Art. 57(1)(m, n) GDPR.
[1238] See artt. 61-62 GDPR.
[1239] Artt. 68-69 GDPR.
[1240] Art. 70(1)(a) GDPR.

issue guidelines, recommendations and best practices regarding many aspects of personal data processing,[1241] including *inter alia* how to establish high-risk data breaches, policies regarding international transfers of personal data, advise for local DPAs regarding enforcing the GDPR through fines and penalties, and regarding reporting of GDPR infringements by citizens. Furthermore, the EDPB (too) has the obligation to encourage the establishment of codes of conduct and certification mechanisms,[1242] and has to review certain decisions of local DPAs.[1243] To date, the EDPB has issued 50+ guidelines and/or recommendations that further clarify, interpret or fill in GDPR-norms, and has endorsed 16 guidelines, position papers, working documents and recommendations of its predecessor, the Article 29 Working Party (WP29).[1244] WP29 has issued, during its existence, issued more than 160 opinions and recommendations, most of which are expected to be endorsed by the EDPB.[1245]

Both the DPAs and the EDPB are thus competent to issue policies that further explain, or fill in the open norms contained in the GDPR.[1246] There are certain democratic 'checks and balances' in place for DPA and EDPB decisions. DPA decisions can for instance be appealed by national courts,[1247] who can eventually refer prejudicial questions to the CJEU. Both DPA and EDPB decisions can be challenged for the CJEU by citizens who are affected thereby, on the basis of article 236 TFEU. Citizens can furthermore file a complaint before the ECtHR when their rights guaranteed by article 8 ECHR are violated. Also, the EU legislator could in theory adapt the GDPR where opportune. However, the democratic legitimacy of soft-law instruments issued by the independent supervisory authorities and the fact that the same authorities see to the application and enforcement thereof, is critically reviewed in literature.[1248] It is, for example, uncertain how the rights of EU citizens to closely participate in the 'democratic life of the Union', as enshrined in

[1241] Art. 70(1)(d-m) GDPR.
[1242] Art. 70(1)(n) GDPR.
[1243] Art. 70(1)(t) GDPR.
[1244] Within the Article 29 Working Party, the local supervisory authorities under the DPD and the European Data Protection Supervisor cooperated, in order to give advice regarding the consistent application of DPD rules on the Member State level, and to the Union bodies regarding personal data matters. It was established under article 29 of the DPD, and seized to exist when the DPD was superseded by the GDPR. The EDPB is its successor. See for the actual overview of their guidelines, recommendations and best practices: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_nl (last accessed 26 September 2021).
[1245] See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec11 (last accessed 9 July 2020).
[1246] See Kranenborg & Verhey 2018, p. 95.
[1247] Art. 78 GDPR.
[1248] See for instance Kranenborg & Verhey 2018, p. 94-98; 278-281, and their reference to *inter alia* M. Szydlo, "The independence of data protection authorities in EU law: between safeguarding of fundamental rights and ensuring the integrity of the internal market", *European Law Review*, 2017, no. 3, pp. 369-387; See also A. van Veen, *Regulation without Representation? Independent Regulatory Authorities and Representative Claim-Making in the Netherlands* (diss.), Utrecht: Utrecht University 2014, available via https://dspace.library.uu.nl/handle/1874/306252.

article 10(3) TEU and more specifically the right of 'interested parties' to be consulted and heard by the EDPB regarding their policy on the basis of article 70(4) GDPR will be safeguarded in practice.[1249]

5.1.4.5 OTHER SOURCES

Besides the GDPR, there are several other sources of secondary union legislation that contain rules regarding personal data protection.[1250] The ePrivacy Directive must be mentioned in that regard.[1251] This ePrivacy Directive contains privacy- and confidentiality rules mainly for the electronic communications sector, and complemented the (repealed) DPD. These rules hold *inter alia* obligations for 'providers of publicly available electronic communications services' and 'providers of public communications networks' to take certain security measures;[1252] to erase or anonymise traffic data that are no longer necessary;[1253] regulation of location data processing;[1254] rules for 'unsolicited communications';[1255] and rules on the storage and re-use of information on users' devices (cookies).[1256] The ePrivacy Directive is to be replaced by the (proposed) ePrivacy Regulation,[1257] although it is at this moment uncertain when that will be, and which form the eventual regulation will take. As the ePrivacy framework is of limited relevance in this study, only occasional reference to its subject matter will be made hereinafter, which includes the regime on 'cookies' incorporated in article 5(3).

[1249] Kranenborg & Verhey 2018, p. 95.
[1250] See also: the Data Rention Directive (repealed by CJEU 8 April 2014, C-293/12 & C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland and Seitlinger*): Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L 105, 13.4.2006, p. 54–6; also: Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, *OJ* L 295, 21.11.2018, p. 39–98. This Regulation addresses personal data processing by institutions and bodies of the European Union, and supersedes the (repealed) Regulation 45/2001. Besides material rules applicable to the EU Institutions – which are to a large extent similar to those of the GDPR, it regulates the European Data Protection Supervisor (EDPS).
[1251] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), *OJ* L 201, 31.7.2002, p. 37–47, as amended by Directive 2009/136, *OJ* L 337/11.
[1252] Articles 4 and 5 ePrivacy Directive.
[1253] Article 6 ePrivacy Directive.
[1254] Article 9 ePrivacy Directive.
[1255] Article 13 ePrivacy Directive.
[1256] Article 5(3) ePrivacy Directive.
[1257] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (ePrivacy Regulation) COM/2017/010 final - 2017/03 (COD).

5.2 GENERAL DATA PROTECTION REGULATION

5.2.1 INTRODUCTION

In the following sections, the General Data Protection Regulation is elaborated, to the extent necessary to address the case study in Chapter 6, and to reflect on the factors identified in section 3.4. It will be shown that the GDPR contains a comprehensive body of rules to comply with for *controllers* and *processors* of personal data relating to citizens who use AV-services. It will also be shown that not all norms are clear, or easy to comply with. As non-compliance results in potential civil liability, and as compliance can be enforced through high penalties by public supervisory authorities, it is necessary to elaborate the most important obligations for the entities addressed by the GDPR. Before diving into the material norms from section 5.2.2 onwards, a short illustration is given of the protected values and principles in section 5.2.2, as a follow-up to the functions of personal data protection in general, as illustrated previously in section 5.1.3.

5.2.2 VALUES AND PRINCIPLES

The GDPR builds upon earlier regulatory instruments including the DPD and the OECD Guidelines, also regarding the underlying values and protected principles.[1258] Like the DPD, the GDPR sees to the protection of the fundamental privacy right of citizens (also acknowledging other fundamental rights and freedoms, such as communication freedom),[1259] enshrined in article 8 CFR, and 16(1) TFEU,[1260] within the framework of the European Union.[1261] At the same time, the free flow of personal data within the EU must be ensured by the Member States and EU institutions. "Obstacles to flows of personal data within the Union" have to be prevented,[1262] and technological developments must be facilitated, although taking due account of a consistent and high level of protection of the privacy rights of EU citizens.[1263] Regarding rapid technological developments, strong protection and enforcement is necessary *inter alia* for "creating the trust that will allow the digital economy to develop across the internal market".[1264] It is indicated that control over personal data by citizens, and both legal and practical certainty contribute thereto.[1265]

> Recalling the earlier observations in section 3.4.3.3, Glancy states that a strong relationship exists between privacy protection of AV-users and trust in such technology, which she correlates with the acceptation, i.e. the uptake of AV-technology. On the negative side, poor

[1258] See Berlee 2018, p. 184-185, who also illustrates similarities in terms of protected values with Convention 108 (see supra fn. 1208).
[1259] Recital (4) GDPR.
[1260] Recital (1) GDPR.
[1261] Recital (2) GDPR.
[1262] Recital (10) GDPR.
[1263] Recitals (6, 7, 10, 12, 13 *inter alia*) GDPR.
[1264] Recital (7) GDPR.
[1265] Ibidem.

privacy protection could lead to "market resistance", while on the positive side strong privacy protection "is one of the best ways to foster trust and confidence in new technologies such as autonomous vehicles"; and "[b]eing proactive about privacy principles also helps in strengthening their trust".[1266] One of the objectives of the GDPR is thus to do just that.

The GDPR thus aims at free flow of personal data, while creating a coherent and strong framework of protection of the privacy rights of EU citizens, through principles and technology-neutral rules that will not be outdated or circumvented by technological developments.[1267] The GDPR distinguishes in general three 'subjects' to whom the rules apply: the *data subject*; the *controller* and the *processor. Data subjects* are those people to whom personal data directly or indirectly relate. Data subjects are equipped with rights allowing them to control the data processing activities carried out by controllers and processors.[1268] A *controller* is the natural or legal person who determines the "purposes and the means of the processing of personal data".[1269] Controllers are the main addressee of the principles and the rules of the GDPR, as elaborated below. When a controller decides to use the services of third parties in order to process personal data on behalf of him, those third parties are indicated as *processors* under the GDPR.[1270] The obligations for *processors* are less in number compared to those for *controllers*, although still significant.[1271]

Although the distinction between *controllers* and *processors* is quite clearly made in the GDPR, definitions the actual qualification of actors involved in the AV-industry might not always be easy to make. Where for instance an AV-manufacturer who intends to store and process vehicle data for the purpose of software-improvement clearly qualifies as *controller*, and the hosting provider whose services are used to store those raw data can be indicated as *processor*, such distinctions are sometimes harder to make. It is for instance questionable who must be deemed *controller* when AV-data regarding for instance the preferences of the "driving behaviour" of a vehicle can be optionally stored within the vehicle (only), but are not accessible by a manufacturer. In this case, it can be argued that the manufacturer is (still) *controller* as he determined the means (in vehicle storage) and purposes (individualised driving preferences) – despite the fact that the manufacturer can in fact not access these data. However, the opposite can also be argued, as the decision to actually store such data is not made by the manufacturer, but rather by the respective AV-users – who may then qualify as *controllers* themselves. Furthermore, it can be troublesome to qualify co-operating actors in the AV-producing chain

[1266] Glancy 2012, p. 1225-1226.
[1267] Recital (15) GDPR.
[1268] Article 4(1) GDPR. See further section 5.2.6.
[1269] Article 4(7) GDPR. See further this section below, and section 5.2.7.
[1270] Article 4(8) GDPR. See further section 5.2.8.
[1271] Ibidem.

as *controllers* or *processors*, when for instance one of the actors manufactures the hardware of AV-sensors, and another actor develops the software to operate them, where sensor data are stored on the servers of the hardware-manufacturer, but which are also accessible for the software-manufacturer for sensor-improvement purposes.[1272] Both the hardware and the software producers might be qualified as individual *controllers*, but the hardware manufacturer may at the same time be a *processor* for the software producer, as the latter uses the services of the former to store sensor-data for software-improvement purposes. To complicate matters, the producers might also be indicated as *joint controllers*, insofar as they would determine purposes (sensor-improvement through hard- and software optimisation) and means (storage on the servers of the hardware producer).

Controllers and *processors* need to conform their data processing activities to the rules enshrined in the GDPR, which are based on seven (or more accurately: nine) basic principles. These principles are, at least to a large extent, derived from the principles enshrined in the OECD Guidelines and, later, the DPD.[1273]

The *accountability* principle encompasses that the 'controller' (the entity who determines purposes and means of data processing)[1274] is responsible for compliance with the norms, and to demonstrate to the supervisory authority and to a certain extent, citizens whose data are processed, that he is complying.[1275]

An AV-rental company wishes to deploy a pay-as-you-drive scheme, in which users can rent a car, and will be billed according to *inter alia* distance covered, and areas in which the vehicles are being used: it is cheaper to drive the AV on the highway than in city centres. Therefore, it is necessary that personal data are being processed (see further section 5.2.2) such as bank account details of the AV-users. The GDPR applies to the data processing activities. The *accountability* principle under de GDPR *inter alia* encompasses obligations for the rental company to administer how it complies with the material obligations for *controllers*.

[1272] See furthermore EDPB 07/2020.
[1273] See Berlee 2018, p. 193-194.
[1274] Article 4(7) GDPR. The *accountability* principle is 'new', i.e. not encompassed in the DPD or the OECD Guidelines. See further section 5.2.10 and 5.2.11.
[1275] Article 5(2) GDPR.

The principle of *lawfulness, fairness and transparency*,[1276] holds that personal data must at all times be processed on a lawful basis, and in way that is fair and transparent for the 'data subject' (an identified or identifiable natural person).[1277]

> These principles entail for the AV-rental company introduced above that among many other things, it must be assured that there is a proper legal basis for the intended data processing, such as (in this case) the performance of an AV-rental contract. Furthermore, the AV-user must be informed of the data processing activities.

Personal data may, according to the *purpose limitation principle*, only be collected for specified, explicit and legitimate purposes, and may generally not be further processed in ways that are incompatible with the original purposes.[1278]

> The personal data that were collected of the AV-users to send them adequate bills for their car-use, may in principle not be used for other purposes, such as tailored commercial offers for (future) services.

The *data minimisation* principle holds that personal data must be adequate, relevant and limited to what is necessary for the purposes.[1279]

> This principle holds that no more information may be collected and processed than strictly necessary for in the aforementioned case the effective billing of the AV-services. This implicates that besides the bank-account details, only driven kilometres and areas in which the AV has operated may be processed.

Furthermore, personal data must be adequate and kept up to date. The *accuracy* principle also prescribes that rectified or erased without delay.[1280]

> It must be possible for the data subjects (the AV-users) to view which data are processed by the rental company. Also, they have to be able to rectify data that are wrong.

On the basis of the *storage limitation* principle, personal data must generally be erased or anonymised when the original purposes for which they were collected are fulfilled.[1281]

[1276] Article 5(1)(a) GDPR. See further section 5.2.4.
[1277] Article 4(1) GDPR. See further section 5.2.2.
[1278] Article 5(1)(b) GDPR. See further section 5.2.7.
[1279] Article 5(1)(c) GDPR. See further section 5.2.7.
[1280] Article 5(1)(d) GDPR. See further section 5.2.6.
[1281] Article 5(1)(e) GDPR. See further section 5.2.7.

> Billing information must be deleted as soon as the invoices have been paid. Should it be necessary, for instance for tax purposes, to store invoices afterwards, it must be considered which personal data *must* remain: any unnecessary data must be deleted or anonymised.

The *integrity and confidentiality* principle comprises that appropriate security must be ensured, in order to prevent unauthorised and unlawful processing of personal data. Technical and organisational measures must be implemented, to prevent accidental loss, destruction or damage of personal data.[1282]

> This principle entails that adequate measures must be taken by the AV-rental company to appropriately secure their systems. It also prescribes, that personal data should as much as possible be stored within the AV, and may only be shared with for instance third parties (including for example cloud-hosting companies) when necessary.

5.2.2. MATERIAL APPLICABILITY: PERSONAL DATA PROCESSING

AVs largely depend on data processing for their operation. When such processed data are *personal data*, the norms of the GDPR apply. The notion of *personal data* under the GDPR is very broad. Therefore, the GDPR applies to many aspects of data processing by or through AVs, as will be illustrated below.

According to article 4(1) GDPR, personal data are defined as

> "any information relating to an identified or identifiable natural person", who is addressed further as the *data subject*. A person is identifiable when he "can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The notion of *personal data* is very broad. WP29 issued a lengthy report on what could be seen as *personal data* under the DPD,[1283] which notion remained largely the same under the GDPR. Although the report has not yet been endorsed by the EDPB, it can be used to illustrate the subject matter that is to be qualified as *personal data*. The element "<u>any information</u>" is taken broadly as encompassing objective and subjective information about a person – sensitive or not (stricter rules may apply for certain categories of sensitive data, see section 5.2.5), on whatever carrier. Whether or not the information is true is irrelevant, both true and false information fall under the

[1282] Article 5(1)(f) GDPR. See further section 5.2.7 and 5.2.8.
[1283] WP29 (136).

scope of the "information"-element.[1284] It is illustrated that besides regular information representations such as databases containing name an address data, also for example a child's drawing reflecting his or her mood (which can be seen as a state of health from a psychiatric perspective), a voice, biometric data and human tissue all fall under the notion of "any information". CJEU case law has confirmed that subjective information in the form of answers to exam questions and the revisions thereof, do qualify as *personal data* in sense of the GDPR.[1285]

Information must "relate to" a person in order to fall under the scope of the personal data concept. WP29 observes that "in general terms, information can be considered to "relate" to an individual when it is *about* that individual".[1286] Medical records containing test-results of a patient, employee data in the database of an employer and someone's image captured on CCTV recordings all contain information that directly relates to certain individuals, as the *content* of the information represents a direct connection between information and a person. When a direct link between a piece of information and a person cannot be established, it can still be information relating to a person when there is an indirect connection with the purpose or result to relate to a natural person. Information regarding the value of a house can be used to determine the amount of taxes to be paid, and the system to track the position of taxi's for service optimisation purposes can be also used to identify the drivers and to monitor their performance, and therefore relate to respective data subjects.

The third element of the definition sees to "identified or identifiable" natural persons. Someone is *identified* "when, within a group of persons, he or she is "distinguished" from all other members of the group".[1287] Someone is *identifiable* when it is possible to directly or indirectly identify him or her, through identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

> The data object "R.W. de Bruin", in this case a name of a natural person, does not *directly* identify someone. A search on Google indicates that there are at least two people in The Netherlands carrying this surname and initials: a dentist and a lawyer. Besides the name, another identifier is necessary for ascertaining an identity. In the latter case, one could identify the author of this study by combining the data object at hand with the name of his employer.

[1284] Ibidem, p. 6-9.
[1285] CJEU 20 December 2017, C-434/16, ECLI:EU:C:2017:994 (*Peter Nowak*).
[1286] WP29 (136), p. 9.
[1287] WP29 (136), p. 12.

> When "R.W. de Bruin" would be combined with "Utrecht University", one would be able to 'single out'[1288] in this case, me.

Names are not the (only) means to decisively identify someone. For example a fingerprint, DNA or social service numbers can also – and sometimes even more concludingly – be used to easily establish the identity of a specific natural person.[1289]

Even pieces of information that do not seem to be of any 'identifying value' at first sight, can still be used, for instance through combination with other pieces of information, to identify someone, and thus be qualified as *personal data*.[1290] An IP-address is an example of a piece of data that could indirectly identify a natural person. Although someone's identity does not directly follow from the IP-address, it is possible to identify a person using the specific IP-address through records that are kept by an internet service provider, which links the IP-address to a specific internet user.[1291] Records of someone's internet surfing behaviour (google-searches; visited websites; Facebook-activity; maps-searches), even when kept in different places, could for instance also lead to the situation that someone can be 'singled out', and thus identified. In order to determine whether or not certain pieces of information can qualify as "identifiable", one should take account of "all the means likely to be used", where "all objective factors" should be assessed, "such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".[1292] It thus follows from recital 26 to the GDPR that mere hypothetical means to de facto identify someone are not enough to qualify data (or a data set) as identifiable. Moreover, it must be reasonably likely (and not requiring prohibited identification methods, or "a disproportionate effort in terms of time, cost and man-power")[1293] that identification can take place at some point. WP29 does indicate that one should take account of technological progress. What is considered unreasonable effort today, can be common practice tomorrow.[1294] It must be noted that "it is not required that all the information enabling the identification of the data subject must be in the hands of one person".[1295] This entails that even when stored in different places, certain pieces of information that, when combined, may

[1288] See on 'singling out' WP29 (136), p. 14.
[1289] See Kranenborg & Verhey 2018, p. 105.
[1290] The CJEU held for instance that besides names, also phone numbers, or information regarding someone's working conditions and hobbies can constitute *personal data*, in CJEU 6 November 2003, C-101/2001, ECLI:EU:C:2003:596 (*Lindqvist*).
[1291] See CJEU 24 November 2011, C-70/10, ECLI:EU:C:2011:771 (*Scarlet/SABAM*).
[1292] Recital (26)
[1293] CJEU 19 October 2016, C-582/14, ECLI:EU:C:2016:779 (*Patrick Breyer*), no. 46.
[1294] Ibidem.
[1295] CJEU *Patrick Breyer*, no. 43.

identify a natural person, can be qualified as *personal data*, when this would not require "disproportionate effort", i.e. resulting in a de facto insignificant risk of identification.[1296]

When *data subjects* cannot be identified through "all likely and reasonable means", information can be considered *anonymous*.[1297] The GDPR does not apply to anonymous information.[1298] It must be noted however, also taking account of the aforementioned observations regarding *inter alia* the rapid technological developments which may facilitate identification processes, it would be very difficult to label certain data (sets) as truly anonymous. When (re-)identification is possible, data are rather *pseudonymous* than anonymous. Pseudonymous data remain *personal data* in sense of the GDPR. The GDPR defines *pseudonymisation* as:

> "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".[1299]

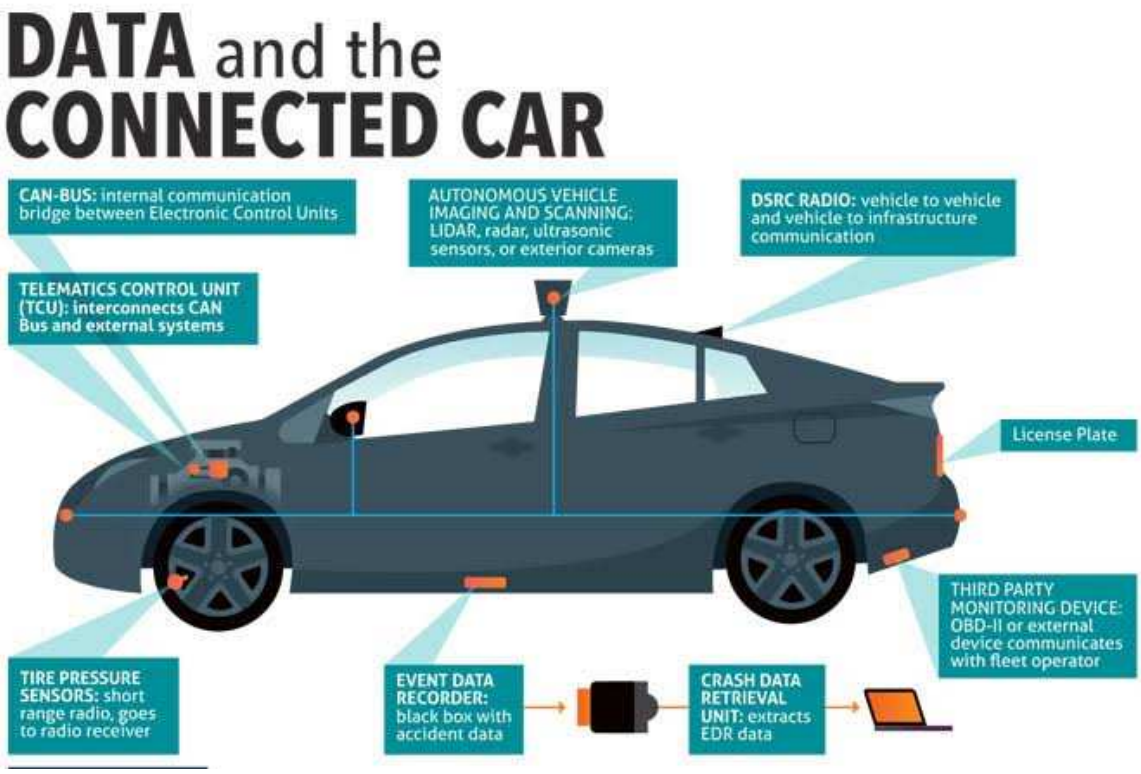
The GDPR applies to personal data *processing.* Processing occurs, when personal data are *wholly or partly* processed by *automated means*, or by other means, when personal data (are *intended to*) *form part of a filing system*.[1300] Virtually anything that one can do with personal data is qualified as such, during the entire 'lifecycle' of personal data, from origination to destruction.[1301] Article 4(2) non-limitedly states that processing

> "means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

It is necessary that processing takes place – at least to some extent – by automated means, or through a filing system. This de facto only excludes the manual and non-structured offline storage of personal data; any other structured or automated storage triggers applicability of the GDPR – in most cases.

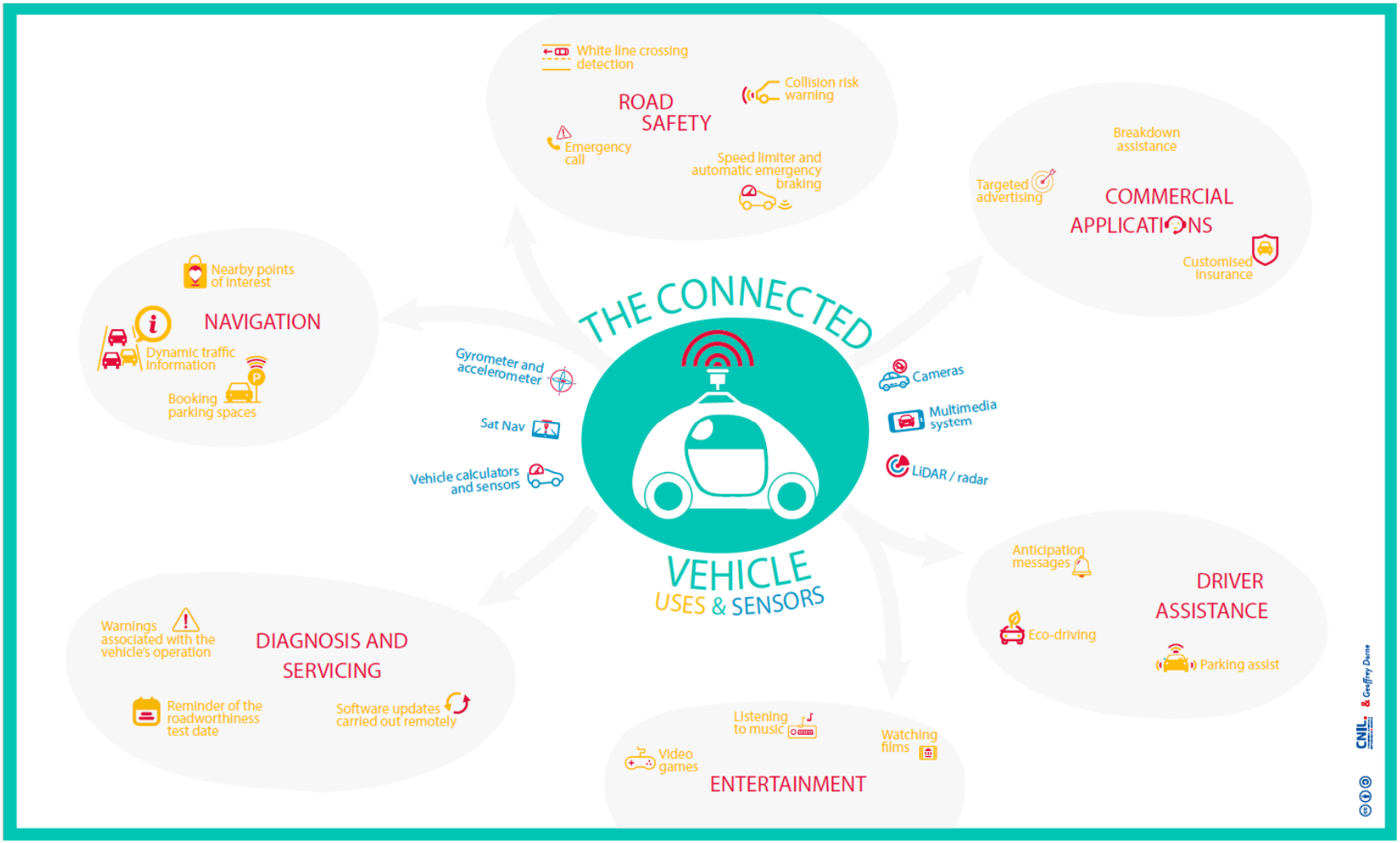
[1296] See also Kranenborg & Verhey 2018, p. 106; Berlee 2018, p. 191.
[1297] See also WP29 (216).
[1298] Recital (26), second part GDPR.
[1299] Article 4(5) GDPR.
[1300] Article 2(1) GDPR.
[1301] See Kranenborg & Verhey 2018, p. 111; Berlee 2018, p. 192.

The EDPB recognized in its Guidelines 1/2020 that connected vehicles (which includes AVs) "are becoming massive data hubs",[1302] and that through such vehicles and their users, large amounts of personal data will be processed. The EDPB refers to an infographic by the Future of Privacy Forum, displayed below:[1303]



Besides the EDPB, also the French data protection authority (Commission Nationale de l'Informatique et des Libertés, CNIL) has published guidelines that are illustrative in this regard,[1304] including the following infographic:[1305]

[1302] EDPB 01/2020, p. 3.
[1303] Future Privacy Forum (staff), "Infographic: Data and the Connected Car – Version 1.0", available via https://fpf.org/2017/06/29/infographic-data-connected-car-version-1-0/ (last accessed 13 July 2020).
[1304] CNIL 2018.
[1305] CNIL, infographic "The connected vehicle – uses & sensors", via https://www.cnil.fr/sites/default/files/atoms/files/infographie_voiture_2017_en_ok.pdf (last accessed 13 July 2020).


THE CONNECTED VEHICLE
USES & SENSORS
ROAD SAFETY
White line crossing detection
Collision risk warning
Emergency call
Speed limiter and automatic emergency braking
COMMERCIAL APPLICATIONS
Breakdown assistance
Targeted advertising
Customised insurance
NAVIGATION
Nearby points of interest
Dynamic traffic information
Booking parking spaces
Gyrometer and accelerometer
Sat Nav
Vehicle calculators and sensors
Cameras
Multimedia system
LiDAR / radar
DRIVER ASSISTANCE
Anticipation messages
Eco-driving
Parking assist
DIAGNOSIS AND SERVICING
Warnings associated with the vehicle's operation
Reminder of the roadworthiness test date
Software updates carried out remotely
ENTERTAINMENT
Listening to music
Watching films
Video games
CNIL. & Geoffrey Dorne

There are many types of personal data that can be processed through the above indicated sensors, cameras, (recording) devices and telematics units that are built in AVs, and/or devices that are connected to it.[1306] One may think of *inter alia* AV-user preference data, regarding for instance infotainment- and seat adjustment preferences; AV-operation data regarding for example GPS-location data; vehicle maintenance/wear and tear data; but also camera recordings that are made inside and around a vehicle, and data that are necessary for "pay as/how you drive"-models, including for instance driving behaviour and data on fuel consumption. In the Guidelines, the EDPB pays special attention to three types of *special category data* (see further section 5.2.5). It is indicated that

> "geolocation data are particularly revealing of the life habits of data subjects", as these may indicate the "place of work and of residence, as well as a driver's centers of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited".[1307]

Also highlighted are biometric data, which "may be used, for among other things, to enable access to a vehicle, to authenticate the driver/owner, and/or to enable access to a driver's profile settings and preferences";[1308] and offence-related data, as it can even be possible "that personal data from connected vehicles could reveal the commitment of a criminal offence or other infraction".

Some personal data processing activities are excluded from the material scope of the regulation. When processing takes place outside the scope of Union law;[1309] when Member States carry out activities under Chapter 2, Title V TEU (common foreign and security policy);[1310] when processing occurs by a natural person in the course of a purely personal or household activity;[1311] or when competent authorities process personal data in a criminal law context;[1312] the GDPR does not

[1306] The EDPB furthermore categorises the personal data that could be processed though connected (and autonomous) vehicles in three categories, as: "(i) processed inside the vehicle, (ii) exchanged between the vehicle and the personal devices connected to it (e.g. the user's smartphone or (iii) collected within the vehicle and exported to external entities (e.g. vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing, see EDPB 01/2020, p. 6.
[1307] EDPB 01/2020, p. 12.
[1308] Ibidem, p. 13.
[1309] Article 2(2)(a) GDPR, sees *inter alia* to processing of personal data for purposes of national security, as such has not been conferred to the EU by the Member States.
[1310] Article 2(2)(b) GDPR.
[1311] Article 2(2)(c) GDPR.
[1312] Article 2(2)(d) GDPR.

apply. Personal data processing by Union institutions, bodies, offices and agencies, is regulated by regulation 2018/1725 (formerly 45/2001) exclusively.[1313]

5.2.3 TERRITORIAL APPLICABILITY

Article 3(1) GDPR stipulates that its rules are applicable "to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not".[1314] According to Recital (22), "the real exercise of activities through stable arrangements" is decisive in this respect, the legal form (e.g. head- or sub quarters) or legal personality is not relevant.[1315] When a controller or processor is *not* established in the union, but the processed personal data relate to data subjects who are in the Union, the GDPR is applicable as well, when such processing concerns either the offering of goods and services, both free and paid, or when it concerns the monitoring of their behaviour within the EU.[1316] It follows from Recital (23) that for the determination whether or not services and goods are offered to data subjects under the GDPR, it must be apparent that "controller or processor envisages offering services to data subjects who in one or more Member States". In that respect, the accessibility of a website or email address from the Union is not decisive, nor is the language in which a website is available when that would be the language used in its country of origin. Factors that could however lead to the valid assumption that "envisaged offering of services" within the Union, include for instance the use of the language of (one or more) Member States, or the use of the Euro or other Member States currencies. Behaviour monitoring might result in the creation of profiles of for instance website users. Would those profiles include people in the EU, this could enable applicability of the GDPR rules through the provision in article 3(2)(b). Article 3 concludes with a third section, which states that the GDPR also applies in places "where Member State law applies by virtue of public international law.

[1313] Article 2(3) GDPR. Furthermore, it must be observed that article 23 GDPR provides general possibilities to restrict the GDPR provisions on the basis of Union- or Member State law. Regarding certain obligations for controllers and processors, exceptions may be regulated, as long as "the essence of fundamental rights and freedoms" are respected, and to the extent that such exceptions are "necessary and in proportionate measure in a democratic society", and must see to the safeguarding of the interests listed under article 23(1)(a-j) GDPR. These interests include inter alia national or public security; defence; crime fighting; protection of the data subject, or the rights and freedoms of others; and the enforcement of civil law claims. The second paragraph contains further requirements exceptions (to be legislated), regarding among other things that provisions must be made as to the purposes of (excepted) processing; their scope; categories of personal data to be processed; storage periods; rights of data subjects (to be informed of the restrictions) et cetera.

[1314] See also EDPB 3/2018.

[1315] See also EDPB 3/2018, p. 6: the threshold is low, especially when services are provided online. The EDPB furthermore highlights that "the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute stable arrangement […] if that employee or agent acts with a sufficient degree of stability".

[1316] Article 3(2) GDPR.

The extraterritorial applicability of the GDPR is broad. Its framework for instance applies to an India-based company without presence in the EU, that is responsible for servicing and further development of the steering software of AVs, when it for example requires that the car users upload driving behaviour and -circumstances (which can be qualified as personal data) regarding "bugs" that appeared when the vehicle was operated in for example unknown or unprogrammed conditions.

Also the "sheer receiver" of personal data located for example in the US, who is responsible for the storage and accessibility of AV-data that are processed for *vehicle-to-infrastructure* communication, is an actor to which the GDPR applies.

The territorial scope of the GDPR has, to a certain extent, been narrowed down by the CJEU in its *Google/CNIL* decision.[1317] In that case, Google was ordered to grant a request to remove certain entries from their search results, on the basis of the *right to be forgotten* of a data subject.[1318] Google did remove such entries, although only for the versions of its search engine with the domain name extensions of the EU Member States, while it refused to remove the results from other, non-EU, versions of the search engine. The CJEU held that Google was not obliged to remove the entries from all its versions, but rather

> "on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request".[1319]

Thus, where the framework of the GDPR is applicable also in certain extra-territorial cases, obligations to remove certain personal data under the GDPR, should not prevent citizens in non-EU countries from having access to such information as a result of extra-territorial application of the GDPR.

5.2.4 LAWFULNESS OF PROCESSING

The *lawfulness, fairness and transparency*-principle, enshrined in article 5(1)(a) GDPR requires that personal data may only be processed lawfully, fairly and in a transparent manner in relation to the data subject. The part that sees to *lawfulness* is elaborated in article 6, and is further

[1317] CJEU 24 September 2019, C-507/17, ECLI:EU:C:2019:772, (*Google/CNIL*).
[1318] See further section 5.2.6.
[1319] CJEU *Google/CNIL* no. 73.

illustrated below. Fairness and transparency are addressed in articles 12 to 14, and are illustrated in section 5.2.6.

Personal data may only be processed when there is a lawful basis for such processing. Article 6(1) lists the following (emphasis added):

a) the data subject has given *consent* to the processing of his or her personal data for one or more specific purposes;
b) processing is *necessary for the performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is *necessary for compliance with a legal obligation* to which the controller is subject;[1320]
d) processing is *necessary in order to protect the vital interests of the data subject* or of another natural person;
e) processing is *necessary for the performance of a task carried out in the public interest* or in the exercise of official authority vested in the controller;[1321]
f) processing is *necessary for the purposes of the legitimate interests pursued by the controller or by a third party***,** except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[1322]

5.2.4.1 Consent

The GDPR first mentions consent as a lawful basis for personal data processing. In fact, it is one of the most troublesome bases for controllers, as there are many conditions to fulfil in order to ascertain that the consent given justly legitimates the (intended) processing, and it is only valid for the duration of the consent (until withdrawal).

> Albeit troublesome, the consent-basis will likely be the only applicable one when none of the other (performance of a contract, legal obligations, legitimate interests: see below) can be relied on, which will be the case for instance when the AV-data-processor has a (purely) commercial purpose for processing special category data (see section 5.2.5). As the EDPB illustrated, also when for example AV-users (on request) want to participate in accidentology studies, in order to better understand the causes of AV-related accidents, for scientific

[1320] Member states may legislate more specific rules in this regard, as follows from art. 6(2) and (3) GDPR.
[1321] Ibidem.
[1322] This point cannot be applied by data processing activities by public authorities in the performance of their tasks. See further Berlee 2018, p. 207-208.

purposes,[1323] and perhaps even to improve the services, (only) the consent-basis may be applicable.

Article 4(11) GDPR defines consent as

> "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[1324]

Pre-ticked boxes, and 'silence' are thus not allowed to construe consent.[1325]

The EDPB explained that consent would only then construe a valid legal basis "if the data subject is offered control and is offered a genuine choice with regard to accepting or declining them without detriment".[1326] The fact that consent needs to be *freely given,* implicates that *inter alia* a refusal to deliver certain services without the users' consent to process a myriad of personal data, while the majority of that data processing is not necessary for the delivery of that service, would not legitimate the intended data processing when the data subject *did* agree.[1327] For example the consent obtained by the provider of a WiFi service to process the personal data of its users for marketing purposes (which is not necessary to operate that service), is not valid, when those users were 'forced' to provide such consent in order to be able to use that WiFi service.

Article 7(4) GDPR stipulates in this regard that:

> "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".

[1323] See EDPB 1/2020, p. 27-28.
[1324] It must be noted that it follows from Recital (43) GDPR that public authorities could likely not rely on consent as a valid legal basis. Recital (32) indicates furthermore that consent must show from a "clear affirmative act", illustrating the "unambiguous indication if the data subject's agreement to the processing", such as a written or oral statement, or the ticking of a box in an online form.
[1325] See also Kranenborg & Verhey 2018, p. 146-147.
[1326] EDPB 05/2020, p. 5. Such (prohibited) negative consequences may include costs for the data subject, loss of a discount, deception, intimidation, coercion, but also limited availability of services or functionalities (while those users who gave consent enjoy unlimited services, or full functionality (EDPB 05/2020, p. 13). In this, the GDPR – and the EDPB – acknowledge a power imbalance between controllers and data subjects, and sees to offer the data subjects certain means to 'correct' such imbalance (p. 8-9)
[1327] See EDPB 05/2020, p. 7.

When the performance of a contract would be tied to the data subjects' consent to unnecessary data processing, this leads to the presumption that the granted consent is invalid.[1328]

A data controller intending to use *consent* as a lawful basis, has to demonstrate that the data subject has consented to the data processing activity, which follows from article 7(1) GDPR.[1329]

Article 7(3) prescribes that consent can be withdrawn at any time by the data subject (and that the controller has a duty to inform data subjects thereof), while withdrawal should be as easy as giving consent. A consent withdrawal does not retroactively invalidate the data processing that occurred while there was consent; it (only) invalidates further processing of personal data.

> The 'cookie regime' of article 5(3) ePrivacy Directive is also relevant in this regard. Cookies are small text files that are stored on devices that are connected to the internet, such as tablets, phones, and computers. Cookies may contain all sorts of information, which may for instance be 'functional' for the users of the device. For example locally stored address-data can be functional in the sense that those data can be used to pre-fill address forms on the website of an online shop. Cookies are also often used for marketing purposes. Information on internet searches or browse-behaviour of device-users can be stored, and shared amongst various internet platforms and providers of commercial services (i.e.: "tracking"). In the ePrivacy Directive, certain rules are provided for the storage and processing of information in cookies.
>
> The EDPB observed that AVs, and devices connected to it, fall under the scope of the ePrivacy Directive, when they are connected to an electronic communications network,[1330] and when cookies are stored therein. This implicates that, the controller has to provide "clear and

[1328] EDPB 05/2020, p. 11. Also in employment relationships, a power imbalance between employer and employee is recognised, and the EDPB observes that "[g]iven the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of refusal" (p. 9). Therefore, the EDPB concludes that consent can hardly ever be a valid lawful basis for personal data processing in employment situations, unless the employer can demonstrate a total absence of detrimental conditions for the employee, should he deny his consent.

[1329] When the data subject is a child, there are even stricter conditions, which are regulated in article 8 GDPR. It furthermore follows from section (2) that when consent is requested "in the context of a written declaration" where also other matters are addressed, that request must be "clearly distinguishable from the other matters in an intelligible and easily accessible form", or it would not be binding in the sense of the GDPR.

[1330] AVs than qualify as "terminal equipment" in sense of directive 2008/63/EC on competition in the markets in telecommunications terminal equipment, *OJ* L 162/20). Article 1defines terminal equipment as: "Equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment"; analysed by EDPB 1/2020, p. 5.

comprehensive information in accordance with [the GDPR],[1331] inter alia about the purposes of processing" and to obtain prior consent to a) store and b) access cookies.[1332] Consent is not necessary when cookie storage or access is functional, i.e. for

> "the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".

Thus, when non-functional cookies are placed or accessed, or other similar (tracking) mechanisms are deployed, the data subject has to give prior informed consent, in sense of article 4(11) and 7 GDPR.

5.2.4.2 Performance of a contract, legal obligation, vital- and public interests

The lawful bases mentioned in article 6(1), under b), performance of a contract; c), compliance with a legal obligation; d), protection of vital interests; and e), performance of a public interest task, are most likely less relevant in AV-related personal data processing, and in general 'easier' to comply with than the aforementioned consent-basis, and the legitimate-interests basis, elaborated below. Therefore, those bases are addressed together in this section.

Processing personal data is deemed lawful, when the controller can show that such processing is necessary to the extent that a) the data subject requests to enter into an agreement with him, and b) perform his obligations towards the data subject under a contract.[1333] This basis is thus limited to those data that are *necessary* for entering into an agreement, or the performance thereof. Should for instance a contract see to the delivery of a book that a data subject has ordered online, the personal data that may likely be processed, are the contact details of the data subject (as this is necessary for the delivery), and the payment information/bank account details of the data subject (necessary for executing the payment). Further data processing, such as for instance the storage of the email address of the data subject in order to send him marketing information in the future, cannot be rightfully done on the "performance of a contract" basis.

> In case someone wants to rent an AV, a rental agreement is likely necessary. The rental company may base precontractual data processing (exchange of information regarding *inter alia* the requirements of the data subject; his driving license (to the extent necessary); contact- and bank account details) and the contractual data processing (regarding *inter alia* non-mandatory insurance; pick-up and return; distance covered; fuel use), on article 6(1)(b) GDPR.

[1331] See article 94 GDPR.
[1332] See EDPB 01/2020, p. 5-6, and their reference to EDPB 5/2019; as well as EDPB 05/2020, p. 6.
[1333] This follows from article 6(1)(b) GDPR.

Processing non-necessary information, such as on board marketing communications tailored to the passengers of the car based on their behaviour, could not be legalised on the 'performance of a contract'-basis.

The EDPB provides another example, of so-called *pay as you drive*-insurance concepts, in which 6(1)(b) GDPR can be used.[1334] In such concepts (which will become less relevant when car autonomy increases), insurance premiums are based on the actual mileage, and are often lowered when the drivers 'behave well' on the road. Therefore, certain systems are deployed that can accurately monitor the covered distance and the driving behaviour and send the respective data to the insurance company. The insurance company will then be able to multiply the covered kilometres with the agreed price per kilometre, and to correct that total amount with the 'scored' driving behaviour. The EDPB indicates that the necessary personal data processing can be based on article 6(1)(b) "provided it can establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed".[1335] While it would be possible to create a rather accurate profile of the movements of the driver, it must be noted that such profiling may not take place on the legal basis of the performance of a contract.

To the extent that a controller has certain specific legal obligations, he may process personal data that are necessary to fulfil these. It is necessary that the respective obligation addresses the controller himself (rather than a third party).[1336] The legal obligation must be laid down by either Union, or Member State law.[1337] The legal obligation does not have to explicate that personal data processing is necessary, it is sufficient when the controller can show that the legal obligation requires him to process certain personal data, without which he cannot comply with his respective duties under the applicable obligation.[1338]

It follows from Regulation 2015/758,[1339] that AVs have to be equipped with an eCall-system, which automatically calls 112 in case of an accident, and requests an ambulance to be sent to the actual location of the car calling the emergency number. The EDPB indicates that the data

[1334] EDPB 1/2020, p. 21-24.
[1335] When communication of personal data is executed over an electronic communications network, and when storage of information in the AV/connected devices is necessary, account must also be taken of the obligations ex. article 5(3) ePrivacy Directive.
[1336] See Kranenborg & Verhey 2018, p. 151.
[1337] Article 6(3) GDPR.
[1338] Ibidem; see also Recital (45) GDPR.
[1339] Regulation (EU) 2015/758 concerning type-approval requirements for the development of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC, *OJ* L 123/77.

processing resulting from emergency calls under Regulation 2015/758 (*inter alia* the indication of a manual or automatic call; vehicle type; vehicle identification number; location; time; and travel destination) are necessary in sense of article 6(1)(c) GDPR.[1340]

The new General Safety Regulation,[1341] requires as of mid-2022 that, vans, trucks and buses with event data recorders (EDR), which must meet the following requirements:

> "the data that they are capable of recording and storing with respect of the period shortly before, during and immediately after a collision shall include the vehicle's speed, braking, position and tilt of the vehicle on the road, the state and rate of activation of all its safety systems, 112-based eCall in-vehicle system, brake activation and relevant input parameters of the on-board active safety and accident avoidance systems, with high level of accuracy and ensured survivability of data;"[1342]

Furthermore, it must be unable that EDRs are deactivated,[1343] and data must *inter alia* be "anonymised and protected against manipulation and misuse".[1344] Also, the data must be accurate in that they specify the "precise vehicle type, variant and version, in particular the active safety and accident avoidance systems fitted to the vehicle".[1345] However, the last four digits of the Vehicle Identification Number may not be stored, or "any other information which could allow the individual vehicle itself, its owner or holder to be identified".[1346]

However, it will be virtually impossible to *anonymise* the stored data in sense of the GDPR, as singling out may be often possible, and/or identification can occur when for instance accident data and/or data revealing the whereabouts of the individuals involved in the accident (as for instance stored in their phones or on social media accounts) are combined with the EDR-data.

[1340] EDPB 1/2020, p. 25.
[1341] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, PE/82/2019/REV/1, *OJ* L 325, 16 December 2019 (hereinafter: GSR 2022).
[1342] Article 6(4)(a) GSR.
[1343] Ibidem, sub b.
[1344] Ibidem, sub c, under ii.
[1345] Ibidem, sub c, under iii.
[1346] Article 6(5) GSR.

Anyway, that prescribed *anonymisation*-activity would involve *processing* of personal data, which is thus allowed under these legal obligations.

The data stored in the EDR may only be processed in order to allow "national authorities, on the basis of Union or national law" to conduct "accident research and analysis including for the purposes of type approval of systems and components and in compliance with Regulation (EU) 2016/679, over a standardised interface".[1347]

Thus, EDR-data stored under the legal obligations of the GSR may *not* be used for any other purposes by for instance car manufacturers.

Personal data may also be processed to the extent necessary "to protect the vital interests of the data subject or of another natural person".[1348] This can be the case when the life of a data subject (or another person) is at stake in an urgent medical situation, and it is impossible to ask consent of the data subject.[1349]

Furthermore, personal data can be processed lawfully, when this is necessary "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."[1350] Also in these cases, the processing should be based on Member State or Union law.[1351]

It is not likely that controllers of AV data will often be able to base their personal data processing on article 6(1)(d or e) GDPR. The EDPB does not address these bases in its case studies in its Guidelines 1/2020.

5.2.4.3 Legitimate interests of the controller or third party

Article 6(1)(f) GDPR contains an open norm, and allows personal data processing that is necessary

"for the purposes of the legitimate interests pursued by a controller or a third party, except where such interests are overridden by the interests or fundamental freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

[1347] Article 6(4)(d) GSR.
[1348] Article 6(1)(d) GDPR.
[1349] See Kranenborg & Verhey 2018, p. 153-154.
[1350] Article 6(1)(e) GDPR.
[1351] Article 6(3) GDPR; see furthermore Kranenborg & Verhey 2018, p. 154-157.

This provision, which functions as a 'rest category' when data processing cannot be based on any other ground, holds a three-step-test for controllers who want to use his 'legitimate grounds' as a basis for processing personal data.[1352]

First, a controller has to ascertain that he has some interest, that can be qualified 'legitimate'. Although the EDPB has not issued relevant opinions or guidelines in this respect yet, its predecessor, WP29 had.[1353] It is held that the interest pursued by the controller should in any case be "real and present" (i.e. not speculative). Future interests, or "an interest depending on the fulfilment of a condition or an expectation for an interest" are insufficient in this regard.[1354] Furthermore, such interests need to be lawful, i.e. not contrary to applicable law, as well as sufficiently clear.[1355] In this regard, the current policy of the Dutch DPA, the Autoriteit Persoonsgegevens (AP) is notable. In its explication of article 6(1)(f) GDPR, it held that purely commercial interests, profit maximisation or monitoring the behaviour of employees or (potential) customers without a legitimate interest, cannot qualify as "legitimate interests" in sense of the GDPR.[1356] This view is new and unique in the EU, and can be said to contradict *inter alia* the view of the English DPA, the Information Commissioner's Office (ICO); the AG to the CJEU and the GDPR itself. The ICO holds that "You can rely on legitimate interests for **marketing activities** if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object" (emphasis added).[1357] Also Advocate General Bobek, holds that "no type of interest is excluded per se",[1358] and furthermore that "marketing or advertising can, as such, constitute a legitimate interest".[1359] Also the GDPR itself states in recital (47) that "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest".[1360] Time will tell whether or not the standpoint of the AP will be endorsed or rejected by for instance the EDPB and the CJEU. Until more clarification is provided on the Union level, given *inter alia* the fact that different SA's take a

[1352] See Kamara & De Hert 2018, p. 12-14; see also CJEU 4 May 2017, C-13/16, ECLI:EU:C:2017:336 (*Rigas*), no. 28; and CJEU 11 December 2019, C-708/18, ECLI:EU:C:2019:1064 (*Bloc M5A*), no. 44 (existence of a legitimate interest), 46 ff. (necessity of the processing activity in the light of that legitimate interest), and 52 ff. (proportionality of the data processing related to the protection of the fundamental rights of data subjects).
[1353] WP29 (217); see also CJEU *Bloc M5A*, no. 44 ff.
[1354] Kamara & De Hert 2018, p. 12-13; WP29 (217), p. 25.
[1355] WP29 (217), p. 25; Kamara & De Hert 2018, p. 12-13; Kranenborg & Verhey 2018, p. 158-159.
[1356] AP 2019, p. 3: "Wat ook niet als een gerechtvaardigd belang kwalificeert, is bijvoorbeeld: het enkel dienen van zuiver commerciële belangen, winstmaximalisatie, het zonder gerechtvaardigd belang volgen van het gedrag van werknemers of het (koop)gedrag van (potentiële) klanten, etc".
[1357] ICO 2019, p. 79.
[1358] Opinion of Advocate General Bobek 19 December 2018, C-40/17, ECLI:EU:C:2018:1039, (*Fashion ID*), no. 122.
[1359] Ibidem, no. 123.
[1360] The 'economic interest' seems to be acknowledged by the CJEU as well. See for instance CJEU 13 May 2014, ECLI:EU:C:2014:317, C-131/12 (*Google Spain/Mario Costeja González*), no. 81, 97.

different approach, the fact that the district court in Midden Nederland has dismissed the AP's standpoint,[1361] and taking into account Bobek's view, it can be argued that legitimate interests may in principle also comprise (purely) commercial interests.

When a legitimate interest has been established, the necessity of the intended data processing must be assessed. This holds that it must be ascertained that "processing of personal data is the least restrictive measure to the rights of the data subject",[1362] which reflects principles of proportionality and subsidiarity, as well as data minimisation.[1363] Should there be any less-intrusive paths that could be followed to pursue the respective legitimate interest, the intended data processing cannot be considered 'necessary'. Conversely, when there are no less-intrusive ways available, the necessity requirement is satisfied.

Thirdly, a balancing test needs to be carried out by the controller. In this test, many factors can play a role, such as the sensitivity of the personal data at hand; the power (im)balance between the data subject and controller; the public availability of the respective personal data and the reasonable expectations of the data subject regarding the (intended) processing activity.[1364] The outcome of a balancing test can thus vary on a case by case basis. It must be noted that the controller always has to keep records of the balancing tests he has carried out.

Tailored marketing for frequent renters

An AV rental company might want to tailor future service offers to their frequent renters, based on their likely needs, which may show from their earlier use of the rented vehicles, for instance in terms of number of passengers, distance covered, locations and environments where AVs had been used. These data are personal data, as they (indirectly, in combination with the rental records kept by the rental company) identify the renter, and perhaps also the passengers. There are two obvious legal bases that can be used by the controller (the rental company): *consent*, and *legitimate interests of the controller* (notwithstanding the circumstance that an exception to the prohibition to process *special category data* needs to be ascertained, as location data qualify as such according to the EDPB,[1365] see further section

[1361] Rechtbank Midden Nederland, 23 November 2020, ECLI:NL:RBMNE:2020:511 (*VoetbalTV*).
[1362] Kamara & De Hert 2018, p. 14.
[1363] See CJEU *Bloc M5A*, no. 46; 50.
[1364] See Kranenborg & Verhey 2018, p. 159-160; *inter alia* referring to CJEU 24 November 2011, C-468/10 & C-469/10, ECLI:EU:C:2011:777 (*ASNEF*).
[1365] EDPB 2020/01, p. 12. Geolocation data may reveal *inter alia* sexual orientation or religious beliefs, through places visited.

5.2.5). [1366] As obtaining *consent* and the fact that it can be easily withdrawn, can be problematic, the rental company may want to opt for the *legitimate interests* ground. He may state (although it is a bit uncertain whether this would be 'durable' given the current opinion of the Dutch AP) that he has a legitimate interest in his "marketing purposes" to make tailored offers to its frequent users. Then, he needs to verify that the intended data processing is indeed necessary to make such personalised offers. When he can establish that he cannot make personalised offers without all intended personal data to be processed, he needs to balance his interests with those of the data subjects. Should the controller evaluate that the intended data processing is not disproportionate to the privacy interests of the data subjects, he could conclude that the *legitimate interests* ground can be used as a lawful basis for his processing activities.

There are several other obligations for the controller to take into account however. He might *inter alia* have to carry out a Personal Data Privacy Impact Assessment (DPIA), and maybe even consult with (the) local DPA(s) (see section 5.2.7). Furthermore, it remains uncertain whether or not the outcomes three-step-test are in conformity with the GDPR/CFR requirements, and can be challenged by the DPA, or by data subjects in court (see section 5.2.10 and 5.2.11).

Enriched driving data for future defence in court?

Another example could be the intended processing of personal data for purposes of a defence in potential future liability claims. As illustrated in section 4.2.2.8, a producer may invoke a *contributory negligence* defence, or a *later-existence* defence in order not to be held liable on the basis of a product liability claim. Therefore, it will be necessary that the producer can for instance produce evidence that the behaviour of the victim contributed to, or resulted in, the damage; or that the producer can prove that the defect which caused the damage came into existence *after* he had put the product into circulation.

For these purposes, a car producer (i.e. the controller) wishes to receive and store "enriched driving data", comprising of *inter alia* continuous information on the driving behaviour of all users of its (non-fully) autonomous vehicles, as well as sensor- and camera data recorded by the respective vehicles. As it is not clear on beforehand which data can be necessary in such *defence*-situations, the producer would like to store as much data as possible.

[1366] Also notwithstanding the fact that article 5(3) ePrivacy directive might apply, when those data are first stored and later extracted from the AV or devices connected to it; see 5.2.4.1. This would not apply for instance when such data are not stored in the AV or connected devices, but instead directly processed on systems of the controller.

Consent is not considered to be the 'best' suitable basis by the producer, as it would be a hard job to acquire consent from *all* respective AV-drivers, and the personal data may only processed as long as consent is not withdrawn by the data subjects. Also the legal obligations under the GSR (see the foregoing section) would not allow the envisaged data-storage and use in this respect. Car producers may however still have a "real and present" legitimate interest in processing and storing (parts of the) the enriched driving data, as some of the cars that they have produced, will unfortunately become involved in traffic accidents. However, the envisaged storing of *all* available data will likely be disproportionate to the indicated purpose, as for instance precise location data, or camera footage of the passengers will often not be required to establish the cause of an accident, and thus to underpin the applicable defences. Furthermore, not all continuous driving data should be necessary, it may be sufficient to store the certain data regarding the moments before and after an accident. Thus, the controller has to specify the personal data that would be minimally necessary for achieving the intended purpose, and not process any other data. He also has to take the rules on *special category data* (see the following section) into account, which may *not* be processed in principle, unless an exception to the prohibition applies. Furthermore, he needs to balance the intended data processing (for legal defence purposes) with the interests of the data subjects whose data are to be processed, and he might *inter alia* have to carry out a DPIA and consult the DPA beforehand. Also, he should incorporate *privacy by design* and *privacy by default* in the technological solution for processing the respective data, as is further illustrated in section 5.2.7.1.

5.2.5 SPECIAL CATEGORY DATA

Where 'regular' personal data may in principle be processed when the controller can demonstrate the existence of a lawful basis, it is by default forbidden to process *special category data*. According to article 9(1) GDPR, *special category data* are formed by personal data revealing:

1. Racial or ethnic origin;
2. Political opinions;
3. Religious or philosophical beliefs;
4. Trade union membership.

Article 9(1) furthermore forbids processing of:

5. Genetic data;[1367]

[1367] Member States may regulate further conditions and limitations in this regard on the basis of article 9(4) GDPR.

6. Biometric data for the purpose of uniquely identifying a natural person;[1368]
7. Concerning health;[1369] or
8. Concerning a natural person's sex life or sexual orientation.

Paragraph 2 lists ten exceptions to the default prohibition. In the light of data processing in the context of AVs, the applicability of the following three can be likely.[1370] First, the prohibition can be lifted in principle when the "data subject has given explicit consent"[1371] to the respective intended processing activities.[1372] It is likely that the necessary consent should be given in conformity with the general rules of article 7 GDPR, and that such consent should see to (more) explicitly formulated purposes.[1373] The EDPB furthermore suggests, "in order to remove all possible doubt and potential lack of evidence in the future", that a "data subject must give an express statement of consent" e.g. in writing and that controller "could make sure the written statement is signed by the data subject",[1374] although this would not preclude other forms of obtaining explicit consent (such as oral consent; consent captured by a recorded telephone conversation; or consent confirmed by "two stage verification").[1375]

Second, it is not forbidden to process *special category* data that have been "manifestly made public by the data subject".[1376] It must show from the behaviour of the data subject, that he intended to publicise the respective special category data.[1377] That may be true when for instance someone has published his medical data online,[1378] but may also implicitly follow from the fact that he

[1368] Ibidem.
[1369] Ibidem.
[1370] The less likely alternatives of article 9(2) GDPR include processing: b) necessary for the "purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection[…]"; c) "necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent"; d) "carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim […]"; g) "necessary for reasons of substantial public interest, on the basis of Union or Member State law […]"; h) "necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional […]"; i) "necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices"; j) "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law".
[1371] Article 9(2)(a) GDPR.
[1372] Unless Member State law provides otherwise.
[1373] See Kranenborg & Verhey 2018, p. 170-171.
[1374] Quotations from EDPB 05/2020, p. 20-21.
[1375] Ibidem,
[1376] Article 9(2)(e) GDPR.
[1377] Kranenborg & Verheij 2018, p. 172.
[1378] See for example AP 2018, p. 41.

allowed his personal data be published in for example phone records,[1379] or in 'yellow pages'. *Special category data* that have been published against the will of the data subject, cannot be used in this regard.[1380]

Third, in cases where processing is necessary "for the establishment, exercise or defence of legal claims", the general prohibition is lifted as well.[1381] Where it is necessary to use certain *special category data* in the course of legal proceedings, i.e. when certain rights cannot be successfully invoked without respective sensitive data being processed, the general prohibition does not apply.[1382]

It must be noted that the existence of an exception to the default processing prohibition of special category data, does not relieve the controller of his duty to also demonstrate a lawful basis in the sense of article 6(1) GDPR. Furthermore, the "extra-special category data" indicated in article 10 GDPR must be observed, which holds that personal data relating to criminal convictions and offences (*offence related data*) must be carried out or delegated by ("under the control of") official authorities, on the basis of EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

> As the EDPB indicated, it is likely that in the deployment of connected vehicles (including AVs), often involves the processing of *special category data*, such as geolocation data and data that can reveal criminal offences or (traffic) violations.[1383]
>
> The EDPB categorises geolocation data as *special category data*, for these are "particularly revealing of life habits of data subjects", and may "reveal sensitive information such as religion through the place of worship or sexual orientation through places visited".[1384] Regarding geolocation data the EDPB suggests that these may in principle not be processed, especially not when there are other options available to fulfil certain purposes. When it is necessary to process location data, for instance to provide weather information, or when pay-per-use business models require the computation of covered distance, the EDPB indicates that location

[1379] Kranenborg & Verheij, p. 172-173.
[1380] This follows *inter alia* from ECJ 16 December 2008, C-73/07, ECLI:EU:C:2008:727 (*Satamedia*), in which it was held that for the application of the data protection rules (then: the regime of the DPD), it is irrelevant whether certain personal data had been published before.
[1381] Article 9(2)(f) GDPR.
[1382] See Kranenborg & Verhey 2018, p. 173.
[1383] EDPB 1/2020, p. 12.
[1384] Ibidem.

data should not be continuously stored and processed; and only with the explicit free, specific and informed consent of the data subject(s) using the vehicle.[1385]

Similar observations are made regarding biometric data (such as voice, fingerprints, and digital models of someone's face for face recognition), that can be used for vehicle access, authentication, and user preference purposes. Also in those cases explicit consent is necessary to lift the general processing prohibition. The EDPB furthermore suggests that alternatives are offered to the data subject, such as car keys or -codes and possibilities to manually configure the car settings to the individual requirements of the driver and passengers.[1386]

The processing of data representing the instantaneous speed of a vehicle and continuous geolocation data could be used to reveal traffic violations (speeding, white line crossing, et cetera). While the EDPB considers that those data are not by itself *offence related data* as defined in article 10 GDPR, it is possible that they become *offence related data* when these would be collected for purposes of investigating and prosecuting a criminal offence – which is reserved to official authorities (or delegates), under strongly regulated conditions. Regarding personal data that *could* reveal criminal offences, the EDPB recommends "to resort to the local processing of the data where the data subject have full control over the processing in question".[1387] Again, explicit consent is necessary to lift the general processing prohibition of continuously recorded location and speed as *special category data*.

5.2.6 RIGHTS OF THE DATA SUBJECT

Data subjects have several rights under the GDPR in order to exercise a certain level of insight in, or influence on their personal data that are processed by, or under auspices of a controller. The *transparency* principle *inter alia* holds active information duties for data controllers.[1388] Furthermore, data controllers have to facilitate that data subjects for instance require that their data are corrected, sometimes even erased, or transferred to another controller. Also, controllers have to take account of the data subject's rights to object against certain forms of data processing, including "automated decision making". These rights are illustrated below. It is also observed that some of these rights implicate serious compliance-challenges for those responsible for personal data processing through AVs.

Information duties

[1385] Ibidem, p. 12-13.
[1386] Ibidem, p. 13.
[1387] Ibidem, p. 14.
[1388] See Kranenborg & Verhey 2018, p. 194; Sharma 2020, p. 198-199.

Articles 12-14 GDPR hold *active information duties* for controllers. Information such as the identity of the controller, the purposes and legal bases of processing activities, the entities amongst which personal data are shared must be proactively shared with data subjects.[1389] Furthermore, data subjects have to be informed of their rights under the GDPR, and *inter alia* data sources, retention periods and, where applicable, automated decision making based on personal data, must be made known to data subjects.[1390] This must be done in a "concise, transparent, intelligible and easily accessible form, using plain and clear language",[1391] free of charge.

> AV-service providers who intend to process personal data of AV-users, or other data subjects, have to inform these people *before* the data will be processed. This duty applies for *all* persons whose data are to be processed. Thus, when for example the bank account details of an AV-renter are processed for invoicing purposes, that renter has to be informed in conformity with the above. Moreover, when for example car passengers (or people outside the AV) are captured on film for safety (improvement) purposes, also these persons need to be informed.

Besides information obligations for controllers, data subjects can exercise certain rights towards controllers which are regulated under articles 15-22 and 34 GDPR. When they choose to do so, controllers have to facilitate this.[1392] It is in principle forbidden to refuse to act upon a request, "unless the controller demonstrates that it is not in the position to identify the data subject".[1393] It is held that controllers have to confirm the identity of the data subject, before allowing the exercise of these rights, in case information is provided orally, or when the controller doubts the identity of the person requesting to exercise data subject's rights.[1394] Controllers have to act relatively quickly on data subject's requests, namely "without undue delay and in any event within one month of receipt of the request".[1395] Information provided ex articles 15-22 (and 13-14 and

[1389] Paraphrased article 13(1) and 14(1) GDPR. These duties see to reducing information-asymmetries between controllers/processors and data subjects, as introduced in section 3.4.
[1390] Article 13(2) and 14(2) GDPR.
[1391] Where the requirements of "conciseness" and "legibility" may come in conflict, a layered approach is allowed, where essential information is provided for first sight, and more detailed information may be provided under a link. See Gawronski, Czarnowski e.a. 2019, p. 118. Information may be provided in writing, by electronic means (where appropriate – for instance through privacy statements on websites), or on request of a data subject, also orally. Besides the information duties ex articles 13-14, there are also more specific information duties, contained *inter alia* in art. 29 and 21(4) GDPR. See Kranenborg & Verhey 2018, p. 194.
[1392] Article 12(2) GDPR.
[1393] Ibidem,
[1394] See 12(1), last sentence; 12(2), last sentence; 12(6) GDPR; Gawronsky, Czarnowski e.a. 2019, p. 121 – 122; Kranenborg & Verhey 2018, p. 193, 201.
[1395] Article 12(3) GDPR. However, when the requests are numerous, or when replying is complex, the one-month-period may be extended with two months. The controller has to inform the data subjects of such delay, including a motivation for that delay. The controller must also inform a data subject of a refusal to act on a request of a data subject, and also of the fact that data subjects can lodge a complaint before the DPA, and that they can seek judicial remedy (Article 12(4) GDPR).

34) GDPR shall be free of charge, unless "requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character".[1396] In those cases, a controller may a) charge a reasonable fee,[1397] or refuse to act on the request. The rights under articles 15 to 22 GDPR comprise the following.

Access right

The right of access to personal data is regulated in article 15 GDPR.[1398] It is seen as conditional to exercise the other rights of data subjects under articles 16 to 22 GDPR.[1399] Article 15(1) GDPR equips the data subject with the right to obtain from the controller information as to whether or not his personal data are processed by that controller. The provision further mirrors articles 13 and 14. This entails that, upon request, a controller is to provide to a data subject *inter alia* the data processing purposes, categories of personal data, (categories of) recipients, intended sharing beyond the EEA-borders et cetera. Furthermore, the controller has the obligation to provide a copy of the processed personal data (in electronic form – unless otherwise requested – when the processing takes place electronically as well),[1400] whereas the 'rights and freedoms of others' have to be respected.[1401] These provisions may have serious implications for controllers, as they have to be able to reproduce a copy of all personal data that are processed regarding a specific data subject, while data of *other* data subjects may not be shared with the person requesting access. This entails that either an extract needs to be made of the respective processed data, or that all files are shared with the party requesting the access, in which all other personal data, are 'blacked out' or otherwise anonymised.[1402] A controller may furthermore leave out protected trade secrets.[1403]

[1396] Article 12(5) GDPR. The controller has to proof that requests are manifestly unfounded or excessive (section 5, last sentence).
[1397] "taking into account the administrative costs of providing the information or communication or taking the action requested"
[1398] This right has also been incorporated in article 8 CFR.
[1399] See Kranenborg & Verhey 2018, p. 201.
[1400] See Sharma 2020, p. 195; Gawronsky, Czarnowski e.a. 2019, p. 137.
[1401] Article 15(3) and (4) GDPR; Gawronsky, Czarnowski e.a. 2019, p 137-138.
[1402] This also implicates that the controller has to make a thorough assessment of which data qualify as 'personal data' of other in this respect. This is not always obvious, as *inter alia* follows from CJEU 17 January 2014, C-141/12 & C-372/12, ECLI:EU:C:2014:2081 (*Y.S.*), in which the CJEU held that a legal analysis in 'the minute' of a draft decision which regarded an application for obtaining a residence permit does not as such qualify as personal data. The court held that: "extending the right of access of the applicant for a residence permit to that legal analysis would not in fact serve the directive's purpose of guaranteeing the protection of the applicant's right to privacy with regard to the processing of data relating to him, but would serve the purpose of guaranteeing him a right of access to administrative documents, which is not however covered by Directive 95/46" (no. 46).
[1403] Recital (63) GDPR;

Right to rectification and right to erasure

Article 16 GDPR regulates that data subjects have the right to rectification of incorrect personal data that a data controller processes regarding them, and that they also have the right to "complete" personal data that were incompletely processed by the controller.[1404]

Under article 17 GDPR, there is a 'right to be forgotten',[1405] to counterweigh the ever expanding technological possibilities to store and use personal data indefinitely.[1406] A controller has to erase personal data on request of a data subject "without undue delay", when: respective data are no longer necessary regarding the original data processing purposes; consent is withdrawn (and there is no other legal ground for the processing); the data subject objects to the processing,[1407] and there is no overriding legitimate ground; personal data have been unlawfully processed; erasure is necessary to comply with Union- or Member State law; or when personal data have been collected in relation to the offer of information society services referred to in Article 8(1) GDPR, to a child.[1408] Not every erasure-request has to be granted. Requests may be denied when processing is for instance necessary for exercising the right of freedom of expression and information,[1409] and for complying with obligations following from Union- or Member State law.[1410] It must be recalled that the obligation to erase personal data, is in principle limited to Member States and states in which Union-law applies.[1411]

> One of the envisaged means to log and store data that are generated by the use of AVs, with a minimum risk of manipulation of those data, uses *blockchain technology*.[1412] Blockchain-

[1404] It follows from art. 19 GDPR that a controller has to inform every recipient of personal data to whom personal data have been disclosed, of any rectification or erasure, unless this would be impossible or involves "disproportionate effort". On request of the data subject, the controller has to inform the data subject of the recipients who have been informed under article 19. See Kranenborg & Verhey 2018, p. 207. The right of rectification does however not enable a data subject (i.e. an exam candidate) to "'correct', *a posteriori*, answers that are 'incorrect'": CJEU *Nowak*, no. 52.

[1405] The introduction of this article is partly the result of the CJEU decision in the *Google/Mario Costeja Gonzáles* case.

[1406] See Kranenborg & Verhey 2018, p. 207.

[1407] On the basis of art. 21(1); see section 3.5.

[1408] Article 17(1) GDPR, my paraphrasing. The second paragraph requires a controller who has made personal data public, "taking account of available technology and the cost of implementation", to take reasonable steps to inform others controllers who are (still) processing respective data, of a request to erase (copies of or links to) that data. It follows from art. 19 GDPR that a controller has to inform every recipient of personal data to whom personal data have been disclosed, of any rectification or erasure, unless this would be impossible or involves "disproportionate effort". On request of the data subject, the controller has to inform the data subject of the recipients who have been informed under article 19. See Kranenborg & Verhey 2018, p. 207; Garnowski, Czarnowski e.a., 2019, p. 155

[1409] Controllers may thus have to make a careful evaluation of on the one hand the right of the data subject to be 'forgotten', and on the other its own right (freedom to conduct business) and of potential third parties to receive certain information, as was the case in CJEU *Google/Mario Costeja González*.

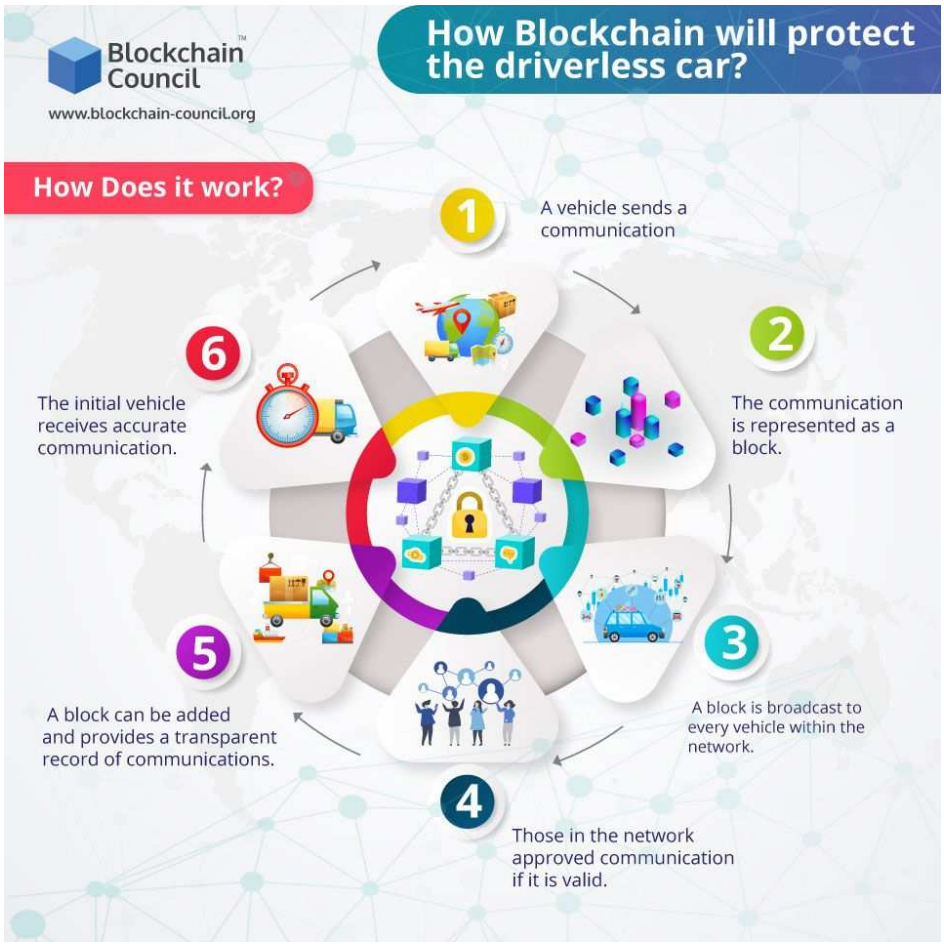
[1410] Article 17(3) GDPR, my paraphrasing.

[1411] CJEU *Google/CNIL*.

[1412] See also Chapter Chapter 6 (case study) and section 2.3 (on AVs and tracing technology). See Guo, Meamari & Shen 2018; Rathee e.a. 2019; Baza e.a., 2019.

based technology can be of valuable assistance to determine accident causes, and thus to help allocating (and apportioning) liability.[1413] In a blockchain,[1414] many different actors "nodes" participate. Bits of information are stored in timestamped "blocks". Such blocks may for example contain information processed by AVs, including for instance location, direction, speed, applied braking power, speed, other traffic participants, et cetera.

Blocks can be added to a "chain" of other blocks, but only after the contents of such block (together with previous blocks) have been verified by (a number of) the other participants. A "blockchain" thus consists of a series of verified blocks. Altogether, these blocks are comprised in a "ledger". Every participant holds a copy of that ledger, which is not stored on a central server. Hereunder, I copied the infographic by the BlockChain Council which depicts how AV information can be stored in blocks of a blockchain:[1415]



[1413] Guo e.a., 2019, p. 1.
[1414] See for a simple explanation of blockchain: Gaurav, "What is Blockchain? A Simple Guide for Dummies", *coincoecap.com*, 4 April 2020, via https://blog.coincodecap.com/what-is-blockchain-a-simple-guide-for-dummies (last accessed 20 July 2020).
[1415] Blockchain Council via twitter, "How Blockchain will protect the driverless car?", 29 January 2019, https://twitter.com/ChainCouncil/status/1090119880580493312, (last accessed 20 July 2020).

As all participants have a copy of the all the blocks in the chain, and the individual blocks are used to verify additions by individual nodes to the chain, it is almost impossible to temper with the contents of existing blocks. This also implicates that it would be technically very difficult to *ex post* rectify, complete or erase personal data under article 16 GDPR.[1416]

The right to rectification, and the right to be forgotten also has problematic implications when 'regular' storage technologies are used. The scope of the obligations namely extends to *all* copies of personal data, including those in back-ups for example.[1417]

Right to data portability

Each data subject has the right to *data portability i*n cases where he provided his personal data to a controller on the basis of consent (in the sense of article 6(1)(a) or 9(2)(a), or for the execution of a contract (6(1)(b) GDPR).[1418] This holds that the controller provide to the data subject the processed data "in a structured, commonly used and machine-readable format". Furthermore, the data subject has the right to request that the controller transmits (without hindrance) the respective data to another controller.[1419]

Controllers responsible for personal data acquired by them either directly from the data subjects, i.e. AV users, or on the basis of their behaviour, have to take the *data portability* provisions into account, when their data processing is based on consent or execution of a contract. It follows from Recital 68 to the GDPR that the *data portability* obligations are *inter alia* to stimulate inter-operable file formats, which is something to take into account when designing database models for AV user-data.

Right not to be subject to automated decision making and profiling.

Data subjects have the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[1420]

According to WP29, the provisions of article 22 GDPR see to *inter alia* the prevention of certain risks that may follow from profiling and other forms of automated decision

[1416] See Verhelst 2017, p. 21; Kranenborg & Verhey 2018, p. 207; See also Guo e.a., 2019, p. 3.
[1417] See Gawronski, Czarnowski e.a., 2019, p. 151-152; Kranenborg & Verhey 2018, p. 212-213.
[1418] Article 20(1) GDPR. WP29 held that also personal data that follow from the behaviour of a data subject "observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities" are in scope of article 20 GDPR: WP29 (242), p. 9-10. See also Gawronski, Czarnowski e.a., 2019, p. 163
[1419] Article 20(2) GDPR, which applies insofar as "technically feasible". Also under article 20(4) GDPR, the rights and freedoms of others may not adversely be affected. This implicates *inter alia* that personal data of others than the data subject requesting portability, should be excluded
[1420] Article 22(1) GDPR.

making. Such risks can include stereotyping, creating a lock-in for persons based on 'suggested preferences', limiting the individuals' freedom to choose certain products and services, such as books, music and newsfeeds.[1421] Even worse, profiling and automated decision making can induce inaccurate predictions of preferences or behaviour, and "denial of services and goods and unjustified discrimination".[1422]

Article 22 GDPR applies to any form of solely automated decision making with "legal effects" or similar significant effects for data subjects.[1423] WP29 defines *solely automated decision making* as "the ability to make decisions by technological means without human involvement".[1424] Such decision making may be done in correlation with profiling,[1425] but profiling is not necessarily part of the automated decision making in scope of the article. As WP29 illustrates: "[i]mposing speeding fines purely on the basis of evidence from speed cameras is an automated decision-making process that does not necessarily involve profiling".[1426]

The other requirement for applicability of article 22, is that automated decision making must have legal effects (or significant other, similar effects) for individuals. The wording of this provision is broad, and not limited to any kinds of legal (or similar) consequences. WP29 illustrates that examples of legal effects may include: "cancellation of a contract; entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit; refused admission to a country or denial of citizenship".[1427]

> Certain AV decisions might fall under the scope of article 22. Let us assume that in some (urban) area's there is a higher risk of damage to a car than in others, and that an AV has access to those data. When algorithms in an AV predict the preferences (on the basis of *inter alia* earlier use and the personal agenda of the user) of a certain 'driver', and correlate these with the data on damage risks in order to offer individualised tariffs and rates to AV users on the basis of a pay-as-you-drive business model, the article 22 provisions apply. There is an automated decision in the

[1421] WP29 (251), p. 5-6.
[1422] Ibidem.
[1423] It is observed that such effects are mostly negative for data subjects. See for instance Gawronsku, Czarnowski, e.a., 2019, p. 179-180.
[1424] Ibidem, p. 8.
[1425] See the following section.
[1426] WP29 (251), p. 8.
[1427] Ibidem, p. 21

individualised tariffs. That decision is based on solely automated processing of earlier use-data in combination with the user's personal schedule, correlated with a potential damage calculation. The individualised tariffs implicate a legal effect (i.e. price to pay for the services).

This right, or more accurately: prohibition for data controllers,[1428] does not apply when such decision is necessary to enter into, or to perform a contract; when the decision is authorised under applicable (Union- or Member State) law which appropriately ensures measures to safeguards the rights, freedoms and legitimate interests of data subjects; or when such decision making is based on the *explicit consent* of the data subject.[1429] In those cases (except in case of authorised decision making on the basis of legal provisions), the controller must implement "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". Furthermore, automated decisions may not be made on the basis of special category data, unless explicit consent is obtained, or a substantial public interest legitimates such processing.[1430]

Revisiting the example above on "smart tariffs", it can be argued by a controller that such automated tariff calculation is believed to be the most appropriate way, as 'human' processing of all the relevant information is more difficult and time consuming. Furthermore, the calculation can be legalised when *explicit consent* is obtained from the data subject.

It must be noted, that besides the general prohibition and the possibly applicable exceptions thereto, the other obligations including *inter alia* the information duties of articles 13(2)(f) and 14(2)(g) GDPR are to be observed.[1431] This implicates that data subjects must be informed of the existence of automated decision making processes, and are to be provided with meaningful information regarding the logic underlying the algorithms, as well as the significance and envisaged impact for the data subjects.[1432] These obligations are furthermore reflected in the data subject's access right ex article 15(1)(h) GDPR. This

[1428] Ibidem, p. 19-20.
[1429] Article 22(2)(a-c) GDPR, my paraphrasing.
[1430] Article 22(4) GDPR.
[1431] See Kranenborg & Verhey 2018, p. 220.
[1432] See also Sharma 2020, p. 223-224.

entails that a data subject has the right to know which specific decisions have been made regarding him, on the basis of automated data processing.[1433]

Right to object

Article 21(1) GDPR applies when personal data are processed on the basis of public interest or the legitimate interest-provisions. Data subjects may object to such data processing, "on grounds relating to his or her particular situation". Explicitly included in the *right to object* is when "profiling based on those provisions" occurs.

Profiling means

> "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[1434]

Shortly, profiling sees to forms of use of personal data enabling the assessment or prediction of behaviour of individuals. This includes for example credit rating of an individual based on his (predicted) behaviour, targeting advertisements to users based on their behaviour (likes, searches and posts) on social media, and defining an individual insurance premium based on the driving behaviour of the insured person(s).[1435]

When a person objects to certain data processing, the controller is to stop that processing activities, unless he can show "compelling legitimate grounds […] which override the interests, rights and freedoms of the data subject", or when processing is necessary for the "establishment, exercise or defence of legal claims".[1436] Under the first paragraph, controllers thus have certain means for not-complying with a request to stop on the basis of a data subjects' right to object, when they can motivate "compelling legitimate grounds". Controllers do not have that option when personal data are used for direct marketing purposes: [1437] objection implicates the obligation to cease the respective data processing in those cases.[1438]

[1433] WP29 (251), p. 27.
[1434] Article 4(4) GDPR.
[1435] See Gawronski, Czarnowski, e.a., 2019, p. 176-177; Kranenborg & Verhey 2018, p. 219.
[1436] Article 21(1), last sentence, GDPR.
[1437] Article 21(2-3) GDPR; see Kranenborg & Verhey 2018, p. 216.
[1438] See Gawronski & Czarnowski 2018, p. 171.

The right to object must be actively brought under the attention of the data subjects whose data are to be processed,[1439] and a data subject must be enabled to object by automated means.[1440]

> Taken together, the rights of data subjects which have been strengthened under the GDPR, provide on the one hand more tools for data subjects to *control* personal data processed by controllers and processors. On the other hand, however, the obligations that these rights implicate for controllers and processors can form a serious challenge to comply with. When AV-data are to be stored in a decentralized way using for instance blockchain techniques, it will even be virtually impossible to meet obligations resulting from the rights to rectification and erasure.

5.2.7 OBLIGATIONS FOR CONTROLLERS

Chapter IV of the GDPR regulates the (other) obligations for controllers and processors. In the following sections, some of these are illustrated. I have chosen to elaborate those obligations which are especially relevant for controllers and processors of AV related personal data and which contain 'open norms', as these leave most room for interpretation by both the regulates and the supervisory authorities. I start with the 'general obligations' under the accountability principle in section 5.2.7.1, The privacy by design and by default principles are highlighted in section 5.2.7.2. Section 5.2.7.3 addresses Data Privacy Impact Assessments. Codes of conduct and certification mechanisms, which can be used to specify the open norms regulated under the GDPR and to demonstrate compliance therewith in section 5.2.7.4.

5.2.7.1 *Accountability*

Article 24 GDPR elaborates the general *accountability principle* for controllers.[1441] This principle enshrines both administrative and material obligations. Regarding the material duties, it must be noted that article 24 holds that the controller is responsible and must at all times *account for* the protection of the personal data that he processes, and thus for the privacy of the persons to whom these data relate. In order to do so, controllers (and processors) must for example keep records of their data processing activities.[1442] Those records must be made available to the DPA on request, and can be used as a starting point to illustrate (or investigate) compliance. Furthermore, controllers must document their agreements with processors.[1443] Controllers may only use the services of processors who can in turn demonstrate that they are complying with the GDPR

[1439] Article 21(4) GDPR.
[1440] Article 21(5) GDPR.
[1441] See Kranenborg & Verhey 2018, p. 225-226.
[1442] Article 30 GDPR.
[1443] Article 28(3) GDPR.

provisions. Those "data processing agreements" must be in conformity with the provisions of article 28(3) GDPR.

TOMs

The material obligations under article 24 hold that the controller is to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation". Those technical and organisational measures (TOMs), must reflect that the controller took due notice of "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". The measures must be "reviewed and updated where necessary". Article 32(1) GDPR provides more detailed obligations regarding TOMs. It is stated that controllers (and processors) are obliged,

> "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural purposes",

to implement TOMs "to ensure a level of security appropriate to the risk" at hand. TOMs could, according to the first paragraph of article 32, for instance include pseudonymization and encryption of personal data, and backup and restore mechanisms. Although even the specified obligations remain rather vague and open, the EDPB and local DPAs have provides some further guidance.

> The EDPB and the French CNIL have issued more concrete recommendations how to address TOMs relating to certain aspects of personal data processing by or through AVs. The EDPB, largely reflecting the CNIL-guidelines,[1444] for instance advises *inter alia* the following TOMs to be adopted by "vehicle and equipment manufacturers, service providers and other data controllers":[1445] "
>
> - encrypting the communication channels by means of a state-of-the-art algorithm;
> - putting in place an encryption-key management system that is unique to each vehicle, not to each model;
> - when stored remotely, encrypting data by means of state-of-the-art algorithms;
> - regularly renewing encryption keys;
> - authenticating data-receiving devices;

[1444] See CNIL 2018, p. 11.
[1445] EDPB 01/2020, p. 19-20.

- ensuring data integrity (e.g., by hashing);
- make access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.);"[1446]

For vehicle manufacturers, the EDPB has further recommendations: "

- partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment");
- implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;
- for the vehicle's vital functions, give priority as much as possible to using secure frequencies that are specifically dedicated to transportation;
- setting up an alarm system in case of attack on the vehicle's systems, with the possibility to operate in downgraded mode;
- storing a log history of any access to the vehicle's information system, e.g. going back six months as a maximum period, in order to enable the origin of a potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies."[1447]

In a case study on data collection including instantaneous speed (or other data that could reveal criminal offences), the EDPB furthermore recommends implementing strong security measures, such as: "

- implementing pseudonymisation measures (e.g. secret-key hashing of data like the surname/first name of the data subject and the serial number);
- storing data relating to instantaneous speed and to geolocation in separate databases (e.g. using state-of-the-art encryption mechanism with distinct keys and approval mechanisms);
- and/or deleting geolocation data as soon as the reference event or sequence is qualified (e.g. the type of road, day/night), and the storage of directly identifying data in a separate database that can only be accessed by a small number of people."[1448]

The British Centre for Connected and Autonomous Vehicles (CCAV, a governmental organization) has also issued principles for *inter alia* TOMs. The CCAV-principles on the one hand go even beyond what is recommended by the EDPB and the CNIL, as they for instance also address the necessity of "awareness" of the importance of organisational security and

[1446] Ibidem.
[1447] Ibidem, p. 20.
[1448] Ibidem, p. 29.

"ownership" on board level (principle 1);[1449] an approach of security risk assessment that covers the whole supply chain (principle 2);[1450] the necessity of "product aftercare and incident response to ensure systems are secure over their lifetime" (principle 3),[1451] the need to co-operate within the whole supply chain to enhance security (principle 4);[1452] the importance of using a "defence-in-depth approach" (principle 5)[1453]; software security that is managed throughout its lifetime (principle 6); and the necessity to design systems to be resilient to attacks and to be able to respond appropriately when defences or sensors fail (principle 8).[1454] On the other hand, the CCAV-principles are narrower than the EDPB and CNIL recommendations. Regarding *inter alia* the control over stored and transmitted data (principle 7)[1455], for instance no distinction is made between 'normal' and special category personal data, and no attention is paid to *inter alia* pseudonymisation measures, or retention periods. The CCAV does indicate that their list is not exhaustive, referring to standards and guidance from *inter alia* SAE and ISO. [1456]

Besides the EDPB and DPAs, industry stakeholders are also addressing TOMs in AVs. The German Verband der Automobilindustrie issued "Data Protection Principles for Connected Vehicles in 2014",[1457] and, together with the Federal and State DPAs of Germany in 2016, a joint statement on "Data protection aspects of using connected and non-connected vehicles". [1458] The European Automobile Manufacturers Association published the "ACEA Principles of Data Protection in Relation to Connected Vehicles and Services" in 2015.[1459] The compliance package of the French CNIL for connected cars must be noted in this regard too,[1460]

[1449] CCAV 2017, p. 2.
[1450] Ibidem, p. 5.
[1451] Ibidem, p. 8 (principle 3) and p. 13 (principle 6). This corresponds to some extent with the EDPB recommendation to implement "technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle"; and "setting up an alarm system in case of attack on the vehicle's systems, with the possibility to operate in downgraded mode". Principle 6 goes further, by *inter alia* prescribing that "secure coding practices" need to be used
[1452] CCAV 2017, p. 9.
[1453] Ibidem, p. 10. This corresponds to some extents with the EDPB-recommendation to "partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment")", but goes further, in that it highlights *inter alia* the importance of remote monitoring of security as well as remote access when necessary, and one-way-data controls.
[1454] CCAV 2017, p. 17.
[1455] Ibidem, p. 14.
[1456] CCAV 2017, p. 18.
[1457] VDA 2014.
[1458] VDA/German DPAs 2016.
[1459] ACEA 2015.
[1460] CNIL 2018.

as well as the EDPB guidelines of 2020.[1461] Most of these documents contain high-level acknowledgements of the importance of personal data protection.

It can thus be observed that some recommendations on TOMs for AV applications are emerging from different sources, although a comprehensive set containing an integral approach that corresponds with the criteria of article 32 GDPR is not yet available.

The fact that the norms are vague, in combination with the large responsibility and obligations to comply for controllers, and the fact that supervisory authorities have strong enforcement possibilities, is criticized. Gawronski, Kloc e.a. quote in this regard the Head of the EDPB, Andrea Jelinek, who responded to a request for more guidance on GDPR norms: "It's a question of which side of the table you're sitting on; as a regulator, we have tasks too. You don't have to fulfil my tasks, so don't expect me to fulfil yours".[1462] They conclude that "you [controllers, *RWdB*] are processing personal data at your own risk and the supervisory authorities will not tell you the rules until you break them".[1463] That is a very bold statement, since the EDPB and the local DPAs do in fact provide (some) guidance,[1464] although the point they are making regarding the vagueness of norms that can still be enforced with (a prospect of) hefty fines and penalties, is also true.[1465]

Data breaches

Also part of the accountability obligations for controllers under the GDPR regards *personal data breaches*. The GDPR prescribes that personal data breaches need to be reported, to the competent DPA (article 33 GDPR), and sometimes also to the data subjects whose data were involved in the breach (article 34 GDPR). A personal data breach is defined in article 4(12) GDPR as follows: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". According to WP29 (and the EDPB),[1466] "loss" includes situations in which personal data might still exist, but

[1461] EDPB 01/2020.
[1462] This is a quote from mrs. Andrea Jelinek in an interview on GDPR enforcement, as also commented on by Bracy, J., "New WP29 chair talks enforcement, role of the DPO", *iapp.org* 30 March 2018, via https://iapp.org/news/a/new-wp29-chair-talks-enforcement-role-of-the-dpo/ (last accessed 21 July 2020), quoted in Gawronksi, Kloc e.a., 2019, p. 8.
[1463] Ibidem.
[1464] See for instance the guidelines and recommendations referred to in these sections, and on related topics to article 24 GDPR.
[1465] See also Koops 2014, p. 12, who observes that "…regulators have spent relatively little effort to communicate best practices […] and, as observed above, they have a communication problem".
[1466] WP29 (250), as endorsed by the EDPB, see https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_nl.

where a controller no longer has control over, or access to a data set.[1467] This for instance covers cases where copies of databases with personal data are lost or stolen. Also situations in which personal data are encrypted by a third party, who threatens to destroy those data unless a ransom is paid (i.e. *ransomware*) must be qualified as personal data breach.

A controller has, on the basis of article 33(1) GDPR, the obligation to notify the competent DPA as soon as possible after having become aware of a personal data breach,[1468] where feasible: within 72 hours. WP29 explained that when a "controller has a reasonable degree of certainty that a security incident has occurred that has led to the personal data being compromised",[1469] he must be deemed "aware" of a personal data breach.[1470]

When notification within 72 hours is not feasible, the controller has to motivate the reasons for the delay. No notification is necessary when a personal data breach "is unlikely to result in a risk to the rights and freedoms of natural persons". Such situations are rare, but may occur when for instance "where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual".[1471] WP29 furthermore illustrates that

> "if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority".[1472]

However, if it appears later that someone may find a way to unencrypt the data, a notification may still have to be done.

[1467] Ibidem, p. 6-7. It can be noted that WP29 (p. 7) furthermore distinguishes – for classification purposes – between breaches of: confidentiality (unauthorised or accidental disclosure of personal data); integrity (unauthorised or accidental alteration of personal data); availability (accidental or unauthorised loss of, or access to, or destruction of, personal data). See also Gawronski, Chomiczewski, e.a., 2019, p. 246-248.
[1468] Article 33(3) lists the information to be provided to the DPA. It is prescribed that the notification "shall at least: a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c) describe the likely consequences of the personal data breach; d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects". When not all information can be provided within the first 72 hours, it may be provided later (paragraph 4), although "without undue further delay".
[1469] WP29 (251), p. 10-11.
[1470] Ibidem, p. 11. Furthermore, according to WP29, it follows from the requirements of article 32 that a controller has to implement monitoring measures for *inter alia* the discovery of data breaches. Thus, a controller should become aware of personal data breaches "in a timely manner".
[1471] WP29 (251), p. 18. Gawronski, Chomiczewski, e.a. observe these terms to be "fuzzy", and point out that a controller must just act "at once" (p. 249-250).
[1472] Ibidem, p. 19.

Every personal data breach has to be documented, according to – and in line with – the provisions of article 33(5) GDPR.

Article 34 GDPR prescribes that

> "[w]hen the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay".

The GDPR does not explicate when there likely is a "high risk" data breach,[1473] although recitals 75 and 85 are indicative in this respect. WP29 observes in that regard:

> "This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur".[1474]

Thus, the controller needs to carry out a risk assessment, and when it appears that either special category data are involved in a breach, or when the breach results in one of the indicated risks, data subjects have to be informed in principle as well as the DPA.[1475]

> A customer database containing information of AV renters (contact details, billing information and actual locations of the vehicles) gets encrypted by an unknown third party. That party requests several bitcoins to be transferred to an anonymous account in return of a key to unencrypt the data. Fortunately, the controller has an actual back-up ready, which he can deploy to guarantee the continuity of his business and he decides not to pay the ransom money. Despite the fact that there was no loss or alteration of the personal data concerned,

[1473] See Kranenborg & Verhey 2018, p. 238.
[1474] WP29 (251), p. 23.
[1475] Communication to a data subject should be done "in plain language" (paragraph 2), and must describe "nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)". Paragraph 3 articulates exceptions to the notification-obligation. Data subjects do not have to be notified when "a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

the controller may still have make a data breach notification. It cannot be excluded that the unknown third party had, or has, - unauthorized - access to the processed data. Within 72 hours after discovery of the breach, he has to notify the competent DPA. As location data are also processed, which may for instance reveal places of worship of the AV renters, also the data subjects whose "special category data" were stored in the database have to be informed of the personal data breach.

5.2.7.2 Privacy by design and by default

The *privacy by design* and *privacy by default* principles are new under the GDPR and are relevant for AV data controllers and processors. These principles are incorporated in Article 25 GDPR, and form to a certain extent a lex specialis of the TOMs regulated in article 24 and 32.

Article 25(1) holds the *privacy by design principle*. It states that both ex ante, when the means of data processing are determined, and when processing commences, certain measures must be taken. In doing so, account should be taken of "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood of the processing itself". The measures referred to, are to be

> "designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subject".

This provision is rather cryptic,[1476] but generally means that privacy must be taken account of when organisations plan to make changes in their organisation, or in the technological means used within the organisation. Furthermore, when for example developing software code, the *privacy by design* principle prescribes that as little personal data must be processed as possible to reach the desired outcome of that software functionality.

The EDPB has interpreted the *privacy by design* principle for certain connected vehicles-cases.[1477] The EDPB held that, when developing technologies that are to be applied in connected vehicles, they

> "should be designed to minimize the collection of personal data, provide privacy-protective default settings [i.e. *privacy by default,* see hereafter, *RWdB*], and ensure

[1476] Kranenborg & Verhey 2018, p. 226-227; Gawronski, Kloc, e.a., 2019, p. 12; Sharma 2020, p. 398-399.
[1477] EDPB 1/2020, p. 14-17.

> that data subjects are well informed and have the option to easily modify configurations associated with their personal data".[1478]

Furthermore, the Board indicates that specific guidance on how the *privacy by design* and -*default* principles must be embedded in this specific technology, could be beneficial for the industry. The EDPB also gives certain general hints on implementation of these principles. Local data processing is for instance advocated and is preferrable over "cloud" processing – which must be avoided as much as possible according to the EDPB.[1479] When personal data *have to* be processed outside the vehicle, for instance to calculate flexible insurance rates, a minimum amount of personal data must be transmitted, and preferably on an aggregated level. This implicates that not the raw data (regarding for instance "force exerted on the brake pedal, mileage driven, etc.")[1480] are to be transmitted, but rather "aggregate scores", on for instance a monthly basis.[1481]

It must be noted that the European Commission has, while the legislative process of the GDPR was still ongoing, issued a mandate to standardisation organisations CEN, CENELEC and ETSI.[1482] They are asked to develop a standard that can used by producers and service providers in the "security technologies and services sector". The aim is to make standards to allow "manufacturers and service providers to develop, implement and execute a widely recognised "Privacy by Design" (PbD) approach in their processes",[1483] and to draft standards for

> "specifying the privacy and personal data protection management processes with an explanation how to realise them, including descriptions of the necessary roles, tasks, documentation, hardware and software requirements, and templates to be used when applying the requested standard(s)."[1484]

[1478] Ibidem, p. 14.
[1479] Ibidem, p. 15, referring to WP29 (196).
[1480] Ibidem.
[1481] Ibidem.
[1482] Commission Implementing Decision C(2015) 102 final, of 20 January 2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy, via https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548# (last accessed 10 January 2021, hereinafter: EC C(2015) final).
[1483] EC C(2015) final, p. 4.
[1484] Ibidem.

With this decision, the EC is mandating co-regulation [1485] regarding the elaboration and specification of the *privacy by design* principle for one specific sector, which may eventually be used, on a voluntary basis, by organisations in that sector to demonstrate that their products or services have been designed in compliance with the *privacy by design* principles. As Kamara observed, this EC mandate is the first of its kind under data protection legislation. [1486] She furthermore states that this is the "first test" for co-regulation in the (reformed) data protection landscape, indicating that more might follow.[1487]

The *privacy by default* principle is incorporated in article 25(2) GDPR. It holds that:

> "[t]he controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".

Thus, by default (*inter alia* through standard settings in software), personal data processing must be limited, in terms of scope (i.e. only such data may be processed that are necessary for achieving the purpose); quantity (i.e. no more data may be processed than necessary for achieving the purpose); retention period (i.e. data may no longer be stored than necessary for achieving the purpose); and access (i.e. only a specified number of people may have access to the data on a "need to know" basis, rather than an indefinite number of people).[1488]

> When deploying AVs, the *privacy by default* principle dictates that the AVs settings are 'standard' set to:
>
> - process as little personal data as necessary, in both a qualitative and a quantitative way;
> - store personal data as shortly as possible;
> - allow access to personal data only on a need-to-know basis, thus preventing unlimited availability and/or public disclosure.

[1485] See section 3.3.3
[1486] Kamara 2017, p. 12.
[1487] Ibidem, p. 13-14
[1488] See Gawronsky, Czarnowski, e.a., 2019, p. 214-215; see also Kranenborg & Verhey 2018, p. 226-227

The EDPB illustrates the following in a case study regarding a rental car where personal data processing includes: previously visited places, entertainment settings and records on called phone numbers. The *privacy by default* principle prescribes to program standard "settings that prevent third parties from processing data generated by the car's dashboard unless they have the user's consent to enable third party access to that data for a specified purpose".[1489]

5.2.7.3 Data Protection Impact Assessment and prior consultation

Besides the general *accountability* obligations, and more specified duties to ensure appropriate technical and organizational measures for personal data protection, the ex-ante implementation of privacy by design and privacy by default, AV-data controllers who intend to use "new technologies" will often have to carry out a data privacy impact assessment (DPIA) *before* commencing the intend processing activity.

A DPIA must be carried out when an envisaged processing activity is likely to result in "a high risk to the rights and freedoms of natural persons", taking account of "the nature, scope, context and purposes for processing".[1490] In doing so, an assessment needs to be made "of the impact of the envisaged processing operations on the protection of personal data".

Which processing activities might result in a "high risk to the rights and freedoms of natural persons" is addressed in article 35(3) GDPR, and further elaborated by the Article 29 Working Party.[1491] Furthermore, DPAs are to publish lists of "kinds of processing operations" that require DPIas to be carried out, as well as those not requiring such impact assessments.[1492] DPIAs are required at least in the following cases: "

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
c) a systematic monitoring of a publicly accessible area on a large scale".[1493]

[1489] EDPB 1/2020, p. 30-31. See furthermore EDPB 4/2019.
[1490] Article 35(1) GDPR.
[1491] WP29 (248).
[1492] Article 34(4-5) GDPR.
[1493] Article 35(3) GDPR.

The Article 29 Working Party lists a number of factors that may indicate high-risk data processing, which *inter alia* include: evaluation or scoring, including profiling and predicting of preferences and behaviour of data subjects; automated decision making in the sense of article 22 GDPR; processing of (highly) sensitive data, including *inter alia* location data; matching or combining datasets; systematic monitoring; processing data of 'vulnerable' data subjects, such as children or employees; data processing through new technological or organisational solutions, such as Internet of Things-applications.[1494]

The EDPB indicates that

> "[g]iven the scale and sensitivity of the personal data that can be generated *via* connected vehicles; it is likely that processing – particularly in situations where personal data are processed outside of the vehicle – will often result in a high risk to the rights and freedoms of individuals",[1495]

in which a DPIA needs to be carried out. The EDPB highlights that even in cases where a DPIA might not be necessary, "it is a best practice to conduct one as early as possible in the design process".[1496]

DPIAs need to contain at least: "

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned." [1497]

There are many standards available for performing DPIAs.[1498] It is observed by the Article 29 Working Party that there are many standards that correspond with the requirements of the

[1494] See WP29 (248), p. 9-11 for the entire overview.
[1495] EDPB 01/2020, p. 17; see also Kranenborg & Verhey 2018, p. 228-229; Gawronski, Czarnowski, e.a., 2019, p. 222-225.
[1496] Ibidem.
[1497] Article 35(7) GDPR.
[1498] See Gawronski, Czarnowski, e.a., 2019, p. 228-229.

GDPR,[1499] but "that it is up to the data controller to choose a methodology" that is compliant with the GDPR-requirements, which are elaborated by the Article 29.[1500]

When the outcome of a DPIA is that the intended "processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk", the competent DPA should be consulted prior to the intended processing activity.[1501] That DPA is to assess whether or not the intended data processing would infringe the GDPR, and provide their advice to the controller.[1502]

5.2.7.4 *Codes of conduct and certification*

As observed by *inter alia* Von Grafenstein, and Kamara, the legislator made an explicit choice to provide broad (and vague), open norms, and to provide principles rather than specific rules, in order to be as technology-neutral as possible.[1503] In order to avoid too much legal uncertainty resulting from the broadness and vagueness of these norms and principles,[1504] the legislator moreover chose to regulate procedural instruments to install tailor-made specifications on the basis of these open norms. These procedural instruments see to the drafting of rules that apply to certain sectors and can relate to certain (forms of) technology, as much as possible together with the specific *regulatees*. In that, the domain-knowledge of the stakeholders can be used, whereas the legislator couldn't.[1505] The instruments in toolbox of the GDPR, are *inter alia* codes of conduct and certification mechanisms, data protection seals and marks.[1506] These instruments can increase legal certainty for innovators, which can be beneficial to innovation,[1507] "because they enable data controllers and processors to specify and standardise the legal principles and broad legal terms".[1508]

[1499] They even provide a list in an annex to WP29 (248), p. 20-21; see also Kranenborg & Verhey 2018, p. 230.
[1500] WP29 (248), Annex 2, p. 22.
[1501] Article 36(1) GDPR.
[1502] Article 36(2) GDPR.
[1503] Von Grafenstein 2019, p. 6-9; Kamara 2017, p. 2-3.
[1504] Which, according to Von Grafenstein (2019, p. 7-8) both "negatively affects the innovative entrepreneurs and […] the individuals concerned". Innovators are hampered, as they do not "know what the regulator is expecting from them"; while in another scenario the regulate *does* know what is expected from him, but "does not want to meet the regulator's expectations and uses the broadness and vagueness of the legal provisions as a loophole, abusing its advanced knowledge about its specific entrepreneurial circumstances to detriment the individuals concerned".
[1505] Von Grafenstein 2019, p. 6, referring to Eifert, M., "Regulierungsstrategien" (Regulation Strategies), in Hoffmann-Riem, W., Schmidt-Aßmann, E, and Voßkuhle, A. (eds.), *Grundlagen des Verwaltungsrechts – Band I*, "Methoden – Maßstäbe – Aufgaben – Organisation", München: C.H. Beck 2012, p. 59.
[1506] According to Kamara (2017, p. 2), the legislator also envisaged the creation of standards as one of the tools in the regulatory toolkit.
[1507] As long as the (financial) burdens are not too high, especially for smaller sized organisations – see Von Grafenstein 2019, p. 9-10.
[1508] Ibidem, p. 10, see also his references in footnote 37.

Article 40 and 41 GDPR regard codes of conduct. Certification (including data protection seals and marks) is addressed in article 42 and 43.

Codes of conduct

Member States, the EDPB, DPAs and the EC should, according to article 40(1) GDPR, encourage the

> "drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small, and medium-sized enterprises".

Codes of conduct can be drafted for specific sectors, and contain specifications of the open norms encompassed in the GDPR, that are tailored for the respective sector. As the second paragraph indicates, this form of co-regulation,[1509] can *inter alia* regard fairness and transparency of processing; ways of data collection; specified legitimate interests; measures of pseudonymisation, privacy by design and -default; sector-specific TOMs; ways to inform data subjects and ways in which they can exercise their rights; ways to notify authorities and data subjects of personal data breaches; international transfers of personal data; and (alternative) dispute resolution mechanisms.[1510]

Codes of conduct can be prepared by "associations and other bodies representing categories of controllers and processors", who have to consult with the relevant stakeholders, where possible including data subjects, who are addressed in those codes.[1511] Once drafted, the code of conduct must be sent to the competent DPA, who is to provide an opinion regarding compliance with the GDPR, and to approve it when it is observed that the code of conduct "provides sufficient appropriate safeguards" – but only when data processing within the borders of one Member State is envisaged.[1512] Then, the code of conduct shall be published by the local DPA.[1513] When data processing is to occur in more than one Member State, the local DPA shall first submit the draft code to the EDPB, who will in turn assess the compliance with GDPR norms, and whether or not it contains appropriate safeguards.[1514] When the EDPB is of the opinion that the draft code of conduct is compliant and holds appropriate safeguards, it will submit its opinion to the European Commission.[1515] The Commission in turn may decide that an approved code of conduct shall have

[1509] See further section 3.3.3.
[1510] See article 40(2) GDPR. The criteria for codes of conduct are further elaborated in EDPB 1/2019.
[1511] This follows from art. 40(2) read in conjunction with recital (99) GDPR; see also Kranenborg & Verhey 2018, p. 241.
[1512] Article 40(5) GDPR.
[1513] Ibidem, paragraph 6.
[1514] Ibidem, paragraph 7.
[1515] Ibidem, paragraph 8.

general validity within the Union, by means of an implementing act,[1516] and publish the code of conduct.[1517] It is for the EDPB to collate all approved codes of conduct (as well as amendments and extensions) in a register, which must be made publicly available.[1518]

> Although to date (12 August 2021) the register is almost empty (it contains 3 codes of conduct), it would improve legal certainty for controllers and processors - and data subjects were to draft one or more codes of conduct. In doing so, more sector-specific guidance can be provided regarding the myriad of open norms contained in the GDPR.
>
> Also in the Netherlands, England and France, the registers on GDPR-codes of conduct are rather empty. The AP (Nl) however, has published a draft opinion regarding the "Data Pro Code", drafted by NederlandICT (now: NLDigital), applicable to IT-providers in the Netherlands.[1519]

Besides elaborated material norms, codes of conduct must also see to the designation of "a body which has an appropriate level of expertise in relation to the subject matter of the code and is accredited for that purpose by the competent supervisory authority", [1520] although without prejudice to the tasks and powers of the competent DPA. Article 41(2-6) contains criteria to assess the appropriateness of such a monitoring body and accreditation. A monitoring body is to act as a 'mini DPA', which has to supervise the activities of controllers and processors under the code of conduct. It can take measures such as "suspension or exclusion of the controller or processor concerned from the code",[1521] and inform the DPA thereof.

When an organisation (controller or processor) adheres to an approved a code of conduct, this may aid them in demonstrating compliance with the GDPR-norms. However, sheer adherence to a code of conduct, does not automatically implicate GDPR compliance.[1522]

Certification

Article 42(1) GDPR stipulates that data protection certification mechanisms, as well as data protection seals and marks, must be encouraged by the Member States, DPAs, EDPB and the

[1516] Ibidem, paragraph 9.
[1517] Ibidem, paragraph 10.
[1518] Ibidem, paragraph 11. The register is kept online, via https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_nl. To date (12 August 2021), three codes of conduct have been incorporated in the register.
[1519] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ontwerpbesluit-ap-gedragscode-nederland-ict, last accessed 22 July 2020.
[1520] Article 40(4) jo. 41(1) GDPR.
[1521] Article 41(4); Kranenborg & Verhey 2018, p, 241.
[1522] See Kranenborg & Verhey 2018, p. 239.

European Commission. Also regarding certification mechanisms, the specific needs of micro, small and medium-sized enterprises have to be taken into account.

Adherence to certification mechanisms, seals or marks can be used to demonstrate compliance with the GDPR norms, also by those who are not subject to the GDPR the territorial scope does not apply to them.[1523] However, having a certification does not reduce the responsibility to remain in compliance with the GDPR, or the competence of the DPA.[1524]

Certifications can be issued by the DPA, or by certification bodies, that are accredited by the DPA,[1525] or the EDPB. When a certification body is accredited by the EDPB, it may award "the European Data Protection Seal". In order to be granted a certificate, controllers or processors have to provide all relevant information and access to the processing activities to the certification body, or DPA.[1526] Certificates can be issued for a maximum period of three years, which can be renewed. When the requirements are no longer met, the certification body or DPA can withdraw the certification.[1527]

All certification mechanisms and data protection seals and marks are to be collated and made available in a register kept by the EDPB. This register is empty to date (12 August 2021).[1528]

To conclude, it can be remarked that the co-regulatory strategy of the legislator to explicate and to tailor the vague and open norms that comprised in the GDPR to the specific needs and requirements of certain sectors and/or processing operations, is not (yet) very successful, as only 3 codes of conduct have been approved so far. The increase legal certainty (which may be beneficial to innovation and protection of the data subjects),[1529] that might result from those instruments, is very limited.

5.2.8 Obligations for Processors

The obligations for processors are addressed in the same chapter as those for controllers, i.e. Chapter IV GDPR. Mostly, stronger obligations apply for controllers, lighter obligations apply for processors. In the following section, an overview is provided of the obligations for processors.

[1523] Article 42(1) and (2) GDPR. "External" controllers or processors have to make "binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects". See Kranenborg & Verhey 2018, p. 242-243.
[1524] Article 42(4) GDPR.
[1525] Ibidem, paragraph 5 jo. Article 43 GDPR.
[1526] Article 42(6) GDPR.
[1527] Ibidem, paragraph 7.
[1528] https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_nl (last accessed 12 August 2020).
[1529] See Von Grafenstein 2019, p. 7-8.

Where applicable, reference is made to the corresponding (stronger) obligations for controllers, elaborated in the foregoing section.

A general "responsibility" as enshrined for controllers in article 24 GDPR (regarding accountability and TOMs),[1530] does not equally apply to processors. Neither do they have direct obligations relating to *inter alia* the implementation of privacy by design and -default principles. However, there are explicit obligations for processors addressed for instance in article 28 and 29 GDPR.[1531] The latter article provides that a processor (or any other person under the authority of the processor or the controller), who has access to personal data, may not process such data, except on (written) instructions of the controller, or on the basis of Union- or Member State law.

Article 28 stipulates, among many other things, that they have to enter in a formal relationship with controllers (a data processing agreement, or a comparable instrument),[1532] which has to be in conformity with the provisions of paragraph 3 and following, and that they have to provide to controllers "sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject." Being held thereto based on a data processing agreement or comparable instrument, the processor has certain obligations on the basis of article 28(3) GDPR towards the controller. These obligations include *inter alia* that the processor may only process personal data on the basis of documented instructions of the controller; that only authorised personnel is entrusted with access to the data, who must be bound to confidentiality; that the processor takes all necessary measures required pursuant to article 32; [1533] that he only uses the services of sub-processors under certain circumstances (see hereafter). Also, the processor is to assist the controller in taking appropriate technical and organisational measures, insofar as possible, to fulfil the controller's obligations regarding responding to requests of data subjects.[1534] The processor is furthermore obliged to assist the controller in ensuring compliance with is obligations with regard to TOMs;[1535] DPIAs and prior consultation.[1536] When the engagement ends, the processor has in principle either to return or to destroy the processed personal data, at the choice of the controller. A processor also needs to

[1530] A processor does however also have to keep a record of processing activities (article 30(2) GDPR), which must be presented to the DPA (4)) and has to cooperate with the DPA as well (article 31 GDPR).
[1531] See for an overview of the obligations of controllers under this article, section 5.2.7.1. See also Sharma 2020, p. 112 ff.; Gawronski & Kloc 2018, p. 81 ff.; and Kranenborg & Verhey 2018, p. 132-133.
[1532] Union- or Member State law that binds the processor towards the controller (paragraph 3) or standard contractual clauses laid down by a DPA (paragraph 8); the European Commission (paragraph 7); or following from a certification mechanism (paragraph 6) could also suffice.
[1533] See section 5.2.7.1.
[1534] See section 5.2.6.
[1535] As addressed in article 32 GDPR, see section 5.2.7.1
[1536] As addressed in article 35 and 36 GDPR, see section 5.2.7.3.

make available to the controller all the information necessary for the controller to demonstrate compliance with article 28 and must enable audits and inspections (mandated) by the controller. A processor is held to report any instructions by the controller that are, according to the processor, not in line with the applicable rules. Furthermore, processors may not engage (other) sub-processors without (written) permission of the controller in principle,[1537] and the same obligations must be agreed with sub-processors as agreed between the controller and processor.[1538]

When the processor does *not* obey to the rules set out in article 28, and determines the means and purposes for data processing himself (thus neglecting the instructions of the controller), he is held to be controller himself in terms of the GDPR, which would thus trigger the applicability of all obligations that the GDPR imposes on controllers.

Besides the obligations towards controllers, processors must themselves keep records of processing activities in conformity with (less strict rules of) article 30(2) GDPR. Also, a processor is obliged to cooperate on request with the competent DPA, under article 31 GDPR.

As stated above, the processor has the substantive obligation to implement TOMs; the requirements are the same as for controllers. However, he does not have to notify DPAs or data subjects of data breaches. Instead, he must inform the controller ex article 33(2) GDPR. The obligation to designate a DPO applies to processors, as follows from article 37.

Furthermore, besides controllers, also processors could adhere to codes of conduct, or certification mechanisms, seals or marks in order to help demonstrating that they comply with the GDPR rules.[1539]

5.2.9 INTERNATIONAL TRANSFER OF PERSONAL DATA.

As personal data processing, including for AV-related purposes, increasingly occurs through cross-border services, it is relevant to illustrate some aspects of the rules that apply to personal data transfer beyond the borders of the EEA, especially in the light of recent case law of the CJEU, which in principle invalidates most grounds that are used for the legalisation of such transfers.

Personal data may in principle not be transferred[1540] to third countries (i.e. non-EEA countries) or international organisations (hereinafter together referred to as "third countries"), unless the

[1537] Article 28(2) GDPR.
[1538] Ibidem, paragraph 4.
[1539] See article 40-43.
[1540] Transferring does not encompass the sheer making available of personal data on a website; it sees to the intended sending from the one actor to the other. See Kranenborg & Verhey 2018, p. 264-265, referring to CJEU 6 November 2003, C-101/01, ECLI:EU:C:2003:596 (*Lindqvist*)

provisions of Chapter V GDPR are complied with, "in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined".[1541] The legislator thus assumes – by default – that third countries have a lower level of protection than that guaranteed by the GDPR,[1542] and the ECHR.[1543] There are three bases for legitimate transfer of personal data to third countries, being *adequacy decisions* (section 5.2.9.1); *appropriate safeguards* (section 5.2.9.2) and; *binding corporate rules* (section 5.2.9.3).[1544]

5.2.9.1 Adequacy decisions

Article 45(1) GDPR enables the European Commission to make and *adequacy decision*, regarding that a specified third country (or organisation) ensures an adequate level of personal data protection. Before deciding on such adequacy, the EC is to evaluate *inter alia* a) the rule of law and the respect for human rights and fundamental freedoms in legislation and case-law of the respective country;[1545] b) the existence and effective functioning of one or more independent supervisory authorities and their enforcement powers;[1546] and c) international commitments of the respective country regarding the protection of personal data.

To date (12 August 2021), the EC has issued adequacy decisions for Andorra; Argentina; Canada (commercial organisations); Faroe Islands; Guernsey; Israel; Isle of Man; Japan; Jersey; New Zealand; Switzerland; Uruguay and South Korea, as well as Great Britain.[1547]

There is a problem with adequacy decisions regarding the United States. The CJEU has decided on two occasions that the adequacy decisions regarding the US were invalid. It first regarded the "Safe Harbor" decision of the EC, and second, the "Privacy Shield" framework. In CJEU *Schrems I*, the court held that in a respective third country, at least a "high level of data protection" must be ensured in order to ascertain *adequate protection*.[1548] Furthermore,

> "the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of

[1541] Article 44 GDPR.
[1542] See Kranenborg & Verhey 2018, p. 263.
[1543] See CJEU 6 October 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*), np. 72.
[1544] Those are the general basis that can be used to underpin international transfer of personal data. Besides these, there also are *special* grounds for transfer, which are listed in article 49 GDPR. These comprise *inter alia* informed consent; performance of a contract at the request of the data subject, or in the interest of a data subject; public interest; the pursuit of legal claims; or vital interests of the data subject; or in some exceptional circumstances, the compelling legitimate interests of the controller (of which the DPA and the data subject must be informed). See Gawronski, Kloc, e.a. 2019, p. 101-103; Kranenborgh & Verhey 2018, p.270-272.
[1545] See article 45(2)(a) GDPR for all the details to be assessed.
[1546] Ibidem, sub b.
[1547]. See for a more comprehensive list, also including adequacy decisions in negotiation Sharma 2020, p. 164-165.
[1548] CJEU *Schrems I*, no. 72.

> protection of fundamental rights and freedoms that is **essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter**"[1549] (emphasis added by me)

of fundamental rights in the European Union. With regard to the Safe Harbor decision, the CJEU found that its framework enabled the interference of fundamental rights of EU citizens, as a result of American national security and public interest requirements.[1550] It was even found that

> "United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security".[1551]

Furthermore, there were no effective supervision and enforcement mechanisms in place, and there were no appropriate means for data subjects to seek administrative or judicial redress towards US based controllers or processors, and could in fact not exercise their rights of access to, and rectification/erasure of personal data. Among many other things, this was held to be an unjustified breach of the privacy rights of EU citizens. The CJEU therefore concluded that the Safe Harbour decision was invalid.[1552]

The Safe Harbor decision was withdrawn and, after intensive negotiations, eventually replaced by the EU-US Privacy Shield (Privacy Shield).[1553] Although Privacy Shield contained more safeguards for data subjects, this decision was invalidated too by the CJEU.[1554] The Court observed that, although the EC earlier found that the US ensures an adequate level of protection, adherence to the Privacy Shield

> "may be limited, inter alia, 'to the extent necessary to meet national security, public interest, or law enforcement requirements'. Thus, that decision lays down, as did Decision 2000/520, that those requirements have primacy over those principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles without limitation where they conflict with the requirements and therefore prove incompatible with them (see, by

[1549] Ibidem, no. 73.
[1550] As a result of the revalations by Edward Snowden.
[1551] Ibidem, no. 90.
[1552] Ibidem, no. 106.
[1553] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *OJ* L 207/1.
[1554] CJEU 16 July 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).

analogy, as regards Decision 2000/520, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 86)".[1555]

The CJEU then finds that the capacities of US authorities on the basis of surveillance programs regarding the access to and use of personal data of EU citizens, while data subjects are not entitled to "actionable rights before the courts against US authorities"[1556] are not limited and precise enough and therefore disproportional. The "new" Ombudsperson-mechanism installed by the Privacy Shield, does furthermore not equip EU citizens with sufficient cause of action,[1557] towards *inter alia* US intelligence services. Therefore, the CJEU declared the Privacy Shield invalid.[1558]

The invalidation of Privacy Shield entails that there is no longer a valid adequacy decision in place for data transfer between the EU and US-based organisations. This does however *not* implicate that any transatlantic transfer of personal data is prohibited, as this could still be (legally) based on EC model clauses or Binding Corporate Rules. However, the *Schrems II*-decision also implicates stricter conditions for these bases, as is illustrated hereafter.

5.2.9.2 Appropriate safeguards

Article 46(1) GDPR regulates the alternative bases for personal data transfer to third countries in the absence of an adequacy decision. As a rule, it states that such processing may only take place "if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and legal remedies for data subjects are available". Such appropriate safeguards may be there, *inter alia* in cases of standard data protection clauses, adopted by the EC, or approved by the EC; of binding corporate rules (see the next section); and/or of approved certification mechanisms or codes of conduct. In such cases, no prior authorisation is required by a DPA.[1559]

Often used are the EC Standard Contractual Clauses.[1560] One of those addresses the intended transfer of personal data between an EU-based controller and a non-EU/EEA-based processor.[1561] This set of model clauses has been the object of the CJEU *Schrems II*-decision too. The Court *inter alia* observed that also when these model clauses are used to "legalise" the international transfer

[1555] CJEU *Schrems II*, no. 164.
[1556] Ibidem, no. 192.
[1557] Ibidem, no. 197.
[1558] Ibidem, no. 199.
[1559] The third paragraph contains measures that need prior DPA authorisation.
[1560] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. See for a more elaborate overview: Sharma 2020, p. 166-169;
[1561] 2010/87/EU: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) *OJ* L 39, 12.2.2010, p. 5–18.

of personal data, it must be ensured that data subjects are afforded "a level of protection essentially equivalent to that guaranteed within the EU, read in the light of the Charter of Fundamental Rights of the European Union".[1562] This requires an assessment to be carried out before (intended) transfer of personal data to a third country, in order to evaluate the "relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in article 45(2)",[1563] whereas they are "required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned".[1564] Should the outcome of the assessment be that data subject's rights are *not* adequately protected, supplementary measures must be taken in order to ascertain appropriate safeguards for the protection of the rights of data subjects.[1565]

> According to the EDPB,[1566] such measures could for instance include the following (I list here the measures that can be applied to the most likely data-export practices for AV-users and -producers). When a data importer does not need to access the respective data, but rather offers a "hosting" or a "backup" service, strong encryption of personal data through state-of-the-art techniques before exporting them *without* sharing the decryption keys with the importer can be opportune. The transfer of pseudonymised data in a way that the data subjects cannot be specified, singled out or cross-referenced, *without* sharing the de-pseudonymisation keys with the importer, can be useful when the importer needs access to aggregated/pseudonymised personal data. When data are merely transited through a third country which does not offer appropriate safeguards, the data exporter can deploy state-of-the-art transport and/or end-to-end encryption techniques before such transit takes place, allowing for decryption in a jurisdiction that *does* ensure adequate protection.
>
> The EDPB also lists measures that it considers *ineffective* in data-export situations. At the moment, the EDPB is for instance "incapable of envisioning an effective technical measure",[1567] to ensure adequate protection of privacy rights of EU citizens in situations where personal data are exported to a cloud service provider based in a third country, who has or needs access to the processed data, whereas at the same time the public authorities of that country can have

[1562] CJEU *Schrems II*, para. 134; ruling no. 2. See also EDPB 2020(b) for the DPA's interpretation of the obligations under *Schrems II* for data exporters.
[1563] Ibidem, ruling no 2.
[1564] Ibidem, para. 142.
[1565] CJEU *Schrems II* para. 132.
[1566] See EDPB 2020(b), p. 22-27. These technical and operational extra measures, must be anchored through (additional) contractual provisions where necessary, see EDPB 2020(b), p. 28-34, as well as extra organisational measures (p. 35-37).
[1567] EDPB 2020(b), p. 27.

access to these data "beyond what is necessary and proportionate in a democratic society".[1568] The same holds true for a business entity based in a third country (where public authorities can get "too much" access to personal data), who can access an information system that is controlled by a EU-based business entity, which is located within a Member State.

Taking notice of *Schrems II*, it must be concluded that it is at the moment *impossible* to bring US-based (hosting/cloud) services in compliance with the GDPR-principles, where the US-based "importer" would be able to access, and/or to process personal data of EU citizens under either his own responsibility, or under responsibility of a EU-based controller.

Should also supplementary measures not result in appropriate safeguards, transfer of personal data may not take place. When a controller (or processor) would still want to export personal data even though supplementary measures could not provide appropriate safeguards, the competent DPA must be notified.[1569]

DPAs are to suspend or prohibit export of personal data when they hold the opinion that the applicable model clauses cannot be complied with, and that the personal data cannot be adequately protected by other means.[1570]

Thus, from the *Schrems II*-decision, it has become clear that EU model clauses cannot "simply" be used to create a legal bases for international data transfers. An assessment of the 'appropriate safeguards' will have to be carried out by the controller who intends to send personal data of EU citizens to places outside of the European Economic Area, and appropriate measures need to be taken where necessary – and where possible. This will de facto make it illigitimate to share data with US-based organisations, as it also follows from *Schrems II* that adequate personal data protection cannot be guaranteed by those organisations vested under the auspices of US security agencies.[1571]

5.2.9.3 Binding Corporate Rules

Binding Corporate Rules (hereinafter: "BCRs") can also be used as a basis for transfer of personal data to third countries. BCRs are regulated in article 47 GDPR. Typically, BCRs see to the intra-company transfer of personal data where entities of a company are located in different (EU and Non-EU) countries. BCRs must be legally binding to all members of the "concerned group of undertakings, or group of enterprises engaged in a joint economic activities, including their

[1568] Ibidem, p. 26. The EDPB refers here to EDPB2020(c), which lists the "European Essential Guarantees" as a referential standard for assessing whether or not third country surveillance measures can be considered in line with the protection of the fundamental rights of EU citizens.
[1569] Ibidem, para. 145; see also EDPB 2020(a), p. 3.
[1570] Ibidem, para. 121.
[1571] See also Kuner 2020; Christakis 2020.

employees".[1572] Furthermore, BCRs should "expressly confer enforceable rights on data subjects with regard to the processing of their personal data";[1573] and must fulfil an impressive list of requirements, summed up in article 47(2) GDPR.[1574] Differently from data transfers based on EC model clauses, BCRs have to be approved by a potential multitude of DPAs (of all countries in which entities of the multinational group are represented), in line with the 'consistency mechanism' of article 63 ff. GDPR. This entails that, once approved by the competent, local DPA(s), also the EDPB has to issue its opinion. This could implicate a lengthy procedure, whereas also the implications of the *Schrems II*-decision likely have to be taken into account.[1575]

> The implications of the *Schrems II*-decision are potentially far-reaching for controllers and processors whose business models rely on transatlantic data processing. AV-related business models do rely heavily on data processing, as is illustrated above. Where this data processing also possibly occurs outside the EEA, which is very likely as most 'scalable' data storage and -processing solutions are cloud-based, involving the exchange of data between data centres throughout the world, special attention must be paid to data processing in the US. Many of the organisations that provide scalable (cloud based) data processing services, have an origin – or at least entities – in the US. Where data processing with processors in the US used to be based on the Privacy Shield framework, this is prohibited as of 16 July 2020. A new ground for the transfer should be sought. As BCRs cost much time to draft and have approved by the competent DPAs and the EDPB, and these to enable data transmission within the entities of a multinational company, these may not be the most suitable alternative. For data processing between controllers in the EU, and processors in third countries (where these are not part of the same company), the most likely alternative ground could be formed by the EC model clauses. However, it also follows from the *Schrems II* decision that it must be duly ascertained by the data exporter and the recipient that the level of protection of the personal data is adequate, taking account of the possibilities of public authorities in the country where the recipient is vested, to access the processed personal data. In cases where the adequate level of protection cannot be ascertained by the exporter and recipient of personal data, supplementary measures must be taken to ensure appropriate safeguards for the data subjects regarding the protection of their rights. Should that also be impossible, the conclusion

[1572] Article 47(1)(a) GDPR.
[1573] Ibidem, sub b.
[1574] This list contains *inter alia* provisions on information duties for the multinational company towards (among others) data subjects (subs a-c; g); it regulates that the general data protection principles should apply (d); that data subject's rights apply and can be enforced (e); tasks for a DPO (h); compliance mechanisms for all individual group members (j); complaint procedures (i); mechanisms for cooperating with DPAs (m); and appropriate data protection training for certain personnel.
[1575] See Kuner 2020, "conclusions"; Christakis 2020, point 7; EDPB 2020a.

must be that the exchange of personal data is in principle not in conformity with the GDPR.[1576] Regarding the opinion of the CJEU that in the current situation, the possibilities for US security organisations to access personal data of EU-citizens are too unspecified and *de facto* unlimited, and that data subjects can hardly enforce their rights against such organisations, it is at the moment impossible to bring the exchange of personal data of EU citizens between an exporter based in a Member State, and an importer based in the US in compliance with the GDPR, in cases where the US-based importer can access and/or otherwise further process the respective data.

When nonetheless personal data would be exchanged between the EU and the US, the competent DPA is to enforce the GDPR as interpreted in *Schrems II*, i.e. they can *inter alia* suspend or prohibit such processing activities.

5.2.10 PUBLIC ENFORCEMENT: SUPERVISORY AUTHORITIES

Supervisory authorities, the DPAs, have to supervise and enforce that controllers and processors account for their actions (or negligence), i.e. compliance with the GDPR.[1577] In this section, the focus will be on the monitoring enforcement duties of DPAs, as regulated *inter alia* in article 57(1)(a, h, i, and u); 58; 83 and 84 GDPR.[1578]

As follows from article 57, DPAs are obliged to "monitor and enforce the application" (a) of the GDPR; to "conduct investigations on the application" (h) of the GDPR after a request of a colleague DPA or another public authority; to "monitor relevant developments" (i) in information and communication technologies and commercial practices; and to "keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2)" (u).

Article 58(1) GDPR equips DPAs with investigative powers. A DPA may order from controllers and processors – or when appointed: their DPO – "any information it requires for the performance of its tasks" (a). DPAs may also "carry out investigations in the form of data protection audits" (b) on the premises of the controllers or processors, regarding compliance with GDPR norms, or to review "certifications issued pursuant to Article 42(7)" (c). When investigating, DPAs may obtain access to "all personal data and to all information necessary for the performance of their tasks" (d). This implicates that controllers and processors have to co-operate with DPAs when they carry out their investigative duties, and to provide them with any information they require, not limited to personal data only, as long as that information relates to data processing activities of the

[1576] It is not likely that the 'special grounds' of article 49 GDPR can legitimately underpin large-scale data-exchange with the US.
[1577] Article 52 GDPR; see Michalowicz & Lubasz 2019, p. 275-276; Sharma 2020, p. 243; Kranenborg & Verhey 2018, p. 277-281.
[1578] See furthermore generally section 5.1.4.4, on the other tasks of DPAs.

respective organisation.[1579] Controllers of processors have to open the door for DPAs, as they may "obtain access to any premises of the controller and the processor, including to data processing equipment and means, in accordance with Union or Member State procedural law" (f).

Besides investigative powers, DPAs also have corrective powers, regulated in article 58(2) GDPR. They may issue warnings that (intended) processing activities (likely) violate the GDPR (a, b). Furthermore, they can order the controller or processor to "comply with the data subject's requests to exercise […] rights under this Regulation" (c); to "bring processing operations in compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period" (d); that a personal data breach is communicated with the data subjects (e); rectification, erasure of certain personal data or restriction of (further) processing of personal data (g); or to suspend data flows to third countries (j). When warnings, reprimands or orders are not sufficient, a DPA has further corrective powers, as it may: (temporary or indefinite) limit or ban certain processing activities (f); withdraw a certificate (h); or "impose an administrative fine pursuant to Article 83, in addition to, or instead of measure referred to in this paragraph, depending on the circumstances of each individual case" (i). It thus follows from these provisions, that DPAs have a large arsenal of corrective powers, of which the possibility to (threat to) sanction a controller or processor may be of most significant importance.[1580]

Article 83 elaborates the possibilities for DPAs to impose hefty fines to non-complying controllers or processors. Fines must be, according to the first paragraph: "effective, proportionate and dissuasive". The second paragraph lists circumstances to be taken into account when the DPA is to determine the amount of a fine, which *inter alia* include the nature, gravity and duration of the infringement, and the impact for data subjects (a), as well as the involved data categories (g); intent or negligence underlying the infringement (b); damage mitigating or aggravating actions taken by the controller or processor; previous behaviour of the respective controller or processor (e; i; k) and the (active) cooperating (or non-cooperating) behaviour with the DPA (f; h). Two categories of fines are distinguished.

The first category (paragraph 4) includes infringements which can result in an administrative fine of € 10 million, or 2% of the annual worldwide turnover in the preceding financial year – whichever is higher – of the infringing undertaking. Fines within this first, *standard category* can be imposed on controllers or processors, infringing their obligations pursuant to articles 8 (child's consent); 11 (processing which does not require identification); 25-39 (*inter alia* obligations

[1579] See Sharma 2020, p. 248-249.
[1580] It must be noted that other sanctions can also be regulated: Article 84 GDPR holds an obligation for Member States to "lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines.

regarding data protection by design and -default; data processing agreements; records of processing activities; cooperating with the DPA; TOMs; data breach notifications; DPIAs and prior consultation of the DPA; and DPOs); and 42-43 (certification mechanisms).[1581]

Article 83(5) holds *high category* infringements, which can result in fines up to € 20 million, or 4% of the annual worldwide turnover in the preceding financial year (whichever is higher). Within this category, infringements are listed regarding: the basic principles for processing and consent (articles 5-7 and 9); the data subject's rights (articles 12-22); international transfer or personal data (articles 44-49); obligations pursuant to Member State law (under Chapter IX); non-compliance with an order of a DPA to limit or suspend data processing activities, or with failure to comply with the obligation to provide a DPA access pursuant to article 58(1). Also non-compliance with orders of a DPA pursuant to article 58(2) can result in such fine.[1582] This explicates that a DPA is in principle free to implement policy to warn and impose 'lighter' sanctions first, and when that does not deliver the required results, to eventually impose administrative fines.[1583]

Thus, local DPAs have the obligation to monitor and ascertain GDPR compliance, which can eventually be enforced with high administrative sanctions. They have (within the bandwidths provided by the GDPR) some freedom in defining the height of the sanctions, and different policies seem to be in place throughout the EU.[1584] The Article 29 Working Party provided a bit more guidance in this respect, in order to achieve equivalent personal data protection in the Member States, i.e. "equivalent sanctions" that are "effective, proportionate and dissuasive".[1585] Although the nature of the sanctions is further explicated by the Working Party, its guidance does not provide recommendations on the height of administrative penalties. The Dutch AP was the first supervisory authority to formulate policy on the height of GDPR-sanctions.[1586]

Until further guidance is provided by the EDPB, the AP is to apply its own penalties-policy. The AP regulated 4 sub-categories (applicable to both *standard*- and *high category* infringements), with bandwidths varying from € 0 – 20.000 (category I, with a "base fine" of € 100.000,-), to € 450.000 – 1.000.000 (category IV, with a "base fine" of € 725.000,-).[1587] The €10.000.000,- or € 20.000.000,- maxima addressed by the GDPR are not 'reached' in these categories, although the

[1581] Fines in this category can also be imposed to certification bodies, when non-complying with art. 42-43 GDPR; or monitoring bodies, regarding compliance with 41(1) GDPR.
[1582] Paragraph 6.
[1583] See Kranenborg & Verhey 2018, p. 289.
[1584] See for an overview of the different DPA sanctions in the Member States: https://www.enforcementtracker.com/# (Enforcementtracker.com).
[1585] See WP(29) 253, p. 5.
[1586] AP 2019a.
[1587] Article 2.3 AP 2019a.

AP states that there can be factors resulting in higher (or lower) fines than those defined in the categories.[1588] Furthermore, the AP states that recidivism can be punished with 50% higher fines,[1589] and the GDPR-maxima can also be applied as the AP sees fit.[1590]

The 'landscape' of fines imposed by DPAs is diverse.[1591] The CNIL has varied for example between a € 20.000,- fine for infringing article 5(1)(c), 12, 13 and 32 GDPR;[1592] and € 50 million fine to Google LLC, for infringement of *inter alia* basic principles enshrined in articles 5 and 6, and information duties of article 13 and 14 GDPR.[1593] The ICO issued fines between € 320.000,- to Doorstep Dispensaree, for infringing article 32 GDPR,[1594] and (an intended) € 204.6 million ,- to British Airways, for infringing article 32 GDPR.[1595] The AP issued fines between € 460.000 to Haga Ziekenhuis for infringing article 32 GDPR,[1596] and € 900.000,- to UWV for infringing the same article 32 GDPR.[1597] The foregoing is just one illustration of what different enforcement policies can result in, as there are significant variations in fining-bandwidths for violations of the GDPR..

Besides enforcing the GDPR on the own initiative of DPAs (under their monitoring and enforcement duties pursuant to article 57 and 58 GDPR) also initiatives of data subjects can

---

[1588] Articles 6-8 AP 2019a.
[1589] Article 8.2 AP 2019a.
[1590] Articles 8.3-8.4 AP 2019a.
[1591] See for instance Enforcementtracker.com.
[1592] Délibération de la formation restreinte n° SAN-2019-006 du 13 juin 2019 prononçant une sanction à l'encontre de la société X, via https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038629823&fastReqId=946473298&fastPos=1 (last accessed 27 Juy 2020), which concerned a *high category* infringement regarding the data minimisation principle and *standard category* infringements regarding transparency and information duties, as well as insufficient TOMs.
[1593] Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC, via https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (last accessed 27 July 2020), concerning *high category* infringements, regarding *inter alia* the lack of information and legal basis (consent e.g.) for the creation of a google.com account when configuring a mobile phone
[1594] Data Protection Act 2018 (part 6, section 149) enforcement powers of the information commissioner enforcement notice 17 December 2019, via https://ico.org.uk/media/action-weve-taken/enforcement-notices/2616741/doorstop-en-20191217.pdf (last accessed 27 July 2020), concerning a *standard category* infringement regarding insufficient TOMS for not properly securing (paper) records containing *inter alia* patient- and prescription data.
[1595] This intention to fine can be found at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (last accessed 27 July 2020), concerning a *standard category* infringement regarding insufficient TOMs leading to a large-scale cyber incidents where clients were diverted to fraudulent website, allowing the harvesting of approximately 500.000 data subjects.
[1596] AP Boetebesluit HagaZiekenhuis 16 juli 2019, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf (last accessed 27 July 2020), concerning a *standard category* infringement regarding insufficient TOMs for not properly sealing off patient data for hospital personnel.
[1597] AP Last onder dwangsombesluit 1 November 2018, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/last_onder_dwangsom_uwv_werkgeversportaal.pdf (last accessed 27 July 2020), concerning a *standard category* infringement regarding not using two factor authentication where that would have been appropriate.

trigger public enforcement activities.[1598] It follows from article 77 GDPR that data subjects have the right to file a complaint with a DPA "in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement", regarding the (alleged) infringement of GDPR provisions. Article 77 creates a one-stop-shop for data subjects to complain against a controller or processor who may not abide by the GDPR rules.[1599] That DPA has to inform the complaining data subject regarding the progress and outcome of the complaint, and that de data subject has the right to seek judicial remedy from the DPA ex article 78 GDPR. The DPA has to process every complaint, as it follows from article 78(2) that a data subject

> "shall have the right to an effective judicial remedy where the supervisory authority […] does not handle a complaint or does not inform the data subject within three months on the progress or the outcome of the complaint lodged pursuant to Article 78".

The outcome of a complaint procedure, must be seen as a legally binding decision of the DPA.[1600] That decision can in turn be subject to "effective judicial remedy", which may be sought not only by the complaining data subject, but rather by anyone – including the respective controller or processor – who is concerned by the decision.[1601]

It must be noted that the right to seek effective judicial remedy regards *all* DPA decisions, including decisions concerning (intended) enforcement measures.

5.2.11 PRIVATE ENFORCEMENT: ACCOUNTABILITY AND LIABILITY

As introduced in the foregoing section, there are ample means for data subjects to have their rights enforced by a DPA, besides the DPA's own monitoring and enforcement tasks. There are however more ways in which the accountability principle for controllers and processors is embodied in the GDPR. Data subjects – and in some cases, other actors – are enabled to enforce their rights against controllers and processors through civil procedures by the GDPR. Besides data subjects, also a "not-for profit body, organisation or association" with a public interest objective, and which is active in the field of data-protection may file a collective action to claim damages as a result of GDPR-infringements.[1602] Such collective actions may be instituted by groups of people who individually suffered damage, but for whom it would not be cost-efficient to start judicial proceedings. Recently, collective actions were for instance started by the Dutch Consumers Association (Consumentenbond) and the Take Back Your Privacy Foundation against social media platform provider TikTok, who claimed the remuneration of €2 billion for the unlawful collection

[1598] See Gawronski 2019, p. 285; Kranenborg & Verhey 2018, p. 303.
[1599] Kranenborg & Verhey 2018, p. 305-306; also recital 141 GDPR.
[1600] Kranenborg & Verhey 2018, p. 307.
[1601] Ibidem, p. 306-307.
[1602] Article 80 GDPR.

and commercialization of personal data of children who participated in the social network.[1603] In the following sections, I will further illustrate the material conditions for civil liability under the GDPR.

5.2.11.1 Effective judicial remedy

Article 79(1) GDPR regulates that data subjects "shall have the right to an effective judicial remedy where he or she considers that his rights [...] have been infringed as a result of the processing of his or her personal data in non-compliance with this regulation". The second paragraph explicates that proceedings against a controller, or a processor, must be brought before the court where the controller or processor is established, or, at the sole choice of the data subject, before the courts of the data subject's residence – unless the controller or processor is a public authority of a Member State, acting in the exercise of its public powers.[1604]

Data subjects could 'simply' require a court order directed at the controller or processor to comply with the GDPR-provisions, but could moreover demand compensation for damages resulting from non-compliance, which is addressed in article 82 GDPR.

5.2.11.2 Civil liability (article 82 GDPR)

With the enactment of article 82 GDPR, the European legislator effectively added unionwide, uniform, civil liability rules to its palette. These rules are to be applied by the courts in the Member States in the same way. CJEU case law, which is to further explicate the texts of the GDPR, is absent to date.[1605] Further guidance for instance in the form of recommendations from the EDPB or its predecessor has not been provided either. This leaves us with the situation that unification of extra-contractual GDPR-liability has only partially occurred, as concepts regarding allocation of liability and, to a certain extent, causation are addressed in article 82, but concepts such as damages to be remunerated and apportionment are not (fully) regulated yet. This implicates

---

[1603] See Molijn, C., "TikTok voor de rechter gesleept om schending privacy, massaclaim van 2 miljard", *NRC*, 31 Autust 2021, online via https://www.nrc.nl/nieuws/2021/08/31/tiktok-voor-de-rechter-gesleept-om-schending-privacy-massaclaim-van-2-miljard-a4056682 (last accessed 16 September 2021).

[1604] In the latter case, courts of the place where the public body is vested have jurisdiction. See Gawronski 2019, p. 28. Sharma (2020, p. 253) argues furthermore that the court is competent in the Member State where the infringement has taken place (although that does not directly follow from article 79).
In this respect, also article 81 GDPR must be noted, which regulates *inter alia* that when a competent court in Member State A has information on the same subject matter, regarding the same controller or processor, on the same processing activities, as pending before the court of Member State B, it has to contact the court in Member State B "to confirm the existence of such proceedings" (1). Paragraph 2 stipulates that when proceedings regarding the same subject matter regarding processing activities by the same controller or processor, are brought before courts in different Member States, "any competent court other than the court first seized may suspend its proceedings", or may (3) "decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof".

[1605] Such guidance may follow *inter alia* from a CJEU decision in the case (C-300/21, *UI/Österreichische Post AG*), regarding among other things the question whether or not it is required that a victim of a GDPR norm breach has actually suffered harm, or that the sole norm-infringement is sufficient to award compensation of damages.

uncertainty for victims and tortfeasors, especially regarding the topics that have not been addressed by the EU legislator. This also implicates that Member State law shall 'fill in the blanks', which may lead to different outcomes between them regarding inter alia the question which damages are to be remunerated, and how these need to be apportioned.[1606]

5.2.11.3 Allocation of liability

In article 82 GDPR, it is regulated that

> "any person [not limited to data subjects, *RWdB*] who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered".[1607]

The second paragraph of article 82 channels liability to "any controller involved in processing" (to a large extent), and regulates that besides controllers, also processors are liable

> "for the damage caused by processing **only** (emphasis added, *RWdB*) where it has not complied with obligations of this Regulation specifically addressed to processors or where it has acted outside or contrary to lawful instructions of the controller".

For the establishment of liability under article 82, three components must be taken into account. First, an *infringement* of a GDPR norm must be proven. Second, *damage* needs to be established, and third a *causal relationship* between the infringement and the damage must be ascertained.

Infringement

Although sometimes otherwise suggested,[1608] the onus to prove a GDPR-infringement rests on the victim. [1609] The accountability principle, enshrined *inter alia* in article 5(2), holding that a controller must at all times be able to demonstrate GDPR-compliance, read together with article 82(3) GDPR can aid the victim in this respect. Article 82(3) states that "a controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage". This entails a presumption of fault at the side of the controller or processor,[1610] and results therein that a victim must make a motivated statement that a GDPR infringement was made. Such a statement can, in theory, easily be underpinned on the basis of information regarding compliance which needs to be actively provided by a controller.

[1606] See also Chamberlain & Reichel 2019, p. 8.
[1607] Article 82(1) GDPR.
[1608] See Truli 2018, p. 26-27; and Gawronski 2019, p. 288-289.
[1609] See also Van Alsenoy 2016, p. 282-283.
[1610] Ibidem.

> Mike is a frequent AV user. He often rents a car from company X, based in The Netherlands. X has outsourced the data storage to company Y, vested in San Francisco. On a bad day, a data breach occurred, resulting in the public accessibility of all personal data processed on Y's servers. This included Mike's payment data and credit card details. The data breach was reported to the Dutch DPA, as well as to Mike. Mike found out, a month later, that his credit card details had been abused, and that large sums were withdrawn from his account. Mike can seek compensation from X, or Y. He needs to establish that the data breach resulted from non-compliance with the norms of the Regulation. He presumes that somewhere in the chain of data processing activities, insufficient Technical and Organizational Measures (TOMs) had been implemented, which he derives from the fact that (at least) both his name *and* his credit card details were stored (and leaked) together, instead of separate, where these data had not adequately been encrypted. Should adequate TOMs have been implemented (such as encrypted storage of names and card details in separate places), it would have been unlikely that the respective bank withdrawals took place. A court could follow Mike in his presumption, and thus assuming 'fault' of the controller (or processor) for implementing insufficient TOMs, contrary to article 32 GDPR. It is then for that controller (or processor) to prove that he was not *in any way* responsible. Should he not succeed, the respective fault will be established.

Damage

It follows from recital 146 that the concept of damage must be "broadly interpreted in the light of the case-law of the Court of Justice which fully reflects the objectives of this Regulation", although without prejudice to Union or Member State law. Data subjects are to receive full and effective compensation for damage they suffered as a result of infringement of GDPR-rules, or delegated and implementing acts. Both material and non-material damage are within scope of remuneration obligations, as follows from article 82(1), in full. Recital 75 GDPR states certain harms that can be the result of (illegitimate) data processing: "

> […] discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage[…]".

Recital 85 GDPR lists examples of damage that can be caused by personal data breaches:

> "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of

confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned".[1611]

Member States will, until further CJEU-guidance is provided,[1612] apply their 'own' rules in this respect, in the spirit of the (recitals to) the GDPR. As shown in sections 4.2 and 4.3, there are certain variations regarding these topics between the Member States.[1613] It would seem for instance that in France and the Netherlands it will be easier to get remuneration for pure economic loss than in England. Furthermore, under French liability rules, it will be easier for "indirect victims" (*victimes par ricochet*) to be awarded remuneration than under the Dutch or the English systems.[1614]

[1611] See in this respect also Walree 2017, p. 922 ff., who highlights that besides material damage (as bank accounts may be plundered after credentials of account holders were leaked), identity fraud is a serious risk, which may *inter alia* lead to "bureaucratic" issues, as a data subject might have to prove time after time that his identity was illegitimately used in order to falsely attribute certain offences and violations to him.

[1612] See also Walree 2021, p. 27-31, who holds that the "damage" concept should be taken as harmonised by the GDPR, and that further guidance is necessary and can be expected. Further guidance can also be expected in the CJEU C-300/21-case, as referred to above in footnote 1604.

[1613] See also Chamberlain & Reichel 2018, p. 8-9.

[1614] It must be noted that in England for example, there is besides "libel" or "slander" no specific tort in place on which a claim for immaterial damages as a result of privacy rights can be based (see Giesen 2000, p. 275). It is thus questionable on which grounds a claim for immaterial damages must be based. However, as follows from the decision of the Court of Appeal in *Lloyd/Google* [2019] EWCA Civ 1599 (2 October 2019), no. 88., which was decided under the withdrawn implementation of the DPD, it is held that "claimants can recover damages for loss of control of their [personal, *RWdB*] data […] without proving pecuniary loss or distress". In The Netherlands, remuneration of immaterial damages as a result of infringement of a fundamental right is possible, on the basis of article 6:106(1)(b) BW which addresses "impairment in the person" (aantasting in de persoon). However, a single violation of a fundamental right does in principle not suffice, it needs for example furthermore be proven that the violation led to mental injury. When mental injury cannot be proven, it must be established that the seriousness of the norm-violation and the seriousness of the consequences, justify remuneration of immaterial damages. This follows from Hoge Raad 15 March 2019, ECLI:NL:HR:2019:376 (*EBI*). This was further elaborated in case law of the Hoge Raad 15 October 2019 (ECLI:NL:HR:2019:1465, see furthermore section 4.2.3.3). It held that remuneration of *other harm in person* in privacy-violations is not self-evident, and a compensation claim must be substantiated with evidence, unless the norm violation was of such a severity or nature that it is obvious that *other harm in person* can be presumed. Thus, when an action is based on an infringement of the GDPR, the bar could sometimes be lowered, which is also illustrated in R. Rijnhout, "Het EBI-arrest, historisch onrecht, effectieve remedie en de AVG", *Tijdschrift voor Personenschade* 2020, no. 1., p. 1-6. In France, single violation of a fundamental right is sufficient to be awarded immaterial damages under article 9 CC (see Giesen 2000, p. 296-297). See also Hartlief, T., "(Smarten)geld zetten op de AVG", *NJB* 2021/2885, no. 39, 9 November 2021, who advocates to base civil liability claims directly on article 82 GDPR, rather than on article 6:106 BW.

There are several examples of national case law in procedures involving liability ex article 82 GDPR.[1615] The judiciary of the Netherlands is the only of the systems under review in this research that has decided on this subject matter.[1616]

The Rechtbank (district court) Overijssel decided that due to a "loss of control over his personal data" the claimant's privacy was infringed, and that his personal data were processed without a lawful ground.[1617] This justifies the award of "immaterial damages", which needs to be determined on the basis of the fairness ("billijkheid") principle. In this case, remuneration of € 500,- was considered fair. In another case, the Rechtbank Amsterdam decided that UWV, the social benefits agency of The Netherlands, had to remunerate € 250,- immaterial damages to an employee, for illegitimately sharing special category data (concerning the health of the data subject) with the new employer of that data subject.[1618] The fact that the respective data were shared automatically, thus without human intervention, was considered as an infringement of article 32 GDPR (regarding TOMs), causing immaterial damage (i.e. "harm otherwise in person" ex article 6:106(1)(b) BW) to the data subject. The court considered that the facts of the case resulted in a permanent loss of control over personal data, whereas however the only recipients of the respective data were the (employees of the) new employer, while this loss of control did not negatively impact the economic or societal position of the data subject, and that the duration of the "anxiety and stress" as a result of the loss of control, was limited.[1619] The Rechtbank Noord Nederland decided that the illegitimate disclosure of personal data formed an infringement of article 5(1)(f) and 32 GDPR.[1620] That disclosure resulted in the permanent loss of control over those data by the data subject, which amounted to immaterial damage at the side of the data subject, as the data subject sustained reputational harm. Again based on the fairness principle, the controller was convicted to remunerate € 250,- for immaterial damages. The court considered thereto that the disclosure indeed infringed the fundamental rights of the data subject, but that the negative effects were limited, in the sense that the respective data were disclosed to only two people, and that no other negative implications for the data subject were proved.[1621] The Rechtbank Noord-Holland considered that showing a portrait of a midwife including her name badge and profession on big screens in the terminals of Schiphol Airport and through several

[1615] See for an overview (as of 28 July 2020) regarding non-material damages: http://www.cearta.ie/2020/03/compensation-for-non-material-damage-pursuant-to-article-82-gdpr/.
[1616] See also Samsom, M.C., "Handhaving van het recht op bescherming van persoonsgegevens via het aansprakelijkheidsrecht", *NTBR* 2021/2, p. 4-16 for *inter alia* a recent overview of Dutch case law in relation to article 82 GDPR.
[1617] Rechtbank Overijssel 28 May 2019 (administrative chamber), ECLI:NL:RBOVE:2019:1827, para. 9.
[1618] Rechtbank Amsterdam 2 September 2019, ECLI:NL:RBAMS:2019:6490.
[1619] Ibidem, para. 18.
[1620] Rechtbank Noord Nederland 15 January 2020, ECLI:NL:RBNNE:2020:247.
[1621] Ibidem, para. 4.107.

social media channels constituted both an infringement of her portrait rights (incorporated under article 21 of the Dutch Copyright Act (Auteurswet) and of article 6(1)(b) GDPR.[1622] Furthermore, the court observed that Schiphol disobeyed its information duties under article 14, and that a personal data breach occurred – be it that Schiphol did not act contrary to articles 33 respectively 34 GDPR. The court decided that the privacy interests and commercial interests of the claimant were violated, and convicted Schiphol to remunerate damages to an extent of €1.500,-. By the highest administrative chamber of the Dutch judiciary, civil damages amounting to € 500,- have been awarded in 2020. In that case, medical (thus special category) data had been processed without the necessary "informed consent" of the data subject.[1623]

> Mike must establish that he has suffered damages. Damages exist *inter alia* in the illegitimate withdrawals. As it seems, it would be (under the regimes of The Netherlands, France and (although less certain) England, sufficient to prove that an infringement of his privacy rights had taken place in order to assume that Mike has suffered "immaterial damages" as well, although it is not certain how such damages must be quantified. When looking at the Dutch case law, the amounts of immaterial damages can observed to be rather modest.

Causation

Besides norm-violation and damage, victims have to prove a causal nexus between the violation and the damage suffered for a successful liability claim on the basis of article 82 GDPR. The GDPR does not harmonise the "material" requirements for causation, thus also here national law applies – until further guidance is provided by the CJEU. As illustrated in Chapter 4, often a "condicio sine qua non"-relationship must (at least in the countries under review in this study) be proven to establish "factual causation", which can be based on a "but-for" test: would the damage have not occurred without the respective event, a causal nexus can be established. Furthermore, under the national regimes, judges tend to aid victims in situations where proof of causation is difficult by for instance rebuttable presumptions. Presumptions regarding causation would be in line with the presumption of fault, that has been incorporated under article 82(3) GDPR, discussed above.[1624]

> It might be relatively easy for Mike to prove that the withdrawals would not have been made without the norm violation, as long as he can show that *he* did not authorise the respective withdrawals. In cases where proving a causal relationship between a GDPR-infringement and

[1622] Rechtbank Noord-Holland 28 October 2020, ECLI:NL:RBNHO:8537.
[1623] Afdeling Bestuursrechtsrpaak Raad van State 1 april 2020, ECLI:NL:RVS:2020:898.
[1624] Van Alsenoy argues that also presumptions regarding causation would be admissible, see for instance p. 275.:

certain damage is difficult, judges could aid victims by making rebuttable assumptions regarding causation.

5.2.11.4 Joint and several liability

Paragraph 4 regulates a one stop shop for *data subjects* (rather than for other parties who suffered damage): where more than one controller and/or processor are involved who are responsible for any damage, any of those controllers and/or processors shall be (jointly and severally)[1625] held liable for the entire damage "in order to ensure effective compensation of the data subject". Thus, any of the actors involved in the chain that (may have) contributed to the origination of the damage, can be sought for full compensation. However, the respective controller or processor can seek redress from "the other controllers or processors involved in the same processing", relating to "that part of compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2".[1626]

> Mike may chose whom to sue – as long as he can prove that that actor was responsible for his damage, or, in fact, that that actor was involved in the damage-inflicting activity (see the previous section). Should for instance the controller (X) be established in San Francisco, and the processor (Y), in Amsterdam, it will be less troublesome for Mike to sue Y, rather than X. When Y's involvement is established, his fault can be presumed on the basis of article 82(3) – unless Y can prove that he was not responsible at all. When Y cannot prove that, Y will be held to remunerate the full amount of Mike's damages. Y can later seek recourse from X, corresponding with the part of the respective responsibility of X.

[1625] See Gawronski 2019, p. 289.
[1626] Article 82(5) GDPR.

5.3 CONCLUSION

In this Chapter, the unified European regulatory framework on personal data protection that applies to processing activities of personal data concerning EU citizens through AVs has been reviewed. This was relevant, as many personal data will be processed through the deployment of AVs. Personal data processing is necessary for enabling AVs to operate, and AV-related services to be deployed. Moreover, current European civil liability rules (see Chapter 4) necessitate personal data processing by both victims of AV accidents to underpin their claims, and by those held liable, for defence purposes.

In the review above, I have focussed on the rules of the GDPR, the (corresponding) policy of the national DPAs and of the EDPB, applicable case law of the Member States and eventually the CJEU. The reviewed regulatory framework regards the protection of *informational privacy*, which is in turn part of the larger framework on *privacy* protection. While the notion of *privacy* appeared hard to define in literature, I found Blok's view useful, who sees privacy as a subjective right (in rem), that sees to the protection of the private sphere of citizens, which is of a personal nature, and which equips the right holder with a right of *non-interference* by others. Different from the broader *privacy*-notion, *informational privacy* as embodied in the GDPR is *not* a right of non-interference, but rather provides (strict) conditions under which such interference, i.e. personal data processing by others, may take place. As illustrated by Solove, *informational privacy* is to prevent harm when the *personal sphere* is not adequately protected. Such problems may *inter alia* relate to unlimited collection, uncontrolled processing and unrestrained dissemination of personal data, and cause financial, psychological and even physical harms.

Among many other things, the GDPR explicitly sees to the prevention of problems and harms such as those indicated by Solove, and in broader perspective, to protect the fundamental rights and freedoms of natural persons – while not preventing the free flow of personal data between the Member States. Also, the GDPR sees to facilitate technological developments, rather than to hinder such developments. Strong protection and enforcement of *informational privacy* is, *inter alia*, found to be necessary for creating citizen's *trust* in, and therefore, uptake of such new technology. This objective is in line with the *trust*-factor indicated in section 3.4.3, which encompasses that new (AV-)technology through which personal data are processed of those who use the technology, should in itself be aimed at preventing harm as much as possible. Furthermore, the *risk* of harm that may potentially occur as a result of the development or deployment of such AV-technology, should ultimately be borne by those who can control the risk (i.e. the controllers and processors of personal data), rather than the data subjects – who have little or no means to control such risk. In line with that principle, the GDPR regulates that when damage nevertheless occurs, that this damage can be easily claimed from the controllers or processors, who are thus held accountable

for the *risks* involved in data processing. Besides civil enforcement, the GDPR allows for public enforcement. When controllers (or processors) do not facilitate the exercise of rights of data subjects, or (otherwise) fail to comply with their obligations, compliance can be enforced by DPAs – who are eventually able to impose penalties up to € 20 million, or 4% of the annual worldwide turnover, and a specifically created liability regime allows data subjects to claim damage compensation caused by non-compliance.

The enforcement rules of the GDPR are rather clear, as are their objectives. Nonetheless, the underlying rules, which *inter alia* aim for technology-neutrality and flexibility, and the corresponding obligations for data controllers and processors, are not. As observed in this Chapter, the many rules are often complex, provide uncertainty for controllers and processors, and are overall not easy to comply with for AV-developers and deployers. Often, the obligations are complex. For example, every intended processing activity must be based on a lawful ground. Regarding personal data processing activities through AVs, the EDPB and DPA's advocate that "consent" of data subjects should be used as the applicable lawful ground. However, such consent is not easy to 'legally' achieve. Furthermore, it is uncertain to what extent one of the most likely other lawful grounds i.e. the "legitimate interests" of the controller justifies data processing for commercial activities. At the same time, some forms of new technology, including blockchain technology (which would in principle be very usable to store AV-data in ways that ensure integrity of such data, as it is very hard to alter these once stored) would likely be intrinsically non-compliant with the GDPR, as data subject's rights of completion, rectification and erasure of personal data can hardly be exercised given the nature of that technology. Furthermore, it is not always clear when the principles of *data protection by design* and -*by default* are satisfied in conformity with the GDPR, as the rules are vague. EDPB-policy suggests that the creation of "more specific guidance" would be useful in this respect. The same is *inter alia* true for the obligatory technological and organisational measures to be taken by controllers and processors to ensure a level of protection that is adequate for the protection of privacy risks that are posed by respective (intended) processing activities. Although some guidance is provided by the EDPB (and local DPAs) regarding AV-specific risks, there are no "general" rules available. Comparable observations can be made regarding data protection impact assessments that need to be performed *before* processing activities take place which form a "high risk" for the privacy of natural persons. Also in these cases, measures need to be taken based on the specific risks of the intended processing activity, and in some cases the DPA must be consulted (when risks cannot be mitigated), but it is for the controller to decide which risk-assessment-method might be appropriate.

The vagueness and openness of GDPR-norms is acknowledged by the legislator, for the sake of flexibility and technology neutrality. The GDPR provides for co-regulatory tools as *certification mechanisms* and *codes of conduct* to fill in the blanks, which can be applicable for specific technologies and/or in specific sectors. Codes of conduct could, according to the GDPR, for instance provide more clarity regarding the fairness and transparency principles, sector specific TOMs; pseudonymisation (techniques), *privacy by design* and -*by default* principles, ways to inform data subjects of their rights, and of data breaches, international transfers of personal data, and alternative dispute resolution mechanisms. However, to date, *only 3* codes of conduct have been approved by the DPAs (including the EDPB), and no certification mechanisms have been adopted. To conclude this paragraph, it must be stressed that the CJEU-judgment in the *Schrems II*-case effectively prohibits the exchange of personal data between the EEA and the United States, which thus precludes the use of services by providers in the States.

Two main observations can thus be made regarding the position of the *regulatees*, i.e. controllers and processors who are to develop and deploy innovative AV-technology. First: the current openness of the norms of the GDPR leave controllers and processors in an uncertain position, as it cannot be ensured when they are 'in compliance'. Necessary guidance could be provided through for instance comprehensive policy by the supervisory authorities, approved certification mechanisms or codes of conducts. As long as such guidance is not sufficiently present, this implicates *uncertainty* for controllers and processor will persist. This could be problematic, as non-compliance by controllers or processors can "stringently" be enforced: supervisory authorities can (and do) impose high fines, notwithstanding civil liability claims which can be awarded to those who suffer damage as a result of GDPR-infringements.[1627] Second: the fact that some forms of (for example: blockchain) technology is intrinsically non-compliant with the GDPR, also indicates that innovations cannot be lawfully further developed and deployed within the European Union, as long as the GDPR criteria are not met. It is however questionable whether or not this "red-tape" would in fact prevent the application of such technology.

The observed compliance-obstacles for controllers or processors may also have consequences for EU citizens as *data subjects*. It may for example occur that controllers or processors wrongfully assume that they are acting in accordance with the open norms of the GDPR, as there will often be uncertainty regarding the question whether the requirements underlying the respective norms are satisfied or not. More extremely, it may also occur that the *regulatees* ignore the fact that they are not complying with the rules, or take the chance that they will not be subject to enforcement by the public authorities or civil actors. In both situations, the result of non-compliance is that the

[1627] See also Koops 2014, p. 7; Kranenborg & Verhey 2018, p. 10-12, 225.

informational privacy of data subjects is not adequately protected. That in turn implicates risks of harm. This may negatively impact citizens' *trust* in technology when data subjects falsely assume that their informational privacy is adequately protected.

Chapter 6. APPLICATION AND CASE STUDY

6.1 INTRODUCTION

In this Chapter, I will analyse to what extent the innovation-influencing factors as identified in section 3.4, are encompassed in the reviewed regulatory frameworks regarding product liability, traffic liability and personal data protection. The analysis will be based on the case study introduced in section 3.5. The application of the three regulatory frameworks is addressed in turn: product liability is reviewed in section 6.2, traffic liability is reviewed in section 6.3, and section 6.4 addresses personal data protection. Each review consists of two parts. First, the rules of the respective regulatory framework are applied to the case study. This is based on one central question per framework, which is formulated as follows: *To what extent would it be likely that [the innovator] is liable towards [the victims (consumers)] based on the facts and circumstances of the case, and which damages could qualify for remuneration?* The respective answers are used to assess the factors in the second part. I evaluate if and how the reviewed regulatory framework implicates *legal (un)certainty*, *stringency* and *flexibility* for innovators.[1628] Second, it is evaluated if and how the frameworks could implicate *risk* and *trust* for consumers. Third, these factors are cross-examined. [1629] This chapter concludes with section 6.5, which holds a resumé and extrapolation of the main findings.

6.2 PRODUCT LIABILITY

6.2.1 INTRODUCTION

In the following sections, first (in section 6.2.2) the question will be addressed to what extent the innovators, i.e. the producer of the AV and/or the developer of its software in its role as producer can be held to compensate the damages suffered by the victims as sketched in the case, i.e. the owner of the vehicle, its passengers, and the bicyclists. The answers are based on the analysis of the regulatory framework regarding product liability, as addressed in section 4.2.[1630] After that, the factors existing in the product liability framework which could influence innovation and acceptance of innovation in the field of AVs are analysed, from the *innovators perspective* in section 6.2.3 and the *consumers perspective* in section 6.2.4.

[1628] These factors are addressed in section 3.4.2 above.
[1629] These factors are addressed in section 3.4.3 above.
[1630] References to legislation and literature are not repeated here, occasional reference is made to 'new' sources, which had not been used in the aforementioned section.

6.2.2 *SOLVING THE CASE*

Whether or not the AV manufacturer and/or the software developer (in their role as producer) are obliged to compensate damages, and if so, to what extent, depends on a number of sub-questions. In section 6.2.2.1 it is analysed whether or not the AV/the software components qualify as a *product*; section 6.2.2.2 addresses the question whether or not *defectiveness* can be assumed; in section 6.2.2.3 it is assessed whether or not *causality* between the defective product(s) and damage is likely to be established; the possible *types of damage* to be remunerated are analysed in section 6.2.2.4; and section 6.2.2.5 addresses the possible *defences* that the producer(s) might invoke.[1631] Issues of proof are addressed within the sections regarding defences, causation and damage.

6.2.2.1 *PRODUCTS: AV AND ITS SOFTWARE*

Given that the AV depicted in the case study is a "movable", it can safely be assumed that it is a *product* in sense of article 1 PLD. Its manufacturer, and – if applicable, when for instance the AV was for instance not sold to a consumer in the EU – the entity putting the AV up for hire or leasing will qualify as *producers* in sense of article 3 PLD.

The question whether or not the producer of the software that is necessary for the AV to operate can be held liable under the PLD, is slightly harder to answer, as software is not a "movable" in itself. Given the current *communis opinio* in literature,[1632] it can be held that software which is necessary for an AV to operate – in this case its core steering software, including the APRS, especially when embedded in a tangible medium, i.e. the AV, is a product too.

Based on the observations above, in principle both the AV manufacturer and the developer of the operating software are producers in sense of the PLD, and thus liable, that is, as long as the other requirements for allocating liability are fulfilled too.

6.2.2.2 *DEFECTIVENESS*

The case study presents two distinct "strands" of possible defectiveness that need unravelling: 1) the victims of the AV-crash must prove that the crash results from defectiveness of the AV itself or one of its components, i.e. the 'hardware', including its embedded steering software; and 2) the victims of the leaked personal data will have to uphold that this results from defectiveness of one specific part of the steering software, i.e. the APRS database.

[1631] As the analysis in the following section forms the application of my analysis of the product liability framework, I will only make occasional references (other than this general reference to section 4.2). References to material not mentioned there, are of course included hereunder.

[1632] See section 4.2.2.2

AV itself

The AV was marketed as a SAE level 5 autonomous vehicle. Therefore, the vehicle does not need a human operator to drive it, or to take back control on request of the car. The public may thus reasonably expect that the vehicle is able to operate itself in a safe way. It is however not yet certain what concretely constitutes the level of safety that may be expected. Some argue that AVs must at least be as safe as when compared to an "average" human driver, while others hold that it may be expected that an AV drives as safely as technologically possible – beyond the level which an "excellent" human driver may achieve. When the AV's safety would have to be compared to an "average" human driver, it must be evaluated whether or not the average driver would have noticed three bicyclists ignoring a red traffic light in the middle of the night. Should the answer be that these bicyclists would most likely have been overlooked by the human driver, defectiveness cannot be proven. A "beyond excellent" human driver should have noticed the cyclists, and the AV which is to be compared to such a faultless driver, can be held defective. As long as it is unclear which criterion must be used in order to evaluate the level of reasonable safety that can be expected from an AV, it is uncertain under which conditions an AV(-component) can be held defective. Notwithstanding this uncertainty, it would be surprising, given the high standards in the existing French and Dutch *traffic* liability regimes and the English AEVA 2018, that an "average human driver" is to be used as a point of reference for judging *defectiveness*. In these regimes,[1633] liability is in principle allocated when a vehicle is involved in (France and The Netherlands), or causes (England, AEVA), an accident, unless a form of *force majeure* can be invoked, to which high standards apply. Liability can only be exonerated in The Netherlands when a "perfect" driver could not be blamed; in France when a *faute inexcusable* of the victim was the sole cause of the accident; and in England when a self-driving mode was enabled inappropriately, or when the vehicle's owner failed to install certain crucial security-updates. When a "new" standard of reference regarding *defectiveness* of AVs is to be determined, I argue – if only for the sake of consistency between regulatory frameworks – that a connection is made with the standards of reference for determining (or more precisely: excluding) traffic liability, i.e. that an AV is assessed to be defective when it's driving behaviour is below what is technically achievable, and/or how the "beyond perfect" human driver would have behaved in a comparable situation.

Besides the overall safety comparison with a more or less skilled human driver, the case presents some other criteria that might be relevant for victims to prove defectiveness. For instance, the self-learning AV-algorithms performed an auto-update of the steering software, which might be correlated with a malfunctioning sensor. The case does however neither explicitly state that this

[1633] See sections 4.3.2 (The Netherlands) 4.3.3.2 (France) 4.3.4.4 (England)

sensor-malfunctioning a) resulted from the auto-update; nor b) indicates that this sensor-malfunctioning could have contributed to the accident. It is safe to state that a malfunctioning sensor, "overlooking" the bicyclists (where an "average" human driver would not have overlooked them"), will likely render the AV *defective* in sense of the PLD. However it will be necessary for the victims to investigate the relationship between both the auto-update and the sensor malfunctioning beyond the facts that have been given in the case, which requires a technical analysis of the AV software, and perhaps the APRS-data can be useful in that respect. This in turn requires specific technical knowledge, which "average" victims will likely not possess.

Thus, proving *defectiveness* is not going to be easy for the victims, as it still is unclear whether the safety level of the AV must be compared to an "average" or a "beyond excellent" human driver, and because pinpointing the role that the auto-update and the sensor-malfunctioning could have played in the origination of the accident requires specific technical skills.

APRS database

As assumed, the APRS, which forms part of the core steering software of the AV, falls under the *product* scope of the PLD. In turn, a database in which vehicle data are stored, forms a critical part of the APRS. In this database, for instance records objects and signs on the road are stored, which can be used to calculate safe speeds and distances to be kept. It is given that the APRS contained a vulnerability that could have been used by unauthorized third parties to access and alter the contents of the database. To the extent the database contains *personal data* of for instance the passengers of the car, this would qualify as a *personal data breach* in sense of the GDPR. It can also be imagined that such vulnerability may impact the overall safety of the vehicle. In theory, data regarding objects on the vehicle's path and roadside signs could be altered by a malevolent party, with excessive speeds or collisions as a consequence.

Although (European) case law has not yet addressed the defectiveness of (vehicle) steering software, I argue, parallel to the conformity-provisions and obligations for sellers of consumer goods with digital elements, to provide security-updates under the Consumer Sales Directive,[1634] that vulnerabilities which could have been prevented by a producer by means of a security-update, should render an AV *defective* in sense of the PLD, especially when such vulnerabilities could lead to *personal data breaches*, or unauthorised access to and alteration of the steering software.

[1634] See further: section 4.2.2.3.

Comparable to assessing the *defectiveness* of the AV, it will be uneasy for victims to prove defectiveness of the APRS, as it would require expert knowledge to establish the existence of software vulnerabilities and the potential consequences thereof.

6.2.2.3 CAUSAL RELATIONSHIP

Victims need to prove the causal relationship between *defects* and *damage.* Where national courts are to a certain extent allowed to alleviate the burden of proof (while not reversing it) for victims, the main rule still is that the onus of proof remains with the victims. Often, a *condicio sine qua non*-test must be used to ascertain a causal nexus: would certain damage also have occurred without the defective product, a causal relationship cannot be assumed.

It is clear that personal and material damage had occurred as a consequence of the crash between the AV an the bicyclists. A precise cause of that crash can however not be distilled from the case. The cause of the crash is far from obvious. In order to be successful in the damages claim, victims have to invest in expert knowledge in order to ascertain causality. Victims could of course be assisted by the courts for instance through presumptions or proportional causality mechanisms (which are not harmonised by the PLD). To be sure, they will most likely be dependent of such aids given the current requirements regarding causality, as long as sufficient technical evidence cannot be presented by them.

Uncertainty regarding causality seems less problematic for the victims of the personal data breach. There has been (only) one personal data breach, which can be indicated as the cause of the identity fraud and the non-reimbursable medical costs as well as the blacklisting of the victim for future insurance. It will be easier to prove that this specific damage would not have occurred but for the data breach, than the causal nexus between the failing AV-systems and the personal and material damage of the victims.

6.2.2.4 HEADS OF DAMAGE

Assuming that defectiveness and causation can be proved, it must be recalled that death and personal injuries as well as property damage (other than to the defective product, and with a €500,- threshold) can be remunerable. There are however some implementation differences in the reviewed Member States. Taking these into account, the following damages are likely remunerable under the respective PLD-implementations:

Cat.	Damage	Compensation	Remarks
1	Material damage AV exterior	No	Damage to defective product is non-remunerable under article 9 PLD
	Material damage to the bicycles	Partial	Damage > €500,- is remunerable
2	Material damage AV: exterior damage, internal material damage (battery compartment)	No	
	Material damage to bicycles (need replacing)	Partial	Above €500,-.
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	No threshold
3	Material damage: total loss AV	No	
	Material damage bicycles (need replacing)	Partial	Above €500,-
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	Yes	No threshold. In The Netherlands, also immaterial damages can be remunerable. Also in France immaterial damages can be remunerable. It is uncertain whether pure economic loss can be remunerable under a PLD claim in England. Immaterial damage such as "nervous shock" can be remunerable in the UK.
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	No threshold
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Depends	Economic loss does not fall under the scope of the PLD. Best chance of remuneration is in France, as long as there is no "illegitimate interest". Compensation is unlikely in The Netherlands and in England.

6.2.2.5 DEFENCES FOR THE PRODUCER(S)

Should defects, damages and causality be proven, there are ample defence opportunities for the producers to escape liability.

It can for instance be argued that the fact that the defect in the operating system came into existence *after* the AV (with incorporated software) was "put into circulation" in the sense of article 7(b) PLD, as this defect was the result of a specific auto-update that was not intended by the producer. On the other hand, it can be argued that this defect formed an intrinsic part of the AV at the time it was marketed, as the operating software enabled auto-updating without "a push"

by the producer, and without a choice of the car-owner.[1635] As long as there is no case law available, it will be uncertain whether or not this defence can successfully be made by the producer. Again in line with the obligations for sellers of "goods with digital elements" under the Consumer Sales Directive, I hold the opinion that providers of such products should have the obligation to supply consumers with (security) updates during a certain period.[1636] In line with that obligation, producers must during that time not be able to invoke the 7(b) PLD defence.

Regarding the vulnerability in the APRS, it seems that the defect did exist before it was put into circulation, but it was only discovered after it was brought to market. Therefore, the producer cannot rely on the "later existence" defence regarding the APRS-vulnerability.

A second possibility is that the producer invokes the development risks defence as incorporated in article 7(e) PLD. A producer is exempted from product liability if he can show that he could not have discovered the defect, taking account of any and all available scientific and technical knowledge accessible at the time of marketing of the respective AV. Given the facts of the case study, it must be shown that the specific defects that occurred could not have been discovered taking account of the most advanced scientific and technical knowledge. This implicates that it must be established that the sensor-malfunctioning as a result of the auto-update could not have been foreseen by the producer. Comparable to the "later existence defence", the point of discussion will be whether or not a producer could foresee all different directions that self-learning, auto-updating operating software may take during the course of its deployment - and its corresponding effects on the functioning of the AV. When the answer to this question would be that not every direction (in general) can be foreseen, and that, more specifically, the respective defect could not have been discovered after a 'diligent search', a successful claim on the development risk defence is plausible. This holds also true for the vulnerability in the operating software: when it can be shown that it was not discoverable for the producer, product liability can be avoided. I argue, in line with the obligation under the CSD to provide software (security) updates, that a producer must not be able to successfully invoke the development risks defence when he had failed to provide such updates.

A third possibility for the producer is to rely on the contributory negligence defence enshrined in article 8(2) PLD. In this case, the fact that the bicyclists ignored a red traffic light might be used to reduce the liability by the producer towards the cyclists (but not the other victims).

[1635] See in this vein for instance Vellinga 2020, p. 157. Differently Tange & Werbrouck 2021, p. 344.
[1636] See the previous section, and section 4.2.2.3.

6.2.2.6 *SUMMARY*

In summary, it can be concluded that it will be not easy for victims to establish defectiveness without a) technical expertise; and/or b) procedural "aids" by judges. This holds also true for the causal connection (*condicio sine qua non*) between defects and damages. Even when defectiveness and causality can be established, damage compensation is limited, as damage to the AV itself is not remunerable, and the hefty damages that may result from the data breach are not covered by the PLD. Furthermore, producers have the opportunity to invoke for instance a "development risk-", a "later existence-" and a "contributory negligence" defence, which may be easier for them to underpin with evidence, as such information is better accessible and interpretable for producers than for victims.

6.2.3 *THE INNOVATORS PERSPECTIVE*

6.2.3.1 *LEGAL CERTAINTY*

As argued in section 3.4.2.2, legal uncertainty could negatively impact investments in innovation. When it is difficult or impossible for innovators to reasonably foresee and to calculate risks that may result from a regulatory framework that applies to the development and deployment of novel technology, a negative impact on investment decisions can be predicted. Despite the fact that the European product liability framework is formulated in a technology neutral way, and has remained largely the same in the decades since its introduction, there are indeed "uncertain outcomes" for innovators when the rules are applied to the facts of the case study.

It is likely that the (implemented) rules of the PLD apply to the AV and its incorporated APRS software, but it is less certain whether or not those products can be qualified as *defective*. Regarding the AV in its entirety, it is, given the current absence of relevant case law, not clear which driving behaviour the public may reasonably expect, and whether that behaviour must either be compared to "average" or "beyond excellent" human driving skills. Moreover, it is not certain that the automatically updated software and/or the malfunctioning sensor rendered the AV *defective*. Also regarding the vulnerability in the APRS, it is not certain whether this would implicate *defectiveness*, as also at this point, case law does not provide the necessary guidance. This in turn leads to uncertainties for producers regarding the standard they have to comply with, in order to "calculate" their product liability risks.

Furthermore the applicable rules require that victims can prove that AV-defects are *condicio sine qua non* for the occurrence of the damage. It is unlikely that victims will easily succeed in proving such causal relationship, at least not without expert skills and procedural aids. It follows from case law however, that it is likely that judges will assist victims at this point at least to some extent.

The *types of damage* to be compensated are more clear, should defectiveness and causality eventually be established. Some uncertainty is present with regard to the answer to the question whether or not pure economic loss is remunerable under the reviewed PLD implementations. In France, it is likely that economic losses are remunerable, which is not the case in England and The Netherlands.

Applicability of the defences that producers may invoke is less certain. Regarding the *later existence* defence, it is not sure whether or not a *defect* such as the malfunctioning sensor that came into existence after the AV was sold, but which might be the result of built-in self-learning capacities of the AV's software, would disallow a successful defence invocation by its producer. It is less uncertain that a producer could successfully invoke a *development risk* defence, as long as he can illustrate the efforts he had undertaken to discover the potential defects. A successful *contributory negligence* claim requires the producer to prove negligent behaviour by victims. This is, to a certain extent comparable to the position of victims to prove *causality*, and thus not an easy task, as this would require technical analysis of the accident data. However, it is likely that producers can more easily access the necessary data, and the required expertise to interpret these data than victims would.

All in all, the most prominent uncertainties concern *defectiveness*, *causation*, and the applicability of the *later existence* and *contributory negligence* defences, which will make it difficult to foresee and to calculate the product liability risks for innovators given the facts of the case study; this could therefore negatively impact their decisions to invest in AV technology.

6.2.3.2 STRINGENCY

As stated in section 3.4.2.3, in order to determine the *stringency* of a regulatory framework, it must be assessed to what extent innovators must significantly adapt their behaviour in order to comply with regulation. Behavioural changes are particularly evident when new regulation is introduced, which necessitates a "behavioural change" by innovators. This was for instance the case upon the introduction of the General Data Protection Regulation, which is further elaborated upon in section 5.2 above, and section 6.4 below. At the same time, *stringency* may also be the result of a heavily regulated market, which makes it burdensome for newcomers to enter a respective market, as large upfront compliance costs are required. Also, high liability risks could bring about a high level of *stringency*.

The Product Liability Framework is far from new, and it has remained largely the same since its introduction in 1985. The rules contained in the PLD in itself, do not result in hefty upfront compliance costs for newcomers. Perhaps only the 'due diligence' regarding the "state of the

scientific and technical knowledge" in order to discover potential defects for *development risks defence* purposes, would qualify as upfront compliance costs that may result from the PLD.

Regarding the liability risks for innovators as such that actually result from the application of the PLD, the following can be observed. As it stands, it is an uneasy challenge for victims to get their damages compensated under the PLD framework (which is further elaborated in section 6.2.4). As stated, expert knowledge and procedural aids are required to establish *defectiveness*, *damage* and *causality*. At the same time, there is ample opportunity for producers to fend off claims, such as by means of the *development risks-*, *later existence*, and *contributory negligence* defences, where producers are in a better position regarding for instance accident data analysis than victims.[1637] This might result therein that victims cannot easily claim compensation from producers, while being exposed to risks beyond their control. These risks, which may result from wrongful auto-updates causing sensor malfunctioning, or vulnerabilities in the APRS, *could* have been controlled by the respective producers. However, the current PLD rules did not necessitate such risk-control, as potential defects might have come into existence after the AV was sold, or could not have been detected at that time.

Based on the above, it can be observed that the current product liability framework is not stringent, and would likely not negatively impact innovation. It can even be argued that the actual framework is not stringent enough (as, among other things, induces rather than removes information asymmetries between producers and consumers), and it is, in a general sense, questionable whether the PLD-purpose of consumer protection for AV users and (other) victims of AV-related accidents is still adequately served.

6.2.3.3 FLEXIBILITY

Two aspects of flexibility can be identified in regulation, as observed in section 3.4.2.4, which may influence the development and deployment of AVs. First, when regulation necessitates certain ex ante compliance, it would be better for innovation when innovators have more manoeuvring space to reach compliance than when the implementation paths are limited. Second, rules that are adaptable to (technological) change are, from a innovation-stimulating perspective, preferred over technology specific rules, which are less adaptable to changing circumstances.

When reviewing the first aspect, it can be observed that the PLD does generally not require much upfront compliance efforts to be made by innovators. As mentioned in the previous section, such efforts may only have to be made in order to ensure that a *development risk defence* claim can be successful. In that regard, producers should ensure that the "state of technological and scientific

[1637] See also Bertolini 2020, p. 60-61; European Commission 2018, p. 8-10; European Commission 2020, p. 27-29.

knowledge" does not indicate a potential defect. The PLD does not prescribe which actions need to be taken by producers, as long as the "most advanced level" of technical and scientific knowledge is taken into account that was accessible for producers – irrespective of the costs thereof.

Regarding the second aspect, it must be stated that the norms of the PLD are formulated in a technology neutral way. Those norms may however not be entirely fit to address the challenges that follow from the development and deployment of AVs, as was illustrated in the previous section. That is not a result of any inflexibility of those norms, but rather of the legislative choices that were made *inter alia* regarding the notion of defectiveness, the broadness of the defences for producers, and the procedural implications of the burden of proof, which has become less easy to satisfy as a result of the increased complexity of the technology.

It can be stated that the current flexibility in the product liability framework does not negatively impact innovation, as the norms are in themselves flexible, and innovators have ample opportunity to choose their own compliance routes.

6.2.4 THE CONSUMERS PERSPECTIVE

6.2.4.1 RISK

In section 3.4.3.2, it was observed that it may negatively impact the adoption of novel technology, when that technology – and the rules that apply thereto – results in *inter alia* financial risks for consumers.

It has become clear from the analysis of the case study, that it is very uncertain that victims can successfully claim damages from producers based on the Product Liability rules. In a procedure, victims will have to prove evidence of *defects*, *damage* and *causality*, which is hardly possible without procedural aids and technological expertise. Compared to accidents with "traditional" non-autonomous vehicles, more specialised technological expertise is necessary, as this would involve *inter alia* an in-depth analysis of the algorithms underlying the auto-update that have been performed, the potential sensor malfunctioning and the effects thereof on the AV's driving behaviour. At the same time, the necessary data and technological expertise are readily available for the defending producers, which thus constitute information asymmetry between producers and consumers.

When the necessary evidence cannot be produced, or when a producer successfully invokes a defence, the victims are unable to have their damages compensated under the PLD. Even in case of a successful claim, some of the damages resulting from the accident will not be compensated. For instance, the damage to the AV itself is not remunerable under the PLD. Moreover, the identity

fraud which took place after the personal data breach which resulted in non-reimbursable costs, qualifies as "pure economic loss", which is not easily remunerable under the implementations in England and The Netherlands.

Thus, the PLD presents a significant risk to victims, i.e. that they cannot establish a successful product liability claim, and that even when a producer can be held liable, not all damages will have to be compensated. These risks resulting from the PLD likely have a negative impact on the acceptance of AVs.

6.2.4.2 TRUST

As illustrated in section 3.4.3.3, trust is an important factor for the acceptance of a novel technology by consumers. Trust regarding *inter alia* the safety of a product is stated to be necessary for adoption of technology, as would be trust in the "reparative capacities" of in this case the product liability framework when victims suffered damage due to a (nonetheless) unsafe product.

Regarding trust in safety of AVs, such as the vehicle depicted in the case study, the following can be observed. Currently, an explicit safety level for AVs cannot be derived from the regulatory framework on product liability. Without further guidance, it may well be the case for now that AVs may "only" have to be as safe as the average human driver, which will implicate less trust than when the safety of an AV must be beyond "excellent" human driving skills. Furthermore, it is questionable whether victims may trust that appliance of the PLD-rules results in a fair distribution of risks between producers and consumers. Based on the observations in the previous section, even a bolder statement can be made. As the risks are significant that victims cannot successfully claim damages under the PLD as a result of "increased complexity" of vehicle-technology – and the increased information asymmetry as a consequence thereof, it can be assumed that this negatively impacts consumer's trust regarding a fair distribution of damages.

6.2.5 CROSS-EXAMINATION

In summary, it has been argued that the PLD implicates uncertainties for innovators regarding *defectiveness*, *causation*, and the applicability of the *later existence* and *contributory negligence* defences, which will make it uneasy to foresee and to calculate the product liability risks for innovators given the facts of the case study; this could therefore negatively impact their decisions to invest in AV technology. Parallel to these uncertainties for innovators, it is also uncertain for victims of AV-accidents whether they can successfully claim damages from a producer of a defective AV, given the hurdles victims face in order to prove *defectiveness, damages* and *causation*, and given the uncertainty whether certain damages are remunerable under the PLD. Furthermore, the current rules can be stated to negatively impact consumer's trust in both the

safety of the products, and the fair damage-distribution between producers and victims of AV-accidents. These uncertainties may both negatively impact innovators decisions to invest in developing and deploying AV-technology - contrary to the innovation-stimulation purposes of the PLD,[1638] and do not positively impact the actual financial risks that can result from accidents in which AV-technology is involved, as well as the consumer's trust that can be correlated with these risks – in spite of the consumer-protection objectives of the PLD.[1639]

On a more positive note (for innovators), the PLD framework does not prove to be very stringent; upfront compliance costs are minimal, and liability risks are mainly for victims, which does likely not negatively impact innovation. Again the circumstance that there is an disbalance in liability risks, which as a result of the current product liability rules rests mainly on the shoulders of victims, will likely not positively impact the consumer acceptance of AV-technology.

Flexibility of the rules stemming from the product liability framework seems not to be problematic for innovators, as the PLD is formulated in a technology neutral way. Insofar as upfront compliance is required, innovators are free to choose the most suitable path for compliance. It is not likely that these flexibilities have a negative impact on the acceptance of AV-technology.

6.3 TRAFFIC LIABILITY

6.3.1 SOLVING THE CASE

A slight variation in the "fixed facts" of the case study is necessary here.[1640] In order to address the potential influence of the current traffic liability regimes on innovation, it needs to be made clear what the current rules may imply for innovators. The traffic liability regimes under review do not address car-producers, which were the "innovators" under review in the foregoing sections . However, this does not entail that traffic liability rules cannot be relevant for innovators. Rental companies adding AVs to their fleet, for example can be subject to traffic liability rules when rented-out AVs are involved in traffic accidents. Therefore, the case study's fixed fact that *"The car was directly sold by the manufacturer to its owner, a "normal consumer""* is amended as follows:

1. The car was directly sold by the manufacturer to its owner, a car-rental company who rented the AV out to a "normal consumer".

[1638] See section 4.2.2.1.
[1639] Ibidem.
[1640] See section 6.1

In the following sections, first the question will be addressed to what extent the innovator, i.e. the AV-rental company, can be held to compensate the damages suffered by the victims as sketched in the case, i.e. the passengers and the bicyclists based on the regulatory frameworks on traffic liability. This question is answered per jurisdiction: Section 6.3.1.1 addresses The Netherlands, I analyse the French system in section 6.3.1.1.1, and I focus on England in section 6.3.1.3.[1641] After that, I analyse the factors existing in the traffic liability framework which could influence innovation and acceptance of innovation in the field of AVs, from the *innovators perspective* in section 6.3.2 and the *consumers perspective* in section 6.3.4.

6.3.1.1 THE NETHERLANDS

The specific risk-based traffic liability rules under article 185 WVW as well as the generic extra-contractual liability rules of article 6:162 BW and the risk liability rules of article 6:173 BW regarding hazardous goods must be applied to the case, in order to assess if and to what extent the respective victims can successfully claim remuneration from the AV rental company. The bicyclists can base their claim on article 185 WVW, which does not apply to the AV-passengers, who could use article 6:162 BW or 6:173 BW as a basis for their compensation claims.

6.3.1.1.1 185 WVW

To successfully allocate liability, the bicyclists need to prove that the AV was involved in a traffic accident – which is not a problem given the facts of the case, and can safely be assumed here. The owner (or keeper), in this case the AV-rental company can only then avoid liability when he can prove *overmacht*, i.e. that the accident was solely due to another person's fault, which was so improbable that the driver (i.e. the AV's steering software) could not reasonable have been taken into account. Liability can be reduced on the basis of the *eigen schuld* (contributory negligence) rules.[1642] *Overmacht* and *eigen schuld* are addressed in turn below.

The case sketches two possible facts that might constitute *overmacht*. Firstly, it is known that the bicyclists ignored a red traffic light. However, considering the applicable case-law, this would not be sufficient to prove *overmacht*, as it can reasonably be expected that bicyclists are ignoring the red-light rules. It would for instance be necessary that, besides ignoring the obligation to stop, the bicyclists could not have been detected by the AV. That could for example be the case when the bicyclists just "appeared" from behind a parked bus whilst driving through the red light. Secondly, there was a sensor-malfunction that can be related to an automatic update that was pushed by the AV-producer, which had not been agreed by the vehicle owner. Further to standard case law, it is

[1641] References to legislation and literature are not repeated here, occasional reference is made to 'new' sources, which had not been used in the aforementioned section.
[1642] I recall that this defence can in practice only be invoked when the victims are at least 14 years old – which is the case here.

likely that these "technical defects", comparable to the more traditional defects of a mechanical nature, will not constitute *overmacht* for the vehicle owner.

Thus, I think it is likely that the rental company is liable towards the bicyclists. In principle, all reasonably attributable damages have to be compensated, unless *eigen schuld* (contributory negligence) can be proven. To that end, it must be evaluated to what extent the victim's own fault contributed to the damage, which can be used to apportion damages between the owner and the victim. It follows from case law however that for victims older than 14 years of age, principles of fairness dictate that at least 50% of the damages needs to be borne by the vehicle owner – even when the victim's share in the causation of the accident exceeded that percentage. Given the facts of the case, a 20% reduction of the liability of the AV-owner seems plausible.

Differently from the Dutch PLD-implementation, there are no types of damages that are a priori excluded from remunerability under article 185 WVW, be it that damage to people and goods inside the vehicle as well as damage to the vehicle itself fall outside the scope of the provision as stated above. In the table hereunder, I indicate which damages could qualify for remuneration.

Cat.	Damage	Compensation	Remarks
1	Material damage AV exterior	No	Damage to AV itself is non-remunerable under article 185 WVW
	Material damage to the bicycles	Yes	-20% (*eigen schuld*)
2	Material damage AV: exterior damage, internal material damage (battery compartment)	No	
	Material damage to bicycles (need replacing)	Yes	-20% (*eigen schuld*)
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	
3	Material damage: total loss AV	No	
	Material damage bicycles (need replacing)	Yes	-20% (*eigen schuld*)
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	No	Damage to people in the AV is non-remunerable under article 185 WVW.
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	-20% (*eigen schuld*)
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Unlikely	It is unlikely that pure economic loss is remunerable under article 185 WVW, especially as the data breach is likely not closely connected to the accident (see further section 6.4).

6.3.1.1.2 6:162 BW

In a claim based on article 6:162 BW, victims have to prove an *unlawful act* (a conduct or an omission) which can be *attributed to* the driver or owner of an AV; and that the unlawful act *caused damage*. Under the current framework, article 6:162 BW holds several hurdles for the victims of AV-accidents to be successful in a damages claim as illustrated below, which are more significant than those regarding traffic liability of article 185 WVW. Furthermore, the AV-owner can invoke certain defences, including *overmacht* (force majeure), and may moreover seek to reduce his obligation to compensate damages on the basis of the *eigen schuld* (contributory negligence) defence.

A first problem regards the question whether or not an *unlawful act* can be constituted. Traditionally, a human driver could for instance be blamed for ignoring a rule of traffic regulation, or to be driving carelessly, i.e. "contrary to what is appropriate in society", or otherwise causing danger or hindrance. When, as in the case, a human does no longer drive the vehicle, it will be hard if not impossible to establish an unlawful *conduct*, especially when an AV operator was not aware of certain defects or dangers that might have become inherent in the vehicle. Contrarily, an unlawful *omission* could still be construed, for instance as the vehicle owner deliberately allowed the AV on the road, while having knowledge of potential unsafety of the vehicle (for example as a result of an omission to implement safety-updates) which might cause a norm-violation. When the AV-owner did not know, and ought not to know, that its vehicle held a defect which might cause a norm-violation, an *unlawful act* cannot likely be construed under the current regime. Given the facts of the case, namely that the auto-update might be related to the malfunctioning sensor concretely holds two problems. Firstly, the auto-update did not require any intervention by the vehicle-owner: it was implemented autonomously, so without the knowledge of the driver. Secondly, it is not evident that the auto-update could be related to the malfunctioning sensor. This requires further (technical) investigation. Thus, I think it is hard to establish an *unlawful act* for victims who seek damage compensation, unless a judge broadly interprets and assumes the unlawfulness criterion. However, I consider it unlikely that a judge would assume unlawfulness under the fault liability rules of 6:162 BW under the given circumstances.[1643]

When an *unlawful act* by the AV-owner is nonetheless assumed, it must furthermore be established that it can be attributed to him. This is less problematic, as the standard for attribution is very low, given that legal blameworthiness suffices in traffic liability cases. When compared to

[1643] See furthermore section 4.3.2.3 and the references/examples there regarding apportionment of damages.

the *meppelse ree*-case, it can easily be construed that the AV should have been able to avoid the collision.

Besides *unlawfulness* and *attributability*, victims have to prove *causality* between the *unlawful act* and the *damage* that occurred. In theory, it is hard for victims to prove such causal relationship. In principle, it is required that the victim can establish that the damage would not have occurred without the unlawful act. In this case, that would be hard, as the facts do not explicate that the auto-update led to a malfunctioning sensor, and it furthermore is not clear that the accident could have been avoided when the sensor would have been functioning. Thus, extensive technical analysis of the accident- and vehicle data is necessary, which likely needs to be carried out by an expert. In practice however, victims are often aided under the 6:162 BW-regime, either through causality presumptions, the reversal rule ("omkeringsregel") or even through a reversal of the burden of proof.[1644] Both mechanisms would significantly aid the victim, as this would in fact require the AV-owner to either rebut the presumption, or to prove an absence of causality – which requires the AV-owner to carry out the necessary technical assessments.

Should *unlawfulness, attributability* and *causality* be established, the AV-owner could reduce liability by proving *overmacht*, or *contributory negligence* of the victims, similar as under an article 185 WVW-claim. When applying the *own* fault-rule to the case, it is likely that the liability of the AV-owner is reduced by 20%.

When an *unlawful act* can be proven (again: I make a strong proviso regarding the *unlawfulness* of the behaviour of the vehicle owner), the following types of damage could qualify for remuneration.

[1644] See section 4.3.2.4.1.

Cat.	Damage	Compensation	Remarks
1	Material damage AV exterior	Yes	Differently from article 185 WVW and the PLD-implementation, damage to the AV is not excluded under article 6:162 BW. However: -20% (*eigen schuld*)
	Material damage to the bicycles	Yes	-20% (*eigen schuld*)
2	Material damage AV: exterior damage, internal material damage (battery compartment)	Yes	-20% (*eigen schuld*)
	Material damage to bicycles (need replacing)	Yes	-20% (*eigen schuld*)
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	-20% (*eigen schuld*)
3	Material damage: total loss AV	Yes	-20% (*eigen schuld*)
	Material damage bicycles (need replacing)	Yes	-20% (*eigen schuld*)
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	Yes	Differently from article 185 WVW, damage to people in the AV is remunerable under article 6:162 BW. However: -20% (*eigen schuld*)
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	-20% (*eigen schuld*)
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Unlikely	It is unlikely that pure economic loss is remunerable under article 6:162 WVW, especially as the data breach is likely not closely connected to the accident (see further section 6.4).

However, as stated above, I consider it unlikely that *unlawfulness* can be proven under article 6:162 BW. What remains, is a possible claim under article 6:173 BW, regarding risk liability of the possessor of *defective goods*, which is elaborated in the following section.

6.3.1.1.3 6:173 BW

In order to establish liability under article 6:173 BW, a victim must prove that the respective good was *defective*, i.e. not meeting the safety requirements that might be expected, which *caused damage*. The AV-possessor (in this case the vehicle owner) may invoke several defences, including that there was no *objective knowledge* of the defect; *overmacht*; that liability must be channelled towards the producer (in case of a *defective product* in sense of article 6:185 BW and the damages exceed € 500,-); and *eigen schuld* to reduce his obligation to compensate damages – as I illustrate below.

It is not yet clear which standard must be taken as a point of reference in order to assess *defectiveness* in sense of article 6:173 BW. Thus, it is at the moment not sure when liability can be

established regarding accidents that can be correlated with AV-accidents. The opinions differ between a rather low standard, comparable to the standard of *defective products* in sense of article 6:185 BW (PLD-implementation) and, given the *Betriebsgefahr* of AV's, comparable to the "best human drivers". It can also be argued that a comparison is made with the *legal blameworthiness* doctrine that is used to assess the attributability in article 185 WVW-cases. Even if it were only for the sake of consistency between the risk liability regimes applicable to traffic accidents, I would plead for applying this latter standard. This would furthermore correspond with the "risk liability" nature of article 6:173. Should such a strict standard be applied to the facts of the case, it is still not sure whether the AV in question would be *defective*. However, it can be construed that it might be expected from a fully autonomous AV that it should be able to avoid collisions as the one depicted in the case.

As discussed above, it can be problematic for victims to prove *causality*, i.e. that the accident was the result of the materialisation of the hazard in the AV, although judges tend to aid victims in this sense.

Even when liability on the ground of article 6:173 can be established, there are ample opportunities for the AV-rental company to fight off the liability claim. The rental company could for instance invoke that there was *no objective knowledge* of the problem in the AVs steering software and/or its sensor, or that the problem got to be known so shortly before the accident that no preventive actions could have been taken – although that requires thorough substantiation with facts which the case does not provide, which thus necessitates further analysis to the origination of the defect. Also, the AV-rental company could state that the AV was defective in sense of the PLD-implementation in article 6:185 BW,[1645] and that liability must be channelled towards the producer. That is *unless* the €500,- damages franchise is not met, or the defect did not exist at the time of putting the AV into circulation – which is for the victim to prove. Comparable to the *later-existence* defence discussion in section 6.2.2.5 the moment of origination of a potential defect in the AV steering software is uncertain, and would in any case require further technical analysis. Even when product liability can be established, the producer may successfully invoke a *later existence-* or a *development risk* defence, ultimately leaving the victims empty handed.

Another possibility for the AV-rental company is to invoke *overmacht* as a defence, which is not likely as shown in the previous sections, and to seek reduction of liability on the basis of *eigen schuld* of the bicyclists, which would likely reduce 20% of the damages compensation obligation.

[1645] However, as illustrated in section 6.2.2.2, this would also require further technical analysis of the accident and vehicle data, and is not going to be easy.

When risk liability for the possessor of a defective AV can be proven (which will be not easy as explained above), the following types of damage could qualify for remuneration.

Cat.	Damage	Compensation	Remarks
1	Material damage AV exterior	Yes	Differently from article 185 WVW and the PLD-implementation, damage to the AV is not excluded under article 6:173 BW. However: -20% (*eigen schuld*)
	Material damage to the bicycles	Yes	-20% (*eigen schuld*)
2	Material damage AV: exterior damage, internal material damage (battery compartment)	Yes	-20% (*eigen schuld*)
	Material damage to bicycles (need replacing)	Yes	-20% (*eigen schuld*)
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	-20% (*eigen schuld*)
3	Material damage: total loss AV	Yes	-20% (*eigen schuld*)
	Material damage bicycles (need replacing)	Yes	-20% (*eigen schuld*)
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	Yes	Differently from article 185 WVW, damage to people in the AV is remunerable under article 6:173 BW. However: -20% (*eigen schuld*)
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	-20% (*eigen schuld*)
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Unlikely	It is unlikely that pure economic loss is remunerable under article 6:173 WVW, especially as the data breach is likely not closely connected to the accident (see further section 6.4).

6.3.1.1.4 SUMMARY

The answers to the question to what extent the innovator, i.e. the entity who markets the innovative AV-technology, being the AV-rental company, can be held to compensate the damages suffered by the victims as sketched in the case, i.e. the passengers and the bicyclists, based on the regulatory frameworks on traffic liability can be summarized as follows.

Under the traffic liability rules of article 185 WVW, it is likely that the bicyclists' damages must be compensated, up to a level of 80% given the *own fault* of the bicyclists resulting from ignoring the red traffic light. The damages of the passengers of the AV, and the damage to the AV itself are however not remunerable under article 185 WVW.

It is unlikely, or at least highly uncertain, that article 6:162 BW can successfully invoked by the victims (including the AV-passengers) against the AV-rental company, as an *unlawful act* may not

be established by the victims, regarding the facts of the case. There was no action or omission that could qualify as such. Even if a judge interprets the rule very broadly, victims will face hurdles regarding the proof of causality.

Whether or not victims (including the AV-passengers) can be successful in a claim based on article 6:173 BW is very uncertain. That is mainly because there is no clear standard yet of *defectiveness*, and the possibilities for the defendant to channel liability towards the producer on the basis of article 6:185 BW). In order to prevent such channelling, victims have to prove that the *defect* did not exist at the time the AV was brought into commercial circulation. Expert technical knowledge is required in that respect. Should victims be unable to establish that the defect existed at the time of introduction to the market of the AV, the claim can be forwarded to the producer(s), under the product liability rules. In that case, victims must, as addressed in section 6.2, prove *defectiveness* (which holds a different standard than defectiveness under 6:173 BW), *causality* and *damage*, which is uneasy, and the *later existence*- and/or *development risks* defences may result therein that a compensation claim is rejected.

Thus, it is likely that the damages of the bicyclists are compensated to a maximum of 80% under article 185 WVW. It is improbable that damages of the passengers are remunerable under an article 6:162 BW claim, and it is very uncertain that a claim under article 6:173 BW can be successful. These observations are illustrated in the table below.

Cat.	Damage	Compensation	Remarks
1	Material damage AV exterior	Unlikely	Excluded under art. 185 WVW; Art. 6:162 BW likely not applicable Uncertain whether a successful claim can be made under article 6:173
	Material damage to the bicycles	Yes	To be compensated by the AV-rental company on the basis of article 185 WVW. -20% (*eigen schuld*)
2	Material damage AV: exterior damage, internal material damage (battery compartment)	Unlikely	Excluded under art. 185 WVW; Art. 6:162 BW likely not applicable Uncertain whether a successful claim can be made under article 6:173
	Material damage to bicycles (need replacing)	Yes	To be compensated by the AV-rental company on the basis of article 185 WVW. -20% (*eigen schuld*)
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	To be compensated by the AV-rental company on the basis of article 185 WVW. -20% (*eigen schuld*)
3	Material damage: total loss AV	Unlikely	Excluded under art. 185 WVW; Art. 6:162 BW likely not applicable Uncertain whether a successful claim can be made under article 6:173
	Material damage bicycles (need replacing)	Yes	To be compensated by the AV-rental company on the basis of article 185 WVW. -20% (*eigen schuld*)
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	Unlikely	Excluded under art. 185 WVW; Art. 6:162 BW likely not applicable Uncertain whether a successful claim can be made under article 6:173
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	To be compensated by the AV-rental company on the basis of article 185 WVW. -20% (*eigen schuld*)
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Unlikely	Not excluded for the bicyclists under article 185 WVW; Art. 6:162 BW likely not applicable; Uncertain whether a successful claim can be made under article 6:173. It is unlikely that pure economic loss is remunerable under article 185 WVW, 6:162 or 6:173 BW, especially as the data breach is likely not closely connected to the accident (see further section 6.4).

6.3.1.2 *FRANCE*

Liability under the *Loi Badinter* can easily be established, as the AV is *involved* in a traffic accident. In the absence of a *conducteur* (driver) of the AV, the AV-rental company as the keeper (owners are deemed keepers) can be sought by the victims for compensation of their damages. This includes the passengers of the AV. In principle all damages which are sufficiently closely connected to the accident qualify for remuneration, as it is not likely that a *faute inexcusable* of (any of the) victims can be proved. Given the applicable case law, it can likely not be established (by the defendant) that the non-motorized bicyclists' ignorance of the red traffic light would qualify as gross negligence from which a "reasonable person" would have refrained. This results therein that 100% of the personal damages of the bicyclists can be remunerable. Regarding their property damage, ignorance of the red traffic light could qualify as *own fault* of the bicyclist, which could lead to a reduction of the damage-compensation obligation of the AV-rental company.

As the facts of the case do not state anything that could qualify as *own fault* of the passengers, I consider it likely that their damages (both personal- and property damages) are remunerable. These observations are illustrated in the table below:

Cat.	Damage	Compensation	Remarks
1	Material damage AV exterior	Yes	Full compensation
	Material damage to the bicycles	Yes	Reduction possible for *own fault* bicyclists
2	Material damage AV: exterior damage, internal material damage (battery compartment)	Yes	Full compensation
	Material damage to bicycles (need replacing)	Yes	Reduction possible for *own fault* bicyclists
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	Full compensation
3	Material damage: total loss AV	Yes	Full compensation
	Material damage bicycles (need replacing)	Yes	Reduction possible for *own fault* bicyclists
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	Yes	Full compensation
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	Full compensation
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Unlikely	Not excluded under the *Loi Badinter*, however the data breach is likely not closely connected to the accident (see further section 6.4).

6.3.1.3 ENGLAND

6.3.1.3.1 NEGLIGENCE

The negligence rules that are traditionally applied in traffic liability cases, adhere to a *breach of a duty of care* of a *driver.* As sketched in the case, there is no human driver involved in the traffic accident. Thus, the negligence rules seem to be of no significance in this respect. Comparable to The Netherlands and France, with the enforcement of the AEVA 2018, there are also risk-liability rules effective that may be used to hold the AV-rental company liable.

6.3.1.3.2 AEVA 2018

Under the AEVA 2018, victims must prove that the AV itself *caused* the accident, and that they have suffered damage *as a result* of that accident in order to successfully hold the insurer, or the AV-rental company liable.[1646]

The causality requirement is different from the risk-based traffic liability rules in France and The Netherlands, where it is sufficient to prove involvement of a vehicle in a traffic accident. Under the AEVA 2018, it will thus be necessary for victims to prove that there is a causal nexus between the behaviour of the AV and the origination of the accident, and in turn between the accident and the damage. As argued above, that will not be easy given the facts of the case. Until further guidance is provided by the English courts regarding for instance presumptions or perhaps even reversal of the burden of proof (which is not very likely given actual case law), I assume that accident data must be acquired, and expert knowledge is required to interpret these data in order to establish causality.

Should causality be established, the obligation to compensate damages that resulted from the AV-accident is to be reduced insofar this can be attributed to *contributory negligence* of the victims.

When causality *can* be established, it must be noted that the insurer (or the AV-rental company as the car owner, when there would be no duty for the insurer to compensate the victims) is obliged to remunerate the personal- and property damages of the bicyclists and the AV-passengers, although damage to the AV itself (and several goods carried within the AV in custody/under control of the insured person) are exempted. These observations are illustrated in the table below:

[1646] It must be noted that the insurance company must be sought for remuneration primarily.

Cat.	Damage	Compensation	Remarks
1	Material damage AV exterior	No	Not remunerable under the AEVA 2018
	Material damage to the bicycles	Yes	Reduction possible for *contributory negligence* bicyclists
2	Material damage AV: exterior damage, internal material damage (battery compartment)	No	Not remunerable under the AEVA 2018
	Material damage to bicycles (need replacing)	Yes	Reduction possible for *contributory negligence* bicyclists
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	Reduction possible for *contributory negligence* bicyclists
3	Material damage: total loss AV	No	Not remunerable under the AEVA 2018
	Material damage bicycles (need replacing)	Yes	Reduction possible for *contributory negligence* bicyclists
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	Yes	Full compensation
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	Reduction possible for *contributory negligence* bicyclists
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Unlikely	Likely not remunerable under the AEVA 2018, and the data breach is likely not closely connected to the accident (see further section 6.4).

6.3.2 *INTERMEZZO: DAMAGES OVERVIEW*

In order to illustrate the similarities and differences between the three reviewed traffic liability regimes, I illustrate in the table below which damage likely (or not) qualify for compensation.[1647]

Cat.	**Damage**	**Compensation possible**		
		Netherlands	*France*	*England*
1	Material damage AV exterior	Unlikely	Yes	No
	Material damage to the bicycles	Yes	Yes	Yes
2	Material damage AV: exterior damage, internal material damage (battery compartment)	Unlikely	Yes	No
	Material damage to bicycles (need replacing)	Yes	Yes	Yes
	Personal damage to bicyclists (hospital costs, inability to work)	Yes	Yes	Yes
3	Material damage: total loss AV	Unlikely	Yes	No
	Material damage bicycles (need replacing)	Yes	Yes	Yes
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	Unlikely	Yes	Yes
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	Yes	Yes	Yes
	Data breach: economic loss (non-reimbursement medical costs; blacklisting)	Unlikely	Unlikely	Unlikely

[1647] It must be noted that reductions based on contributory negligence have not been taken into account in the table.

6.3.3 *THE INNOVATORS PERSPECTIVE*

6.3.3.1 *LEGAL CERTAINTY*

As stated in section 3.4.2.2, material legal uncertainty could negatively impact investments in innovation. Uncertainty may occur when it is difficult or impossible for innovators to reasonably foresee and to calculate risks that may result from the regulatory frameworks on, in this case, traffic liability. Different observations can be made regarding the three reviewed jurisdictions.

In **The Netherlands**, there are even further differentiations to be observed regarding legal certainty. The "dedicated" framework of article 185 WVW regarding liability for motor vehicle accidents, results in little or no legal uncertainty for innovators. The rules are formulated in a technology neutral way, and are similarly applicable to autonomous vehicles as to "traditional" motor vehicles. The single involvement in a traffic accident is sufficient to establish liability for the owner or keeper of the vehicle, in this case the rental company. It is furthermore clear how damages are apportioned, be it that the actual calculation does necessitate an analysis of *own fault* of the victims, which is to be carried out by the defendant. This can be complex, as expert knowledge will be required to analyse for instance accident data. It is also certain that there are no damage remuneration obligations towards for example passengers of the AV, and passengers of other motorised vehicles that can potentially be involved in a crash. Whether or not compensation obligations might follow from other liability regimes, including *unlawful act* (6:162 BW), or risk liability for *defective goods* (6:173 BW) is however less certain. It is likely that article 6:162 cannot successfully be invoked against the AV-rental company, as an unlawful conduct or omission can likely not be construed on the basis of the facts of the case study. Whether or not the AV-rental company is to compensate victims on the basis of article 6:173 BW is very uncertain. That uncertainty can be related to the question whether or not the AV can be qualified as *defective* – which is for the victims to prove. Although I would argue that the *Betriebsgefahr* that is inherent to autonomous vehicles must bring about a low standard of defectiveness, and that the AV in question should be qualified *defective*, it will be difficult for victims to prove causality and damage, whereas there are ample defence-opportunities, as well as the – uncertain – possibility to "channel" liability to the producer. Although it cannot be excluded that the AV-rental company can be held liable under article 6:173, it will be complex for victims to be successful in a claim (see for a further analysis of their position section 6.3.4). Thus, regarding the Netherlands, little or no legal uncertainty results from article 185 WVW, more uncertainty is concerned with article 6:162 BW, and most uncertainty follows from the application of article 6:173 BW. The result thereof, is that it is likely that non-motorised victims of traffic accidents must be compensated by the AV-rental company, but that is not likely that any other victims can successfully hold the rental company liable.

Legal certainty in **France** can be considered very high. Any involvement in a traffic accident triggers liability of an AV-keeper (owner: i.e. the rental company), in the absence of a human driver. Damages can be easily calculated: all damages depicted in the case study are remunerable in principle, as no *faute inexcusable* is likely to be proved.

Although the **English** AEVA 2018 has just entered into force, it can already be observed that the mechanism it provides, entails some more uncertainty than the Dutch article 185 WVW and the French Loi Badinter. That is because the involvement of a vehicle is as such not sufficient to trigger liability of the insurer or AV-owner, but it rather is necessary to establish that an AV (at least partially) *caused* an accident. Comparable to the causality requirements under the Dutch article 6:162 BW and 6:173 BW, this necessitates technological expertise to be relied upon by the victims of AV-related traffic accidents. Furthermore, due to the "new" character of the AEVA, not much guidance is present regarding the scope of the defences and redress possibilities.

In sum, my assessment of the *legal certainty* that results from the regulatory frameworks on traffic liability shows a diverse picture: the French Loi Badinter provides a very high level of legal certainty for innovators, as does the Dutch article 185 WVW regime. The English AEVA 2018 has some inherent uncertainties, regarding the question whether or not an AV (partially) caused a traffic accident. Even more uncertainties follow from article 6:173 BW. It is rather unpredictable when AVs qualify as *defective goods* under this regime, and to what extent victims would be remunerable is also highly uncertain. Article 6:162 BW holds less uncertainties: it is unlikely (although not impossible) that AV-rental companies as the one in the case study are to remunerate victims of accidents.

6.3.3.2 STRINGENCY

A regulatory framework can be *stringent* when innovators must significantly adapt their behaviour as a result of new regulations, or when it is burdensome for newcomers to enter a – heavily regulated – market, as a result of high upfront compliance costs, as elaborated in section 3.4.2.3. Also regarding *stringency*, different observations can be made when looking into the three jurisdictions under review.

In **The Netherlands**, there are no relevant "new" rules (differently from England for example, in which the AEVA might become law anytime soon) which may introduce regulatory stringency. It can furthermore be observed that neither the regimes of article 185 WVW, article 6:162 BW nor of 6:173 BW present high upfront compliance costs for newcomers on the market. A proviso must be made regarding the latter regime, which is related to current *legal uncertainties*. If it would follow from future case law that an AV as depicted in the case study must be considered *defective*, and, moreover, that an AV-owner would be liable for defects that originated as a result of

automatic software-updates (which cannot be "channelled" towards producers as the defect would be deemed to have come into existence after purchase the AV-rental company purchased it), this will entail *stringency* for AV-owners. The owners are then made responsible for risks they cannot control nor influence, as the respective auto-updates as sketched in the facts of the case study, are made without any involvement of the car owner. However, as it stands, it will be very complex for victims to be successful in a 6:173-claim (and even more so in a 6:162-claim), where this would not only require "stretching" or at least novel interpretation of the definition of *defectiveness* under article 6:173 (and *unlawfulness* under article 6:162), but also regarding their proof-position. As further addressed in section 6.3.4, they have to prove *defectiveness* (or *unlawfulness* under article 6:162), *damage* and *causality*, as well as that the defect was not present at the time that the AV was put into commercial circulation, which points can only be underpinned after thorough analysis of the vehicle- and accident data, which in turn requires expertise that is not readily available for most victims. In summary, the current Dutch regulatory framework on traffic liability cannot be considered stringent for innovators.

The **French** Loi Badinter is neither new, nor entails high upfront compliance costs for newcomers on the AV-market. Therefore, the Loi Badinter cannot be considered stringent for innovators.

The **English** AEVA 2018 is, different from the regulatory frameworks of France and The Netherlands, brand new and implicates certain compliance costs for innovators who are to deploy AV's in their rental car fleet. AV-owners must for instance take out an insurance, in order to prevent liability for accidents caused by "their" AVs. This would not constitute "high" stringency. However, even when insured, there remain some liability risks for innovators, who for instance fail to perform safety-critical updates, contrary to what the insurance policy might hold in that regard, or who, contrary to the insurance policy, allows alterations to be made to the AV's steering software. This can be problematic in case of updates that are "pushed" to the vehicle, which cannot be prevented by the car owner (as depicted in the case study). That being stated, the costs to comply with these obligations, seem to be limited to me, although it will in fact depend on the insurance premiums, and the costs involved in "contract management" in order to prevent missing safety-critical updates, and in order to carefully scrutinise which software-alterations are allowed or not under the prevailing insurance policy.

In summary, the regimes of France and The Netherlands entail little or no *stringency*, whereas the English AEVA 2018 does require some compliance costs to be made, although these costs seem not to be very significant or burdensome.

6.3.3.3 *FLEXIBILITY*

As explained in section 3.4.2.4, *flexible* regulation may positively impact innovation. Two types of flexibility can be distinguished. Regulation can firstly be considered *flexible* when it provides innovators with multiple compliance paths (rather than to prescribe one, or a limited number of compliance paths). Secondly, regulation can be deemed *flexible* when it can be easily adapted to technological or societal change.

In **The Netherlands**, neither of the reviewed regimes specifies one, or a limited amount of routes to follow in order to comply with certain rules. Regarding adaptability of the norms to the introduction of AV's, the following can be observed. As article 185 WVW is formulated in an open and technology neutral way, AVs are in scope: the rules need not to be adapted in order to address this novel technology and are thus highly *flexible*. This holds also true for article 6:162 BW, i.e. it would apply to unlawful actions or omissions by an entity who instruct, or fails to prevent, an AV to cause damage. Article 6:162 BW can however not be applied to hold the case study's AV-rental company liable, as there can no action or omission be attributed to that entity which qualifies as unlawful – although this circumstance does not result therein that the regime of article 6:162 must be deemed inflexible. The regime of article 6:173 BW is also flexible, despite the current *uncertainties* concerning its scope and applicability. The norms are also formulated in a technology neutral way, be it that no clear answer can be derived from the applicable rules to the question whether or not the AV must be deemed *defective* for example. All in all, the regimes in The Netherlands entail a high level of flexibility.

Also in **France**, the rules of the Loi Badinter are not prescribing specific compliance routes to be followed by innovators. Furthermore, the Loi Badinter is formulated in a technology neutral way, and can be considered applicable to AVs as the one depicted in the case study. Thus, the Loi Badinter entails a high level of flexibility.

The **English** AEVA 2018 is, differently from the Dutch and French regimes, formally technology specific, in that it applies only to automated vehicles ("designed or adapted to be capable, in at least some circumstances or situations, of safely driving themselves") that are listed by the government, and only when they are in "self-driving mode". This definition is however broad, and encompasses virtually all AVs with a SAE-level 4 or higher. In fact, it will apply to any fully autonomous vehicle as the one illustrated in the case study. The AEVA-rules are sufficiently adaptable to several types of AVs beyond a certain level of autonomy. Below that level, the AEVA-rules have no significance for innovators. Furthermore, the AEVA-2018 does require that innovators comply with certain norms, i.e. that they take out the necessary insurance, and that they refrain from activities that are prohibited in the insurance policies, such as non-implementation of safety-critical updates, and preventing certain adaptations of the steering

software. Innovators are however left free in deciding *how* to comply with these norms, as for instance no specific insurance model is prescribed. Also, it is for the innovators to decide how to comply with the respective insurance policies.

In summary, the French and Dutch traffic liability regimes are entirely technology neutral, and flexible enough to address and apportion damages that may result from AV-related traffic accidents. Under these regimes, there are no specific compliance obligations for innovators. Despite the fact that the AEVA 2018 *is* technology-specific, it can stated to be sufficiently applicable to AV-related accidents, where the vehicles in question are at least designed and/or capable to drive themselves, and listed by the Secretary of State. The compliance obligations that result from the AEVA 2018 for innovators, offer ample compliance paths to choose from.

6.3.4 THE CONSUMERS PERSPECTIVE

6.3.4.1 RISK

In section 3.4.3.2, it was observed that it may negatively impact the adoption of novel technology, when that technology – and the rules that apply thereto – results in *inter alia* financial risks for consumers.

Where the regulatory frameworks regarding traffic liability in **The Netherlands** seem not to be hindering innovation to a large extent, it holds certain negative implications for victims who seek compensation for damages resulting from AV-related accidents as the one depicted in the case study. The only "type" of victims who seem to be "easily" able to seek remuneration are non-motorised victims of accidents in which AVs are involved.[1648] Other victims, such as those inside the AV causing an accident, or passengers of other motorised vehicles involved in an accident will likely be unsuccessful in a claim based on article 6:162 BW. That is because there would likely be no unlawful act or omission that can be attributed to the AV-rental company. And even *if* an unlawful act can be proven, it will be complex – at least without help from a judge - to underpin a causal relationship between the unlawful act and the damage, as this requires expert knowledge for the interpretation of vehicle- and accident data. Victims will face similar complexities when seeking remuneration on the basis of article 6:173 BW, regarding proving *inter alia defectiveness, damages, causality* and (when necessary) the circumstance that the *defect originated after marketing* of the AV – all of which is impossible without thorough analysis of the vehicle- and accident data. Moreover, the *defect* notion under article 6:173 BW needs "lenient interpretation" by a judge in order to establish the AV-rental company's liability. At the same time, the AV-rental company can invoke several defences, including the defence of not having *objective knowledge* of the defect in question, and has the opportunity to redirect the claim to the producer of the AV. All

[1648] It must be noted that damage to the vehicle itself is however not remunerable under article 185 WVW.

in all, there is a realistic risk that victims inside the AV (or another motorised vehicle involved in the crash) cannot claim damages from the rental company under the current traffic liability regime in The Netherlands.

Under the **French** regime, risks for AV-passenger or passengers of other motor vehicles such as those under the Dutch regime, are absent. All victims can opt for damage compensation, which is only limited in very specific cases of *faute inexcusable*, or *own fault* of the victims.

The **English** AEVA implicates more uncertainty for victims seeking damage compensation than the French Loi Badinter and the Dutch article 185 WVW-regime, as *damages* and *causation* need to be proved by victims. Furthermore, presumptions of causation to aid victims in their proof-position are less likely made by English judges than when for instance compared to more "lenient" Dutch judges. Also, expert knowledge will be necessary interpret vehicle- and accident data, which is necessary to underpin compensation claims. However, the AEVA 2018 offers less risks of non-compensation than the Dutch regimes of article 6:162 and 6:173 BW regarding personal and property damages, which are likely compensated, even when the victim was a passenger of the AV that caused the accident. Put differently, the risk under the Dutch regimes that AV-passengers are not compensated is significantly smaller under the AEVA. However, it is likely that *contributory negligence* can lead to a reduction in the insurer's (or owner's) obligation to compensate damage that goes beyond the maximum reduction in The Netherlands.

In summary, victims of French AV-related traffic accidents have the best chances that their damages are easily compensated, and the risks of non-compensation (also in spite of the compensation- and recognition purposes of extra-contractual liability regulation)[1649] of AV-passengers is highest in The Netherlands. The AEVA 2018, article 6:162 BW and article 6:173 BW implicate uncertainties (entailing *inter alia* information asymmetries between innovators and consumers) for victims, and necessitate expert knowledge in order to successfully underpin a liability claim towards AV-innovators.

6.3.4.2 TRUST

Trust is an important factor for the acceptance of novel technology by consumers, as illustrated in section 3.4.3.3. Trust could *inter alia* regard the "reparative capacities" of the traffic liability frameworks when victims suffered damage following from an AV-related traffic accident.

As highlighted in the previous section, those victims "in scope" of article 185 WVW may trust that their damages as a result of an AV-related crash are compensated, at a minimum of 50%, when the AV-rental company is "legally blameworthy" of the crash. In the pre-AV-era, other damages

[1649] See section 4.1.2.

than those remunerable under the WVW, or damages of other victims than those addressed by the WVW – including passengers of the respective or other vehicles that were involved – could be claimed from a driver who committed an *unlawful act*. Those drivers are however no longer involved in the AV-era. Therefore, it will be hard to establish an unlawful action or omission by a "human" driver, which renders it unlikely that the damages and/or the victims that are outside the scope of article 185 WVW are remunerable. As a "last resort", AV-passengers who suffered damages, could try to claim remuneration from the AV-rental company on the basis of article 6:173, however – as illustrated in the previous sections – this will be uneasy, and is hardly ever applied in practice. It is thus likely, that these, other than non-motorised victims cannot trust that their damages can be remunerated under the current regime in The Netherlands. This may negatively impact trust in AV-technology, and could negatively impact adoption of AV-technology in the Dutch market.

Similar trust-issues are unlikely under the scope of the **French** Loi Badinter regarding the facts as presented in the case study. To the contrary: the French regime provides a very generous compensation mechanism, which I consider beneficial for the trust of citizens in AV-technology, and in their trust that if nonetheless damages occur as a result of an AV-related traffic accident, that the victims are compensated.

In **England**, victims of AV-related accidents to which the AEVA applies, are aided by a set of rules providing them the possibility to claim damages from insurers or owners of AVs that (wholly or partly) caused a traffic accident. It is however necessary that the AV in question is listed by the English government. Would that not be the case, the AEVA-rules do not apply, and victims are likely not to be compensated by vehicle owners. When the AEVA applies, it entails less certainty for victims than the French Loi Badinter, or the Dutch article 185 WVW, as it requires victims to prove such causation. However, when liability can be established, the "nature" of the victim (whether or not motorised, or being passenger of the AV itself) is not important; the AEVA does not differentiate between them as the Dutch rules do. Thus, *when* the AEVA 2018 applies, it will implicate less *trust* issues for some "types" of victims than those not addressed by the Dutch WVW, although the French Loi Badinter implicates a higher level of trust for AV-accident victims.

In summary, the Dutch regime entails significant *trust* issues for victims that are not in scope of the WVW – for instance AV-passengers as depicted in the case study. The English AEVA provides, when it will be applicable, a proof-hurdle as it must be established that the AV (partially) caused the accident. The French Loi Badinter entails the highest *trust* level of all regimes under review.

6.3.5 *CROSS-EXAMINATION*

The above review of traffic liability regulation in The Netherland, France and England shows a diverse picture. However, some general observations can be made here. Neither of the regimes seems to be of a very *stringent* nature, and all of them are *flexible* enough to address traffic accidents in which AVs are involved. The distribution of *risks* between innovators and consumers is what forms the biggest difference between the reviewed systems, or more specifically: the (un)certainties surrounding that distribution. The French framework is the clearest and offers most legal certainties for both innovators and victims: it is the vehicle owner or -keeper who is liable in almost every thinkable AV-related traffic accident. While this is also true when the Dutch WVW applies, the rules stemming from article 6:162 BW and even more so 6:173 BW are the least clear. A significant observation is that article 6:162 BW can likely *not* be used as a basis for a compensation claim by motorised victims of AV-accidents the same way as motorised victims of humanly driven vehicles could, as in many occasions there will be no *unlawful act* that can be attributed to a human driver. Even if it could, it will be difficult for victims to underpin *causality* and *damages*, as this requires the availability of data that are related to the accident, and the means to interpret these. Similar problems arise for victims who seek compensation under 6:173 BW, who have to prove *defectiveness*, *damages*, *causation*, and if applicable, that the defect originated after the commercial sale of the AV. This all implicates that it is highly uncertain whether or not motorised victims are to be compensated after an AV-crash happened, if not improbable. This means *de facto* that in The Netherlands, motorised victims of AV-related accidents have a very high *risk* that they will not be able to successfully claim damages from owners or keepers of AVs (or their insurers), where non-motorised victims could, and even where motorised victims of *non*-AV-related accidents often could.

That could in turn negatively impact *trust* in AV-technology by those who are to adopt it, in order for the deployment of AVs to be successful in The Netherlands. In England, it is more likely that both motorised *and* non-motorised victims can claim compensation for damages they suffer from an AV-accident, although they might face difficulties of a procedural nature. As victims have to prove that AVs (wholly or partly) caused an accident and the damages that result therefrom. This however does not entail such a significant risk for victims than the Dutch rules do, and shall form less *trust*-issues in my opinion.

6.4 PERSONAL DATA PROTECTION

6.4.1 SOLVING THE CASE

As illustrated in the previous sections, the traffic accident brought about several types of damage. Some of these damages are explicitly not remunerable under the traffic liability rules, as these qualify as "pure economic loss", or are of another immaterial nature. Under the GDPR, which is addressed in section 5.2, damages that can be related to improper personal data protection by a *controller* or a *processor* are however remunerable.[1650] Besides being liable (on the basis of civil, extra-contractual liability) those controllers or processors who were not complying with GDPR-rules can be furthermore subject to public enforcement, ultimately in the form of administrative fines. In the following sections, the question will be addressed if, and to what extent, the innovator, i.e. the producer of the AV of the case study – who can be also deemed *controller* in sense of the GDPR – can be held to compensate the damages of the crash-victims, and to what extent they can be subject to administrative fines. In order to answer that question, I address the ex-ante compliance obligations for the controller including lawfulness of the data processing; potential obligations to carry out Data Protection Impact Assessments; the obligation to implement adequate technical and organisational measures to protect personal data; privacy by design and privacy by default-principles; as well as international transfers of personal data (section 6.4.1.1). Responsive obligations including those to answer legitimate questions of data subjects, and to respond to a Personal Data Breach are evaluated in section 6.4.1.2. As it is necessary nor possible to evaluate *every* GDPR-compliance aspect in this case study, I have made some assumptions, i.e. that the other criteria of the GDPR (including for instance other accountability obligations including the upfront information duties)[1651] are duly complied with by the AV-producer.

Civil liability of the controller is addressed in section 6.4.1.3; public enforcement in the form of potential administrative fines is addressed in section 6.4.1.4. Thereafter, I evaluate the factors which may influence innovation that exist in the GDPR-framework for *innovators* in section 6.4.2; and for *consumers* in section 6.4.3. I conclude with a cross-examination in section 6.4.4.

[1650] References to legislation and literature are not repeated here, occasional reference is made to 'new' sources, which had not been used in the aforementioned section.
[1651] I chose to assume *inter alia* ex ante and ex post information duties, as these are very case- and actor-specific, whilst the evaluation in this part sees to compliance obligations that are more "generic" and related to the AV-technology under investigation.

6.4.1.1 *EX-ANTE COMPLIANCE*

Lawfulness

One of the core ex-ante compliance obligations for data controllers (i.e.: the AV producer) is to ensure and document the lawful grounds for the processing of personal data. In line with that obligation, it must also be documented for special category data that are being processed, which exception to the general processing prohibition applies. It can be derived from the facts of the case study, that the following personal data are being processed by the AV manufacturer (probably along with many other personal data):

1. Vehicle identification numbers;
2. Names and addresses of AV-passengers;
3. Details on driving behaviour of (in any case) the respective AV through the APRS, including its geolocation;
4. Insurance details of the AV-passengers and the bicyclists.
5. Nature of the injuries and recovery prognoses of the AV- passengers and the bicyclists;

The personal data listed above under 1, 2 and 4 can probably be qualified as "regular" personal data; the data (under 5) regarding injuries and recovery prognoses are *special category* data, as these reveal information regarding data subject's health. This will also hold true for details on driving behaviour (3), to the extent that geolocations are logged.

Although different answers to the lawful-basis question may be possible, it can be argued that vehicle identification numbers must be processed by the AV-producer to comply with the obligations under Regulation 2015/758 (eCall). The case does not illustrate why names and addresses of AV-passengers, and details on AV-driving behaviour are being processed by the AV-producer. However, it might for instance be that these data are processed on the basis of *consent* by the passengers, who for instance want to be able to personalise the AV's features (including for example seat position; internal climate; synchronisation with infotainment systems; either "sportive" or "smooth" driving behaviour of the car) and to remember these settings for each time they enter the car. Another option would be that processing of driving behaviour, names and addresses would happen in the *legitimate interest* of the AV-producer, for instance to be able to settle a later claim, or for judicial defence purposes. In that case, the legitimate interest of the producer must be weighed against – and prevail over – the privacy interests of the AV-passengers, and the results thereof must be documented as well. The latter also holds true for the processing of the insurance details of AV-passengers and bicyclists.

As it is in principle prohibited to process *special category data* regarding geolocations and health data of the AV-passengers and the bicyclists, it is necessary to determine which exception applies

in order to lift that prohibition. This could for instance be the exception to establish, exercise or to defend against a legal claim, or the *explicit consent* of the respective data subjects. I recall that regarding geolocation data, the EDPB (European Data Protection Board) in principle forbids continuous processing, unless "explicit, free, specific and informed" consent is given by the data subjects. The EDPB position could have problematic implications for the AV-producer who does not want to, or who cannot rely on "specific and informed consent" in order to be able to process geolocation data which may be helpful in defending himself against for instance a product liability claim, or a traffic liability claim in The Netherlands or England. As observed in section 6.3, it may in these jurisdictions be crucial for either a claimant or a defendant to have access to data regarding *inter alia* the specifics regarding geolocation and driving behaviour to either underpin a liability claim, or to base a defence upon respectively. Also in product liability cases, driving behaviour data – including geolocation – may be necessary to process in order for the victim to establish defectiveness and causality, or for the producer to underpin a defence. Should "specific informed consent" not be given by the AV-passengers or withdrawn, these data may not be (further) processed in that regard according to EDPB policy. Although EDPB-policy can in principle be overruled by a court when it would turn out to be inconsistent with the GDPR, it is likely that the EDPB and the local DPAs will base their enforcement practices upon that policy. This could thus leave the AV-producer in a difficult position: where current traffic- and product liability regulation do not *prescribe* the AV-producer to process and store APRS-data, he is implicitly required to, should he wish to be able to defend against a liability claim using such data, whereas at the same time he cannot, according to the EDPB policy, rely on the exception to the processing-prohibition that is provided for the "establishment, exercise or defence of legal claims" under the GDPR without being subject to potential enforcement measures by a DPA.

All in all, none of the (envisaged) data processing activities is *a priori* non-compliant under the GDPR, although certain upfront efforts are required to establish the respective lawful bases and, where it concerns *special category data*, the relevant exceptions to the general processing prohibition. Problems can arise for the AV-producer regarding the processing and storing of special category APRS-data for judicial proceedings purposes without specific and informed consent of the data subjects.

Data Privacy Impact Assessment

The case explains that an APRS (Accident Prevention and Registration System) is used, which allows for communication between the vehicle and other users of the infrastructure. It is likely that *inter alia* geolocation data are continuously exchanged between the vehicle and other infrastructure-users, which are processed in order to prevent accidents, and stored for the

unfortunate occasions that nonetheless accidents happened, in order to help determining crash-causes. This 'triggers' that a Data Privacy Impact Assessment (DPIA) needs to be carried out, as this implicates large scale processing of special category data (in sense of article 35(3) GDPR) outside the vehicle, which may result in a "high risk to the rights and freedoms of natural persons".

As highlighted in section 5.2.7.3, it is required that, in addition to the "regular" accountability obligations, the envisaged processing activities need to be thoroughly documented, which also shows that the controller has balanced the (legitimate) interests in the processing activities, i.e. the prevention of accidents, with the protection of the informational privacy of the data subjects, i.e. the AV-passengers and other road users, as well as the measures that are intended to minimise the privacy risks of those data subjects. When it shows from the DPIA that there are "high risks" for the privacy of data subjects, the competent DPA must be consulted *before* the processing activities (in this case: through the APRS) may take place.

The DPIA-obligations hold many "open norms", regarding for instance the question what exactly entails a "high risk to the rights and freedoms of natural persons", or which measures would appropriately minimise the indicated risks. Although there are many standards available in the market for carrying out DPIAs, there are no specific models or codes of conduct available for AVs/APRS, let alone that such models or codes are approved by the authorities – despite that adherence to such codes of conduct is indicated by the legislator as one of the "good practices" to help demonstrating GDPR compliance.

TOMs

The AV-producer furthermore has to implement appropriate Technical and Organisational Measures (TOMs) to ensure an appropriate level of data security. Besides the general measures proposed under article 32 GDPR, including *inter alia* pseudonymisation, the implementation of backup-and-restore procedures, the regular testing and improving the effectiveness of such TOMs, DPAs including the EDPB have suggested some principles for TOMs that are more specific for the AV industry. Although there are differences between the focal points of the different DPAs, there are overlaps between the suggested measures as well. These overlapping measures see for example to the encryption of the personal data generated by and processed through AVs as well as the media and (external) devices through which these data are communicated; hashing; authentication measures; data- and activity logging; separating the storage and communication of personal data from the storage of AV-operating software (where the EDPB and CNIL suggest a further separation of special category data), which must in turn be partitioned from the "infotainment" systems and -communication; and implementing a "safe mode" in case a vehicle is attacked. These measures must be based on a risk assessment, should be frequently evaluated,

updated and improved. Whereas these suggestions can be used as a general basis for implementing TOMs by AV-producers as sketched in the case study, it must be observed that there is no comprehensive set of TOMs readily available, and that none of the guidelines, or industry "best practices" has been officially accredited by the data protection authorities.

The facts of the case study illustrate "poor" security of the APRS at some point, which even resulted in personal data breaches with consequences of increasing severity within the three scenarios (see further section 6.4.1.2). This implicates that insufficient TOMs were implemented in order to protect the data security of the personal data of the AV-passengers and the bicyclists, especially where *special category data* were involved such as the health data of the victims. It can thus be assumed that the norms of article 32 were violated.

Privacy by design and privacy by default

Similar to the observations made regarding TOMs and DPIAs, the material obligations following from articles 25(1) and (2) GDPR, regarding privacy by design and privacy by default respectively, are vague. Let alone that the text of article 25(1) is rather incomprehensible, it is hard to establish when an AV-processor would have fulfilled his obligation to (as interpreted in section 5.2.7.2) to process as little personal data as necessary for the AV-software to operate, and when is has complied with his obligation to enable the software to operate using a minimum amount of personal data "by default". Fortunately, some guidance is provided through the EDPB recommendations, which amongst other things prescribe that "local" processing of personal data is to be preferred over sharing personal data outside an AV, and when processing outside the vehicle is nonetheless unavoidable, a minimum amount of personal data should be involved, preferably in aggregated form, rather than the raw personal data themselves. Although the facts of the case study do not indicate that the privacy by design and privacy by default principles are insufficiently observed, further guidance in the form of co-regulation – which has been announced and delegated by the GDPR will definitely be helpful for *controllers* in securing their ex-ante compliance, and thus the protection of informational privacy of AV-users.

International transfers

It is mentioned in the case that the AV uses software which is developed by a company that is based in the US. Furthermore, it is stated that the software developer has access to the personal data processed through the AV (including the APRS). This indicates that personal data of EU-citizens (i.e. *inter alia* the passengers and the bicyclists) are exported from the EU to the US, and that the US-importer has access to these data "in the clear", in order to maintain the software in good condition for the AV-producer and -users. It is likely that a controller-processor relationship

exists, where the AV-producer qualifies as *controller* and the software developer as *processor* under the GDPR. In the absence of a valid adequacy decision, and without indication that BCRs (Binding Corporate Rules) apply, the most likely "tool" to base the data export in sense of article 46 GDPR are EC model clauses. Since *Schrems II* however, it must be concluded that this practice would be intrinsically incompatible with the protection of the fundamental right to privacy of the EU-citizens, irrespective of the tool used to base the data export upon. Thus, the GDPR-norms are violated (by the AV-producer who is the *data controller* in sense of the GDPR) when the software developer remains able to access those personal data.

There are however ways to "legalise" the export of personal data by the AV-producer to the software developer for whom it is necessary to access the systems for maintenance purposes. That could for example be the case when personal data are strongly encrypted by the controller in such a way that the controller (or public authorities requesting access) cannot decrypt these. It is however questionable whether or not the software developer remains able to properly maintain the software: it can for instance be that a bug originates in the software as a result of its self-learning capacities, which messes up the (personal) data processed through the AV's systems, in which case it would be necessary for the developer to trace the error, which could hardly be possible without having access to the respective data. Pseudonymization, which is also indicated as a possible alternative for legalising personal data-export to the US, may lead to the same problems for the software developer: it is at least questionable whether or not he would be able to repair the software when he would only have access to aggregated, pseudonymised personal data, instead of the actual data themselves.

Summary

As illustrated, there are many obligations that the AV-producer must comply with, even before he may deploy his services. It seems likely that the necessary "lawful bases" for most of the intended data processing activities through the AV's systems can be found according to the facts of the case study. The storage of APRS-data for legal defence purposes is however problematic, when the AV-producer would not want to rely on the "specific and informed consent" by the data subjects, which the EDPB provides to be necessary in order to lift the prohibition to process special category data, such as geolocation data. Therewith, it seems that the EDPB has disqualified the specific provision in the GDPR, that the processing prohibition can be lifted for the establishment exercise or defence of legal claims. A comprehensive set of guiding principles that are either provided or accredited by the data protection authorities – for instance in the form of certification mechanisms or codes of conduct, is absent. Thus, uncertainties remain for the AV-processor to determine when he can be considered compliant with the obligation to implement adequate

TOMs, the proper observance of privacy by design and privacy by default principles, and even more so, the obligation to carry out a DPIA. The facts of the case study do however not indicate that the AV-producer did not comply with these obligations. The illustrated data-export to the software developer seems very problematic, as it is impossible at the moment that the intended access by the software developer to the personal data processed to the AV's systems can be brought in conformity with the current rules of the GDPR, as interpreted by the CJEU and the EDPB. Full ex ante compliance regarding the facts of the case study thus seems impossible as it stands.

6.4.1.2 RESPONSIVE COMPLIANCE

Responding to requests by data subjects

As introduced in section 5.2.6, data subjects ought to have "control" over their personal data processed by third parties. This implicates *inter alia* that controllers are to provide access to the personal data relating upon a request by a data subject; and that they have to facilitate data subject's rights to rectification and erasure; data portability; the right to object to certain forms of data processing, including profiling. Given the facts of the case study, at least two of these rights, i.e. the right to rectification (article 16 GDPR) and the right to erasure (article 17 GDPR) are problematic for the AV-producer. It is stated that the APRS uses blockchain technology for the storage of personal data that are kept in order to help establishing the causes of accidents, and to determine "what went wrong". The blockchain technology is used to prevent "manipulation" of accident data as much as possible. As sketched in section 5.2.6, data stored in a blockchain are shared among multiple participants (if not every participant) of that chain. When someone would, for whatever reason, want to alter the data that is stored in, and distributed through, that blockchain, it is necessary to do so in all copies that are distributed in that chain – which is virtually impossible. In a way, this is an accurate TOM, as the availability and integrity of the personal data stored in the respective blocks will be very high: should one block become corrupted, a backup is kept in the other links of the blockchain. At the same time, this property of blockchain technology forms a big problem for AV-controllers who have to adequately respond to specific data subject requests. Due to the nature of technology, it will namely be virtually impossible to erase or modify the personal data once stored in the blockchain. Thus, it will be hard if not impossible to satisfy data subject's right of erasure and/or rectification when using "regular" blockchain technology as sketched in the case study.

Responding to personal data breach(es)

The case indicates (at least) two potential *personal data breaches* in sense of article 33 GDPR. First there is the vulnerability in the operating system which could have led to a breach of

confidentiality of the personal data processed through the operating system. However, it is not sure whether or not this vulnerability has actually resulted in a breach of confidentiality. The AV-producer (the *controller*) needs to investigate whether or not the vulnerability amounted to a personal data breach – which cannot be derived from the facts of the case, and if so, respond accordingly in conformity with the GDPR (see further below) within 72 hours after the controller has become aware of the fact that there would have been a *personal data breach* indeed.

Secondly, it is given, that the APRS was poorly secured, leading to consequences with increasing gravity in three scenarios. In the first scenario, it is highlighted that vehicle identification numbers have been publicly exposed; the second scenario illustrates that also full names and addresses of the passengers were publicly accessible; and in the third scenario it is added that sensitive data regarding the nature of the injuries, recovery prognoses and insurance details of both AV-passengers and bicyclists were publicly available after the accident.

It can be observed that all three scenarios qualify as a *personal data breach* under article 33 GDPR, as the confidentiality of the personal data has been compromised. Besides, it can be concluded that the "poor security" of the APRS would be a violation of the obligation of the controller to implement adequate TOMs in sense of article 32 GDPR in itself, especially under the second and third scenario. The *personal data breach* must, in any of the three scenarios, be reported to the local DPA within 72 hours after the AV-producer had become aware of the breach in principle. The case does not indicate if and when the producer had become aware, however it follows from EDPB/WP29 guidelines (as elaborated in section 5.2.7.1) that a controller has to implement measures to establish immediately whether a breach has taken place. Although the case is not specific in this sense, failing to report a breach to the competent authority constitutes violation of article 32 GDPR. Furthermore, an occasions "where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (article 34), also data subjects have to be informed without undue delay. High risks may exist when a breach could lead to physical or (im)material damage, including identity theft or -fraud, discrimination, reputational damage or financial loss. This can be deemed to be the case when special category data are involved in the breach. This is in any way true for the third scenario, as the compromised data include information on injuries and recovery prognoses, which are "health data", and thus special category data. Furthermore, it is given that these data have been used to commit identity fraud: a malevolent third party used the data in order to claim remuneration from the insurance company as if he were a victim of the AV-accident. The first category does likely not result in a "high risk" in sense of article 34 GDPR, neither does the second scenario: vehicle identification numbers and names and addresses of AV-passengers are no special category data, and it is not likely that unauthorised use of these data could lead to damage of any significance. Thus, in any of the scenarios the

personal data breach must be reported to the DPA in conformity with article 33 GDPR, and in the third scenario, also data subjects have to be informed conform article 34 GDPR. When the DPA and, where necessary, data subjects are properly informed and remedial actions are taken the AV-producer complies with his notification obligations. Should he however fail to do so (in due time), he would violate article 33 respectively 34 GDPR.

Summary

The responsive compliance duties of the AV-producer as reviewed above on the basis of the facts of the case study, exist therein that they are to adequately respond to data subjects' requests. It will be problematic if not impossible to fulfil obligations regarding the right of erasure and of correction of personal data when applicable, given the blockchain technology that is used to process personal data (which is in turn used to ensure maximum availability and integrity of accident data). The public availability of personal data can be considered a *personal data breach* in all three scenario's, resulting in an obligation for the AV-producer to notify the competent DPA. Under the third scenario, also the respective data subjects whose data regarding injuries, recovery prognoses and insurance information were exposed, must be informed.

6.4.1.3 CIVIL LIABILITY

Article 82 GDPR provides that a controller or processor who infringes the norms of the GDPR, is to remunerate anyone who has suffered material or immaterial damage as a result thereof. Victims have to prove norm violation, damages and causation. As controllers and processors must be able, on the basis of the accountability principle, to demonstrate compliance with the norms, it will be rather easy for victims to underpin a norm violation in a damages claim. A presumption of fault is incorporated under article 83(3), aiding victims further in their proof position. The GDPR does not provide further guidance regarding the proof-position of victims regarding causation and damages, which implicates that national rules of the Member States apply. Hereafter, I address the likeliness of success of a compensation claim by the motorised and non-motorised victims of the AV-accident, regarding their damages that can be related to GDPR-infringement(s). Norm violation and potential defences, causation and damages are addressed in turn.

Norm violation and defences

It follows from the previous two sections, that the facts of the case study comprise several (potential) violations of the GDPR-norms by the AV-producer. The exchange of personal data between the EU-based AV-producer and the US-based software developer is observed to be in violation of article 46 GDPR; insufficient TOMs were implemented contrary to article 32 GDPR; and the (intrinsic) inability of the controller to fulfil data subject's requests of data erasure and rectification violates article 16 respectively 17 GDPR. When it would furthermore appear that the

AV-controller did not observe his obligations to notify the DPA and – as applicable in the third scenario – data subjects of a personal data breach (and to take remedial action), also article 33 and 34 GDPR are violated – although this cannot be established from the case study.

For the victims, it will suffice to make a motivated statement that the respective norms are violated by the AV-producer. He will be only then exempted from liability, if he can demonstrate that he is "not in any way responsible for the event giving rise to the damage".[1652] Regarding the exchange of personal data, it is unlikely that the AV-producer can successfully invoke this defence, as it is obvious that he uses the services of the US-based software developer in a way that is incompatible with the GDPR. Furthermore, regarding the lack of appropriate TOMs, it will be also hard if not impossible to demonstrate that the security obligations were fulfilled: would that have been the case, data breaches as those depicted in the case study should not have happened. It is only then likely that the AV-producer did not infringe the data subject's rights, if he is able to demonstrate that the right of rectification and erasure of personal data can effectively be exercised, which would implicate that substantial changes had to be made to the "standard" blockchain technology, which is unlikely given the facts of the case. When the AV-producer can illustrate that he has fulfilled his obligations to notify the DPA and (for the third scenario) the data subjects and taking remedial actions, he cannot be held responsible for infringement of articles 33 respectively 34 GDPR.

Thus, perhaps besides the data breach notification obligations, it is likely that the other norm violations can be established.

Causation and damages

It will be less easy for the victims to establish a causal relationship between the norm violations and the damage. However, victims could be aided in their proof position by the national courts. The standard for establishing causality would in every of the reviewed jurisdictions be formed by a but-for test. The GDPR furthermore sees to the compensation of material *and* immaterial damage – although without prejudice to Union or Member State law. Those local regulations thus have to be used to base a compensation claim upon. It must be noted that the civil damages that have been awarded are rather modest in individual cases, as has been illustrated in section 5.2.11.2: the highest amount that had been awarded (in The Netherlands) was € 1.500,-.

When applying these principles to the three scenario's, the following can be observed. In the **first** scenario, there has been a certain norm violation as insufficient TOMs led to the disclosure of vehicle identification numbers. However, the facts of the case do not indicate that any damage

[1652] Article 82(3) GDPR.

occurred at all, also due to the fact that these vehicle identification numbers may only indirectly identify data subjects.

In the **second** scenario, besides vehicle identification numbers, also full names and addresses of AV-passengers have been exposed. Although concrete indications of material damage do not follow from the case study, the AV-producer could perhaps be convicted to remunerate immaterial damages in accordance with case law in the Netherlands, as the exposure resulted in "permanent loss over control over personal data" regarding full names and addresses. The actual damage will however in my opinion be limited, and may be related to the annoyance that is caused by "unsolicited" commercial communication. It is not unthinkable that such (and other immaterial) damages are awarded under the regimes of France and The Netherlands – as these types of damages are in principle "in scope" of the applicable regimes,[1653] rather than in England. Furthermore, it seems unlikely that other typical forms of damage that are mentioned in the GDPR such as reputational harm, financial loss or identity fraud could occur as a result of the exposed names and addresses.

The **third** scenario more concretely indicates that the victims sustained material damage. The exposure of data regarding the injuries, recovery prognoses and insurance details have led to financial loss: a third party has illegitimately claimed compensation of hospital costs of one of the bicyclists, refraining the data subject from successfully claiming his hospital costs from the insurance company. This damage would not have occurred without the norm-violation of implementing insufficient TOMs by the *controller*, i.e. the AV-producer. It is likely that these damages have to be compensated – in all reviewed jurisdictions. Should comparable issues also occur for the other victims, these are to be remunerated by the AV-producer as well. Furthermore, the unlawful availability of the intimate special category data regarding the victim's injuries and recovery prognoses *might* have a negative impact on their reputation or otherwise harms the victims in their person, which may be held remunerable in France and The Netherlands. However, it will not be easy to quantify such immaterial damages, given the current absence of (European) standard case law. It is furthermore known that in the **third** scenario other forms of damage occurred: one of the AV-passengers was paralysed; another one broke some limbs; the AV sustained so much damage that is observed a "total loss"'; and the bicyclists all suffered personal damage – one of them must even miss a leg and can never work as a doctor in the future. The question if and to what extent these damages must be remunerated by the AV-controller, depends on the possible causal relationship with the infringement of the GDPR-norms. This is not likely.

[1653] See section 5.2.11.3 on allocation of liability, and damages to be awarded under the GDPR. The latter remains a matter of national regulation. Under the appliable rules of France and The Netherlands, immaterial damages as a result of privacy-infringement can in principle be remunerated, where this is likely impossible in England. See more specifically footnote 1614 on these topics.

Although the lack of adequate TOMs may have caused unlawful exposure of personal data, it is unlikely that the indicated occurrences of personal physical damage are related thereto.

The following table holds an overview of the possible damages that qualify for remuneration under a civil liability claim based on GDPR-infringement:

Cat.	Damage	Compensation	Remarks
1	Likely none	No	Unlikely that exposed vehicle identification numbers amount to any (im)material damage
2	Immaterial damage: likely resulting from permanent loss of control over personal data (full names and addresses)	Partially	Remunerable in France and The Netherlands – quantification is uncertain; Likely not remunerable in England
3	Material damage: financial loss as a result of unclaimable medical costs	Yes	Remuneration is likely in all jurisdictions
	Immaterial damage: likely resulting from permanent loss of control over "regular" ánd special category data (regarding injuries and recovery prognoses)	Partially	Remunerable in France and The Netherlands – quantification is uncertain; Likely not remunerable in England
3'	Material damage: total loss AV	No	Causal nexus between GDPR-infringement and this damage is not likely
	Material damage bicycles (need replacing)	No	Causal nexus between GDPR-infringement and this damage is not likely
	Personal damage AV passengers (hospital costs, spine injuries, partial paralysis, inability to work)	No	Causal nexus between GDPR-infringement and this damage is not likely
	Personal damage bicyclists (hospital costs, missing a leg, missed career opportunities)	No	Causal nexus between GDPR-infringement and this damage is not likely

Summary

It is likely that several GDPR infringements took place, which can presumably be proved easily by the data subjects. These infringements see to the inadequate implementation of TOMs; unlawful exchange of personal data between the EU-based controller (AV-producer) and the US-based processor (software developer); and the intrinsic inability of the controller to fulfil data subject's requests of data erasure and rectification. It is likely that the financial damages as sketched in the third scenario must be remunerated upon a claim in all three reviewed jurisdictions. Immaterial damages resulting from exposed personal data as illustrated in the second and third scenario

could be remunerable in France and The Netherlands, although the amounts of damages are not easy to quantify.

6.4.1.4 ADMINISTRATIVE SANCTIONS: PENALTIES

As elaborated in section 5.2.10, the GDPR equips data protection authorities with a strong arsenal of corrective measures. One of their powers, is to impose administrative fines upon controllers or processors who infringe the GDPR-norms. The DPAs do have a margin of appreciation regarding enforcement policy, and the eventual height of penalties, as long as these are "effective, proportionate and dissuasive". To date, the Dutch DPA is the only authority of the reviewed jurisdiction who has provided a more specific penalty policy, which it maintains until further guidance is given by the EDPB. As evaluated, the "penalty landscape" is very diverse: the imposed fines for comparable GDPR-infringements show a significant variation between, and even within the reviewed jurisdictions. The landscape is even *so* diverse, that it is hard to predict the height of the penalties that can be imposed for the norm violations of the controller, based on the facts of the case study. With these proviso's, I have therefore chosen to illustrate the maximum fines for the GDPR-infringements that likely result from the facts of the case study. These infringements include: implementation of insufficient TOMs under article 32 GDPR; the enduring employment of the US-based software developer contrary to the inability to provide adequate safeguards under article 46 GDPR; and the failure to effectively respond to data subjects who seek to exercise their rights of correction and erasure of their data under articles 16 and 17 GDPR. I thus assume that the AV-producer did comply with his obligations to ensure a lawful basis for his processing activities; the obligation to carry out a DPIA; and his obligations to notify the DPA of a personal data breach in the first and second scenario, and also the data subjects of the third scenario.

The GDPR differentiates between two fining-categories. Article 82(4) lists GDPR-infringements that can be fined with a maximum of € 10 million, or 2% of the worldwide annual turnover (WAT) in the preceding year – whichever is higher, which I indicate below as the "low category". Article 83(5) lists "high category" infringements which can be fined with a maximum of € 20 million, or 4% WAT – whichever is higher.[1654] It must be noted that an infringement listed under the low category of article 83(4) can shift to the high category fines of article 83(5) for several reasons, including the negligence of the infringer, or the gravity of the infringement.

The norm-infringements of the case study, can thus amount to the following fines. The lack of sufficient TOMs can in principle be sanctioned with fines of the low category. Such fines may however "change colours" in the third scenario on the basis of the provisions in article 83(2(d &

[1654] See section 5.2.10 for a (high level) overview of the fines actually being issued by the DPAs, and furthermore http://www.enforcementtracker.com. It must be noted that the fines are often (if not always) higher than the civil damages that have been awarded so far (see also section 5.2.11.2).

g) GDPR, as the exposed personal data there include special category data, rather than the "regular" personal data that are compromised within the first and second scenario. The infringement of article 46 GDPR, regarding appropriate safeguards for the export of personal data to, in this case, the US, is punishable with a high-category fine. Also the failure to allow data subjects to exercise their rights under article 16 and 17 GDPR can amount to a fine of the highest category.

The table below illustrates the maximum fines as follows, which – for the sake of completeness – also contains the maximum fines for non-compliance with the norms regarding lawfulness, DPIA's, privacy by design and privacy by default:

Infringement	**GDPR art.**	**Maximum fine**	**GDPR art.**
Insufficient TOMs, scenario 1 & 2	32	€ 10.000.000 / 2% WAT	83(4)(a)
Insufficient TOMs, scenario 3, involving special category data	32	€ 20.000.000 / 4% WAT	83(2)(d&g)
Inappropriate safeguards for personal data export to the US	46	€ 20.000.000 / 4% WAT	83(5)(c)
Inability to effectuate data subjects' rights of rectification	16	€ 20.000.000 / 4% WAT	83(5)(b)
Inability to effectuate data subjects' rights of erasure	17	€ 20.000.000 / 4% WAT	83(5)(b)
Other categories:			
No lawful basis for processing/prohibition to process special category data	9	€ 20.000.000 / 4% WAT	83(5)(a)
Failure to carry out a DPIA, or to consult the DPA before processing	35	€ 10.000.000 / 2% WAT	83(4)(a)
Failure to implement privacy by design and/or privacy by default principles	25	€ 10.000.000 / 2% WAT	83(4)(a)

6.4.2 THE INNOVATORS PERSPECTIVE

6.4.2.1 LEGAL CERTAINTY

As stated in section 3.4.2.2, material legal uncertainty can have a negative impact on investments in innovation. Uncertainty may occur when it is difficult or impossible for innovators to reasonably foresee and to calculate risks that may result from, in this regard, the regulatory framework on personal data protection.

The GDPR, which forms the cornerstone of the regulatory framework on personal data protection, deliberately contains many open norms, and avoids to be technology specific as much as possible and flexible to technological change, as illustrated in section 5.2.7.4. The European legislator however chose to enable the drafting of technology- or sector specific rules, in order to overcome

the problems regarding legal certainty for regulatees that may result from the open and often vague norms. It is envisaged that more dedicated, clear rules for specific technology or sectors through codes of conduct, certification mechanisms, seals and/or marks can bring the necessary clarity, and thus certainty regarding the material contents of the norms. Furthermore, also DPA-policy is in practice used to "fill in" some of the open ends of the GDPD. However, to date there are as little as 3 codes of conduct approved, and no certification mechanisms, seals or marks that provide any further guidance for the AV-producer as described in the case study. Moreover, the EDPB-guidance is not sufficiently specific to enable the AV-producer to establish with certainty when he would be in compliance with his GDPR-obligations, or not.

As illustrated in the previous sections, it is for the AV-producer hard to establish *inter alia* when there is sufficient lawful basis for processing personal data; whether or not he can legally rely on the provision that lifts the prohibition to process special category data for legal proceedings purposes; when the TOMs to secure the personal data he processes, can be deemed appropriate; whether or not a "high risk" for the privacy of AV-passengers results from the envisaged processing activities and the DPA must therefore be consulted; and whether or not sufficient privacy by design and privacy by default measures have been taken. Regarding these subjects – amongst many others, it is thus not easy to predict whether or not the data processing activities are in compliance with the GDPR or not, and to what extent the AV-producer risks administrative enforcement, which can amount to € 20 million or 4% of his WAT, or a civil liability claim by a data subject – although the financial risks related to civil liability claims are insignificant, given the current case law.

As it stands, it can easily be established on the facts of the case study *that* the AV-producer is not in compliance of certain GDPR-obligations, regarding for example the exchange of personal data with a processor located in the US; the implemented TOMs; and data subjects' rights. Although the maximum height of penalties that can be imposed on him clearly follow from the GDPR, the amounts thereof that are actually likely cannot easily be calculated, as, apart from the Dutch DPA policy, further guidance is not provided yet by the European or the local authorities.

In sum, the relatively new GDPR-framework does implicate *considerable legal uncertainties* for innovators such as the AV-producer in the case study. Some of these uncertainties may decrease over time, as codes of conduct and/or certification mechanisms might eventually be accredited, or when further useful guidance is provided by the DPAs. Until further clarity follows from such measures – or from European case law in that respect, legal uncertainty remains (with questionable consequences for the GDPR's purpose to stimulate the free flow of personal data

within the Union),[1655] as it will be hard for controllers and processors to assess their (in)compliance with the GDPR-norms while the respective civil liability- and public enforcement risks are serious but also uncertain.

6.4.2.2 STRINGENCY

Regulation can be considered *stringent* when innovators must significantly adapt their behaviour as a result of new rules, or when it is burdensome for newcomers to enter a – heavily regulated – market, as a result of high upfront compliance costs, as I elaborated in section 3.4.2.3.

From its introduction in 2018, the GDPR has formed a set of rules that, also as a result of the hefty enforcement measures, can be considered burdensome for those who are to process personal data such as AV-producers: large upfront investments are needed in order to carefully address the norms of the GDPR – and therewith the informational privacy of citizens. The GDPR-objectives are clear and sound, as they see to the protection of the fundamental right of informational privacy of citizens (which is further elaborated in the light of the case study in section 6.4.3), the material norms and corresponding duties for organisations who seek to lawfully process personal data are however not. The ex-ante compliance obligations, including those addressed in the case study above (regarding *inter alia* establishing lawful bases for processing; implementation of appropriate TOMs; carrying out DPIAs; and implementing privacy by design and -by default) cost time and money even before data processing activities may be commenced, while it can often not be ensured that all obligations are duly complied with as a result of rules that are insufficiently clear, which is elaborated in the previous section.

Besides the aforementioned lack of clarity regarding some of the norms, others prove to be a moving target. The *Schrems II*-case law (and the *Schrems I*-decision beforehand), effectively at once prohibited certain international data processing activities that have been common practice for a long time. Many forms of personal data processing using the services of providers that are located in the United States are deemed incompatible with the GDPR, as the informational privacy of EU-citizens cannot be sufficiently guaranteed. While the importance of adequate personal data protection cannot be underestimated, the result of the *Schrems II*-decision is that controllers such as the AV-producer are left with an acute problem: he urgently has to replace his software developer by one based in a jurisdiction within the EEA, or a jurisdiction which provides adequate safeguards in sense of the Regulation. In the situation his "third-country processor" *can* be replaced in order to reach compliance, migration of services and personal data implicates among other things that more time and money needs to be invested by the AV-producer. Should it *not* be possible to migrate the data processing activities to another service provider (which might be the

[1655] See section 5.2.2.

case when the original provider has a de facto technology-monopoly for instance), this may in the worst case disable the AV-producer to further deploy his products and services, or result in a large enforcement- and liability risk should he choose not to comply with the norms. Besides the effective prohibition of certain third-country-based services, the GDPR furthermore prohibits certain forms of blockchain technology, where for example data subjects' rights cannot be effectuated. Also here, the underlying rationale that data subjects must be able to "control" personal data is important, be it that it *does* confront innovators with a challenge: technology needs to be adapted in order to become GDPR-compliant. Meanwhile, the AV-processor cannot use the technology without enforcement risks, and must invest in complying alternatives.

All in all, regarding the case study and the rules of the GDPR that apply thereto, the GDPR-framework can be considered *stringent*, as much time and money must be invested in order to reach compliance against a set of norms that are often too open or vague, which must be done before data processing activities may be started. At the same time, certain services involving transatlantic personal data processing that have long been commonplace, have been invalidated by the CJEU, leaving innovators such as the AV-processor with no other option than to change their business processes – implicating more compliance costs and *stringency*. More *stringency* follows from the significant risks of public enforcement and (although less significant)[1656] civil liability when the (I recall: often open and vague) norms of the GDPR turn out not to be complied with.[1657]

6.4.2.3 FLEXIBILITY

As stated in section 3.4.2.4, *flexible* regulation can positively impact innovation. Two types of flexibility are distinguished in the aforementioned section. Regulation is *flexible* when it provides innovators with multiple compliance paths (rather than to prescribe one, or a limited number of compliance paths). Secondly, regulation is considered *flexible* when it can be easily adapted to technological or societal change.

The regulatory framework on personal data protection scores high on flexibility. Its norms are formulated in a technology neutral, and often open way, which can thus easily be adapted to technological and societal change. The envisaged system in which further material rules can be drafted through sector- or technology specific codes of conduct and/or certification mechanisms would in theory be a very useful tool for developing clear and certain rules within specific sectors.

[1656] Which may become "more significant" when collective actions will be increasingly used to claim damages, and when such (high) claims are eventually awarded).
[1657] Also here, it must be noted that this high stringency level might not lead to fulfilment of the GDPR purpose regarding the "free flow of personal data" within the Union, as introduced in section 5.2.2.

Alas, there are no codes of conduct or certification mechanisms in place yet for the AV-sector, with *uncertainty* and *stringency* as results, which is addressed in the previous sections.

The absence of prescriptive, overly specific rules furthermore leaves innovators such as the AV-producer with many different options for reaching GDPR-compliance. This is another indicator that the regulatory framework is rather flexible. This might change as a result of technology- and/or sector specific delegated regulation in the form of codes of conduct or certification mechanisms, but in the absence thereof, innovators are not limited in the paths they may choose to reach compliance – be it that the norms are currently too *uncertain* and *stringent* as observed above.

6.4.3 THE CONSUMERS PERSPECTIVE

6.4.3.1 RISK

In section 3.4.3.2, it was observed that it may negatively impact the adoption of novel technology, when that technology – and the rules that apply thereto – results in *inter alia* financial risks for citizens.

As observed, the GDPR brings data subjects whose rights are not duly observed by a controller or processor who infringes the norms of the Regulation in a good position to claim remuneration of damages they have suffered as a result thereof. As a result of the accountability-principle that applies to *controllers* such as the AV-producer of the case study, it will be relatively easy for a victim to establish that one or more of the GDPR-norms was infringed. It will be less easy to establish a causal relationship between the norm violation and the alleged damages, however the GDPR does not prohibit that a victim is aided through procedural means of *inter alia* assumptions.

Not only material, but also immaterial damages should in principle be remunerable. Nonetheless, it depends on respective applicable tort systems of the Member States which forms of immaterial harm are compensated. It is likely that claims regarding the compensation of pure economic loss for example are more easily awarded in France and The Netherlands than in England.

In sum, given the facts that causality and damages must be proven; procedural aids have not been incorporated under the GDPR; and the modest amount (and height) of damages that have actually been awarded, the *risk* for citizens that they will not be compensated, can be evaluated rather high.[1658] This high *risk*-evaluation can be reduced to some extent, as a result of the public enforcement measures that have been installed by the enactment of the Regulation. The public-enforcement threat, as well as the potential precedent that could result from the recently filed

[1658] This might change in the future, as collective actions under article 80 GDPR become more commonplace, and prove to be successful for data subjects.

collective claims against large personal data processing organisations, could in theory increase the compliance with the rules, and thus reduce the risks for data subjects as a result of non-compliance. However, as further elaborated in the following section, it is questionable what the actual "preventive" effects will be of those enforcement mechanisms. Therefore, I assess the *risk* to be *considerable*.

6.4.3.2 TRUST

Prevention and reparation of harm resulting from unjust processing of personal data lies at the core of the GDPR-norms. This would be reached by on the one hand enabling data subjects to have insight in, and to exercise control over their personal data that are processed by third parties, on whom strict obligations are bestowed to duly observe the informational privacy of these data subjects. On the other hand, reparation of harm should be reached by enabling data subjects to have the GDPR-norms enforced by either a public authority or by themselves through civil liability claims. These measures are aimed at creating trust in technology through which personal data are processed, which is in turn an important factor for the acceptance of a novel AV-technology by consumers, which is illustrated in section 3.4.3.3 and 5.2.2.

As follows from the case study, it can be observed that data subjects are equipped with certain tools to have the harm repaired which may follow from improper observance of the GDPR-norms by for instance an AV-producer, however the mechanism can be questioned. There are some procedural hurdles to be taken (for instance regarding the proof of causation and damages), and to date the amounts of (immaterial) damages that have been awarded, are rather low. Thus, it cannot be stated that data subjects may trust that whenever they suffer harm as a result of GDPR-infringement, their damage will be compensated.

Citizen's trust that GDPR-norms are taken into account may however to some extent be fuelled by the enforcement possibilities of the DPAs, as well as by collective claims addressed at non-complying actors. Whether or not data subjects may trust that their informational privacy is indeed properly observed by controllers and/or processors, depends *inter alia* on their willingness and ability to comply, and on the enforcement capacities of the data protection authorities. As observed in the previous sections, the GDPR currently holds many open and vague norms (regarding for instance lawfulness, DPIAs, TOMs, privacy by design principles et cetera), and some of these are in fact very hard to comply with (regarding for example international transfers, and data subjects' rights through blockchain-technology). This could result therein that controllers such as the AV-producer wrongfully assume that they are complying with the (open) GDPR-norms, as certainty regarding ex-ante compliance can hardly be established. This may even lead thereto that compliance is ignored by controllers or processors, or that they take the chance that they will not be 'caught' by the DPAs, or that they risk being held liable by data subjects. As

long as the respective norms remain open and not specified further (either through delegated regulation, DPA policy, or case law for instance), a risk remains that the norms are not fully complied with, whether or not deliberately, and that trust that informational privacy is duly observed by third parties would be unfounded.

6.4.4 CROSS-EXAMINATION

The operation of AVs will result in many forms of personal data processing by third parties such as AV-producers as depicted in the case study. Some of those processing activities are even the implication of the rules stemming from the current product- and traffic liability frameworks. The GDPR applies to all such data processing activities. The GDPR offers a framework of *flexible*, adaptable rules and principles. In fact, innovators are free to choose how to comply. However, many of the norms are *uncertain* as a result of the openness of the norms, whereas envisaged sub-regulation in the form of for instance codes of conduct, certification mechanisms, or even comprehensive guidelines by the data protection authorities are not yet in place. Although this may (and likely will) change over time, the current situation is one of much uncertainty regarding ex-ante compliance by controllers and processors. Furthermore, some transatlantic data processing activities which have long been commonplace have now been declared incompliant with the GDPR, and novel means of data processing through blockchain technology seem to be incompatible with the rights data subjects are endowed with under the GDPR. Non-compliance may result in *stringent* enforcement, either through administrative fines which can be imposed by the data protection authorities, or through (individual or collective) civil liability claims by data subjects. All in all, the current GDPR-norms can observed to be *too stringent* for innovators.

Data subjects are in theory equipped with good means to repair damage which they may suffer as a result of an infringement of GDPR-norms. However, data subjects do face significant procedural hurdles in order to be remunerated (immaterial) damages. which leads thereto that the damage *risks* are (unjustly) not allocated at those parties who do not comply. Yet, it cannot be concluded that citizens may *trust* that their informational privacy is duly observed by controllers or processors at all times, again mainly as a result of the uncertainties regarding the question when the GDPR-norms are adequately complied with, however the strong public enforcement measures could contribute to awareness by innovators to take due account of the rules.

6.5 SUMMARY AND FINAL CROSS-EXAMINATION

6.5.1 LEGAL CERTAINTY

The **product liability framework** holds several uncertainties for innovators, regarding the notions and establishment of *defectiveness*, *causation*, and the applicability of the *later existence* and *contributory negligence* defences, which will make it difficult to foresee and to calculate the

product liability risks for innovators given the facts of the case study. The respective **traffic liability frameworks** show a more diverse picture. A high level of legal certainty for innovators follows from the risk-liability rules of the French Loi Badinter, and the Dutch 185 WVW-regime. However, the English AEVA-2018 framework contains inherent uncertainties mainly regarding *causation*, and the Dutch regimes of article 6:162 respectively 6:173 BW hold uncertainties regarding the notion of *defective goods* (6:173), *unlawfulness* and *causation* (6:162). All in all, the studied traffic liability rules can however be observed to implicate less uncertainty that the product liability rules do, given the clarity that the Loi Badinter and article 185 WVW provide, whereas such clarity is not provided under any of the studied regimes in which the PLD-rules have been implemented. The **regulatory framework on personal data protection** implicates considerable uncertainties for innovators relative to the product liability- and traffic liability frameworks, as many of the GDPR-norms (regarding for example *lawfulness, TOMs, DPIAs, privacy by design and -by default*) are vague and open, which are insufficiently specified by delegated regulation, or through guidance by the data protection authorities, whereas the "penalties" for non-compliance are significant, as this may result in civil liability claims by data subjects, and administrative fines up to €20 million, or 4% of the worldwide annual turnover of a non-complying innovator.

6.5.2 STRINGENCY

The **product liability framework** cannot be considered stringent: no significant upfront compliance costs are required, and furthermore the actual liability risks for innovators are marginal, due to the processual risks that are to be borne by the victims who seek compensation. This is also true for the majority of the reviewed **traffic liability rules.** The French Loi Badinter is evaluated to be non-stringent, as are the Dutch 185 WVW and 6:162 BW-regimes. A slight exception is the Dutch article 6:173 BW regime, where an AV-owner (in his role as innovator) can be liable for an AV that can be considered defective, while he cannot control nor influence that defectiveness as a result of autonomous updates of the AV's software. Also the English AEVA entails some stringency, as "new" insurances must be taken out when the Act enters into force; and certain behaviour must be either employed, regarding the safety-critical updating of the AVs' software, or refrained from, such as the "illegitimate" alteration of the steering software. The **personal data protection framework** however, entails high stringency for innovators as much time and money must be invested in order to reach compliance against a set of norms that are often too open or vague, which must be done before data processing activities may commence. Furthermore, certain transatlantic data processing activities have been effectively prohibited in case law. As a result, innovators have to change their business processes if possible – implicating compliance costs and *stringency*. More *stringency* follows from the significant risks of public enforcement and civil liability when the norms of the GDPR turn out not to be complied with.

6.5.3 *FLEXIBILITY*

All of the reviewed regimes offer sufficient flexibility to adapt to technological and societal change, *inter alia* through the use of technology neutral norms, and leave the paths open for innovators to choose how to comply. It must be noted however, that within the English **traffic liability regime** the AEVA 2018 only applies to AVs from SAE-level 4 upwards, and has no significance for "less autonomous cars". However, the AEVA 2018 is sufficiently capable of addressing traffic liability regarding the facts of the case study.

6.5.4 *RISK*

The **product liability framework** currently entails risks for victims who seek compensation for damage caused by an AVs such as illustrated in the case study. It is very uncertain that they can successfully claim damages, as the onus of proof rests with them regarding *defectiveness, damages* and *causation*. Such proof cannot likely be produced without access to, and in-depth analysis of data and algorithms (or the logged decisions by that algorithms), which requires (expensive) expert knowledge. At the same time, defendants have ample opportunities for defence, and are likely better equipped to underpin their defence with technical evidence than victims would, regarding the aforementioned points. Beside this, it must be noted that damage to the AV itself does not have to be compensated by a liable producer. Furthermore, the case study illustrated that some forms of damage (i.e. pure economic loss) are not remunerable in the majority of the reviewed jurisdictions (The Netherlands and England) under the product liability framework. Similar observations can be made regarding the Dutch **traffic liability framework** that applies to damage compensation of the motorised victims in the case study (passengers of the AV), i.e. the regimes of article 6:162 and 6:173 BW. It will be uneasy for victims to prove an *unlawful act* by the AV-rental company (6:162) or *defectiveness* of the AV (6:173), *damage* and *causal nexus* between the (alleged) unlawful act and the damage, and (in 6:173 cases only) that the *defect originated after the AV was brought into circulation* without technical expertise. Non-motorised victims will likely have none, or significantly less of these problems, as the risk-liability regime of article 185 WVW in fact establishes that AV-owners or keepers (i.e. the rental company) are always liable after their vehicle was involved in an accident, and leads to the obligation to remunerate either at least 50% or 100% of the damages. Also under the French **traffic liability regime**, risks for victims in damage compensation matters are virtually absent. Under the English AEVA 2018-system, victims need to prove that *damages* following from an AV-accident were (at least partially) *caused* by an AV – which will require the availability of accident-related AV-data, and technological expertise which is necessary to interpret these. Although the English system does not differentiate between motorised and non-motorised victims (as the Dutch system does), it must be noted that *contributory negligence* could lead to a 100% reduction in the obligation for the AV-insurer or -owner to compensate damages. The **personal data protection framework**

does *risks* for victims who seek compensation of damages that may result from GDPR-infringement. As *controllers* and (to a smaller extent) *processors* under the GDPR have, under the accountability principle, 'active' duties to demonstrate compliance, it will be relatively easy for victims to prove non-compliance, which triggers liability of the non-complying actor. Victims still have to prove *causation* and *damages*. While GDPR does provide generous compensation possibilities, as immaterial damages are explicitly brought under its scope, it will however be uneasy for victims of non-complying controllers or processors to be remunerated on the basis of its provisions.

6.5.5 TRUST

With the advent of autonomous vehicles, the risks for citizens increase that potential damage suffered by them cannot be claimed easily – if at all – under the **product liability regime and traffic liability** rules of The Netherlands (i.e. 6:162 BW and 6:173 BW, which apply to motorised AV-related traffic accidents). This could negatively impact the trust in AV-technology. Contrarily, the **traffic liability regime** in place in France, as well as the Dutch article 185 WVW-regime that applies to non-motorised victims, and (to a slightly smaller extent) the English AEVA-2018 can be seen to positively impact trust, as these make it in fact easy for victims to successfully claim damages. On the basis of the **personal data protection regime**, victims of GDPR-infringements cannot fairly trust that they are able to successfully claim remuneration of (even immaterial) damages. Furthermore, the GDPR explicitly aims at increasing trust that data subjects are brought *in control* of their personal data, and that third parties who process such data duly observe the informational privacy of citizens. As a result of the uncertainty regarding the actual obligations that follow from the often very openly formulated GDPR-norms, and given the current lack of further guidance through delegated regulation or comprehensive DPA-policy, it is however questionable to what extent *controllers* and *processors* actually comply. It can be that regulatees wrongfully assume that they are complying with the respective norms, but it is also possible that, due to its complexity and uncertainty, compliance is ignored by controllers or processors, and/or that they take the chance that they will not be 'caught' by the DPAs, or that they risk being held liable by data subjects. This would negatively impact data subjects' trust that their informational privacy is sufficiently protected.

The table below illustrates these observations, for each of the reviewed regimes and for both the innovators- and the consumers perspective. I have added some colours and codes to the fields in the table as well, which are further explained in section 7.1.

Extra-contractual liability								Personal data protection			
Product liability				**Traffic liability**				**GDPR**			
Innovators		***Consumers***		***Innovators***		***Consumers***		***Innovators***		***Consumers***	
Leg. Cert. (2)	Uncertainties regarding defectiveness, causation, defences lead to difficult risk-calculations for innovators	Risk (1)	High risks that damages cannot successfully be claimed. Burdensome to prove *defect; damage; causality* for victims as availability of data and technological expertise is needed for interpretation thereof, while producers have ample defence opportunities. Furthermore: pure economic loss not remunerable in EN and NL; damage to AV not remunerable at all.	**Leg. Cert.**	NL 185 WVW: no significant uncertainties (4) NL 6:162 BW: considerable uncertainties (unlawful act, causation) (2) NL 6:173 BW: very many uncertainties (defective good, causation, channeling to producer) (1) FR Loi Badinter: no significant uncertainties (4) EN: less uncertainties (causation) (3)	**Risk**	NL 185 WVW: no significant risks (4) NL 6:162 BW: significant risks (proving unlawfulness, damage, causation) (1) NL 6:173 BW: significant risks (proving defectiveness, damage, causation; origination of the defect after market introduction) FR: no significant risks (4) EN: some risks (causation, damage) (2)	**Leg. cert. (2)**	Considerable legal uncertaintiy follows from open norms, including *inter alia* lawfulness, TOMs, DPIA, Privacy by design and privacy by default	Risk (2)	Significant risks for consumers (for whom it is uneasy to prove causation and damages), which is slightly lifted as a result of accountability principle and information duties

Stringency (4)	No stringency	Trust (1)	Increasing autonomy can lead to decreasing trust that damages resulting from AV-related accidents can successfully be claimed	**Stringency**	NL 185 WVW: no stringency (4)	**Trust**	NL: 185 WVW high chances of successful claims positively impacts trust (4)	**Stringency (1)**	High stringency: ex-ante compliance costs while certainty is low, and enforcement/liability risks are high. Prohibition of certain forms of transatlantic data processing and use of blockchain technology	Trust (2)	Aim of the GDPR is to increase trust; there will be a positive effect of compliance (under threat of administrative sanctions However: uncertain chances of successful claims negatively impacts trust. Furthermore: uncertainty regarding compliance for innovators could lead to false compliance assumptions; and/or in combination with complexity of the norms, to ignorance thereof.
					NL 6:162 BW: no stringency (4)		NL: 1:162 BW: Increasing autonomy can lead to decreasing trust that damages resulting from AV-related accidents can successfully be claimed (1)				
					NL 6:173 BW: some stringency (defective goods) (3)		NL: 6:173 BW: Increasing autonomy can lead to decreasing trust that damages resulting from AV-related accidents can successfully be claimed				
					FR Loi Badinter: no stringency (4)		FR: high chances of successful claims positively impacts trust (4)				
					En AEVA 2018: some stringency (insurance, contract management), although not very significant or burdensome (3)		EN: fair chances of successful claims positively impacts trust (3)				

Flex. (4)	High flexibility, open and technology neutral norms and absence of prescriptive compliance paths for innovators			**Flex.**	NL: High flexibility, open and technology neutral norms and absence of prescriptive compliance paths for innovators (4) FR: High flexibility, open and technology neutral norms and absence of prescriptive compliance paths for innovators (4) EN: High flexibility, open and technology neutral norms and absence of prescriptive compliance paths for innovators (4)			**Flex. (4)**	High flexibility, open and technology neutral norms and absence of prescriptive compliance paths for innovators		

6.5.6 *CROSS-EXAMINATION*

Some general observations can be distilled from the summaries above. As it seems, increasing autonomy in cars lead at the same time to problems in terms of legal certainty for innovators, and problems in terms of risk and trust for consumers. Regarding product liability for example, the fact that an AV can make the autonomous decision to perform an update to the steering software, brings about uncertainty regarding the question whether or a victim can successfully hold the AV-producer liable. For the victim, the circumstance that he needs to prove *defectiveness, damage* and *causation*, whereas defences such as *later existence*, *development risks* and *contributory negligence* can more easily be established by the producer implicates risk uncertainty: it may very well be that he cannot successfully hold the producer liable, in which case he risks that his damages are not remunerated. At the same time, regarding the uncertain answer to the question whether or not the AV he has marketed is *defective*; whether or not that defect *caused damage*; and whether or not he can be exonerated on the basis of one of the aforementioned *defences*, the producer cannot effectively calculate his liability risk – although he is in a better position than the victim, as he likely has more accident-related AV-data readily at his disposal than victims do, as well as the technical knowledge to interpret these. Similar mechanisms follow from the Dutch 6:162 BW and the 6:173 BW regimes: uncertainties regarding *unlawfulness, defectiveness, damage, causation*, and *defences* lead thereto that innovators cannot calculate liability risks, where at the same time the victims risk that their damage remains uncompensated. Inverse systematics can be observed from the French Loi Badinter and the Dutch 185 WVW-regimes: based on the facts of the case study, it can be easily foretold that the AV-rental company is liable for damage following from the traffic accident in which the AV is involved. At the same time, the victims to whom these regimes apply, do not risk that they are left empty handed. To the contrary, they may rightfully trust that (at least a large amount of) their damage is to be compensated by the innovator. To a slightly smaller extent, a comparable systematic can be observed to follow from the GDPR. A norm violation incurs liability of the norm violator towards a those who suffer damage therefrom. The accountability principle leads thereto that norm violations can easily be discovered. Whether or not victims may trust that their damage is compensated, depends on the question if they can prove causality between the norm violation and the damage – which is in fact the only uncertainty. This implicates that it will be well-calculable for non-complying innovators to estimate their liability risks, whereas at the same time victims may often trust that their damage can be compensated.

Another interesting relationship (or absence thereof) can be distilled from the case study between *flexibility* and *legal certainty*. Whereas one could assume that flexible norms leads to legal uncertainty, this does not consequently follow from the studied regimes. Where flexible, open, technology neutral norms do seem to induce uncertainty (for innovators) under the GDPR as well as the product liability framework, such correlations cannot be found in for example the Loi

Badinter, or the 6:185 WVW-regime. These regimes are thus both flexible enough to cope with technological developments, and still provide the necessary legal certainty (for both innovators and consumers). Other correlations cannot consistently be observed from the case study. However, it must be noted that the personal data protection regime sees to the creation of a *stringent* set of rules, in order to ensure maximum observance of, and compliance with the informational privacy rules, which are aimed at strong privacy protection. Whereas it might be expected that has the desired effects, a lack of material certainty regarding the "contents" of the norms could lead to the opposite: false compliance assumptions or even deliberate non-compliance, which in turn could negatively impact citizens' trust that their informational privacy is duly protected.

Chapter 7. CONCLUDING THE SECOND PART

7.1 INTRODUCTION

The research goal of this second part was to investigate to what extent the *factors* as introduced in section 3.4 can be identified in the regulatory frameworks under review, i.e. the harmonised product liability framework, and the non-harmonised traffic liability frameworks of The Netherlands, France and England, as well as the harmonised framework regarding personal data protection. With the assessment of these *factors*, conclusions can be drawn as to the question how the respective frameworks may correlate with innovation in the field of AVs, and acceptance thereof – and thus the uptake of the results of innovation. Answers to that question can in turn be used in the third part (Chapter 8 and Chapter 9). In that final part, recommendations will be made regarding the potential improvement in view of both the *innovators perspective* and the *consumer perspective*. As indicated in section 3.4, a balance must be found between the *factors* within both perspectives. Improving the *factors* within the *innovators perspective* would only be sensible when the *consumers perspective* is not overlooked: for sustainable growth and innovation in the field of AVs,[1659] it is necessary that both innovation is stimulated and that optimal conditions are created for acceptance – and uptake of the results thereof.[1660]

In the following sections, the factors identified in the reviewed frameworks are summarised, and are placed in each other's perspectives. In order to do so, I used the table included in section 6.5.6 as starting point. An overview of the *factors* is given in that table: for each reviewed regulatory framework it contains a high-level overview which is qualified with a score from 1 to 4. A "1" is the lowest score, a "4" is the highest score – which is further explained below. The "scored factors" are then plotted on a pentagonal grid. Clockwise, each of those grids depicts the scored factors *legal certainty, stringency, flexibility, risk* and *trust.* Each grid thus contains five points, which are connected in such a way that it constitutes a "web graph". A smaller web, where the plotted points are relatively close to the "core" of the web, represents a lower score than a wider web. The wider a web, the "better" its score of the *factors*, and conversely, the smaller a web, the more room for improvement of the individual factors.

As stated, the scores represent a spectrum varying from 1 to 4, and are based upon my observations in the corresponding paragraphs in section 6.5. When *legal certainty* is scored with a "1", this represents that the respective regulatory framework implicates (relatively) most uncertainty for innovators – and thus the highest hurdles for innovation, whereas a "4" implicates the "least" uncertainty – in which case innovation is likely not hindered from an "legal

[1659] As stated in section 3.2, these topics stand high on the EU (Innovation) agenda.
[1660] See also the Proposed AIR (as cited *inter alia* in section 3.2).

(un)certainty" perspective. A little less uncertainty is scored with a "3", and more, or considerable, uncertainty is indicated with a "2". Similarly, *stringency* can be scored in a range of "1" ("most stringency"); "2" ("considerable stringency"); "3" ("less stringency") and "4" ("least stringency") for innovators. *Flexibility* can in the same range be scored with "1" ("most inflexibility/least flexibility"); "2" ("considerable inflexibility"); "3" ("less flexibility") and "4" ("least inflexibility/most flexibility") for innovators. The *consumers perspective* is scored in a comparable way. *Risk* is scored between can "1" ("most risks"); "2" ("considerable risks"); "3" ("less risks") and "4" ("least risks") for consumers. *Trust* can be scored in a range of "1" ("least trust"); "2" ("considerable distrust"); "3" ("less trust") and "4" ("most trust") for consumers. This translates in the following overview:

Innovators perspective		
Legal certainty	1	Most uncertainty
	2	Considerable uncertainty
	3	Less uncertainty
	4	Least uncertainty / most certainty
Stringency	1	Most stringency
	2	Considerable stringency
	3	Less stringency
	4	Least stringency
Flexibility	1	Most inflexibility/least flexibility
	2	Considerable inflexibility
	3	Less flexibility
	4	Most flexibility/least inflexibility
Consumer perspective		
Risk	1	Most risks
	2	Considerable risks
	3	Less risks
	4	Least risks
Trust	1	Least trust
	2	Considerable distrust
	3	Less trust
	4	Most trust

A proviso is in order here. The presentation of the *factors* below is based on knowledge and expertise gained from this research, and does therefore *not* form an empirically justified modelling of "absolute" values. Within these constraints, the awarded scores contain the author's relative valuation of the respective factors. Where for instance "legal certainty" is scored "2" within the evaluation of the product liability framework (for *inter alia* uncertainties regarding defectiveness, causation and damages lead to difficult risk-calculations for innovators) even if someone else would score these factors not as a "2" and "4" but for example as a "1" and "3", this can still be meaningfully put in perspective with the same factor within the Dutch traffic liability framework, which scores "4" (for it contains no uncertainties for innovators). In principle, the

same applies to the *consumer perspectives*' score: where for example the English AEVA 2018 is awarded with a "3" for *trust* (as chances are fair that damages-claims are successful, which is positive for trust), it can be illustrated that the French Loi Badinter scores even better with a "4" (as this regime implicates high chances that damages-claims are successful).

Another proviso must be made regarding the motivations for the "calculation" of the scores. As stated, the scores represent a spectrum, varying from presenting "most" to "least" hurdles for innovation or acceptance. The extremes (1 versus 4) can be objectified better than the scores in between the extremes. In my scoring, I have again used a relative approach, although a "normative view" cannot be precluded. When taking *risk* for example, a "2" represents risks for consumers, although not so much risks as a "1", which "2" I indicate as *considerable*. A "3" still represents risks – and is not risk-free, yet these are of a *less considerable* nature. Also here, the scores are not intended to give an absolute evaluation of the factors, but may rather be useful to sketch the relative differences or similarities between the factors in the respective regulatory frameworks.

A third proviso is that the results addressed below, follow from my studies of the *factors* within the three indicated regulatory frameworks according to a case study. Although I believe, as elaborated in section 3.5, that this case study is relevant and holds many elements that will likely be typical for future development and deployment of AVs and the legal and regulatory questions related thereto, my results must first and foremost be viewed with that limitation in mind.

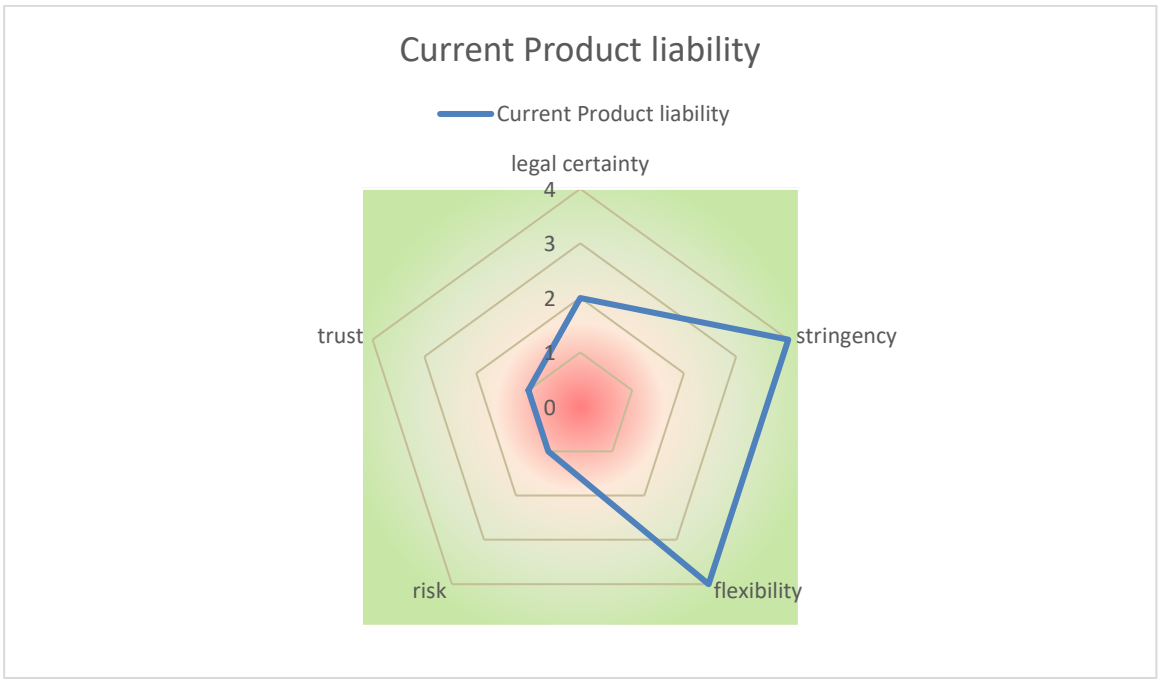
That being stated, the *factors* regarding the product liability framework are addressed in section 7.2; section 7.3 addresses traffic liability; and section 7.4 regards personal data protection. The final section contains summarised answers to the second research question of this study.

7.2 PRODUCT LIABILITY

In the foregoing Chapter, it was analysed to what extent the innovation-influencing *factors* can be identified within the regulatory framework regarding product liability, on the basis of the case study introduced in section 3.5. The *factors* within the *innovators perspective* were assessed in section 6.2.3; section 6.2.4 holds the assessment from the *consumers* perspective. These findings can, in conformity with the scoring method introduced above in section 7.1, be scored as follows:

Innovators perspective		Consumer perspective	
Legal certainty	2	Risk	1
Stringency	4	Trust	1
Flexibility	4		

When these scored *factors* are plotted in the web graph, this results in the following overview:



The graph and table illustrate that the current product liability regarding the *innovators perspective,* the factors *stringency* and *flexibility* have good scores (both a "4": least stringency and highest flexibility), but that *legal certainty* is problematic. This is mainly caused by uncertainties regarding the question when an AV-producer would (not) be liable for *defects* within AVs. It is for instance uncertain when a product must be considered *defective*, when the *causation*-requirements will be fulfilled, and to what extent a producer can rely on *defences* regarding

origination of the defect *after market introduction*; *development risks* and *contributory negligence*. Those uncertainties make it difficult to foresee and to calculate the product liability risks for innovators given the facts of the case study. However, considering the case study and as elaborated below, it is likely that the actual risk regarding bearing the damage eventually remains with the victim, for whom it will be difficult without procedural aids and technological expertise to have their damages remunerated. Therefore, *legal certainty* is considerable, and is scored "2".

Both the *consumer-perspective factors* score a poor "1" as well. The current framework implicates a high *risk* for (consumers as) victims of AV-related accidents that their damages cannot be successfully claimed from the producer of a defective AV(-component). In a procedure, victims will have to prove evidence of *defects*, *damage* and *causality*, which is hardly possible without procedural aids, proper access to AV-data and technological expertise. Compared to accidents with "traditional" non-autonomous vehicles, more specialised technological expertise is necessary, as this would require *inter alia* an in-depth analysis of the algorithms underlying the AV-software and the decisions made by these algorithms. Furthermore, not all damages that are suffered by victims as a result of the defective AV, are remunerable. At the same time, the necessary data and technological expertise are easier available for the defending producers. Furthermore, it is likely that producers could often successfully invoke a defence. *Trust* scores a "1", as the current product liability rules do not require AVs to be as safe as technically possible: it might be sufficient that AVs drive as safely as "average human drivers", rather than the "beyond excellent" driving skills that the (Dutch) traffic liability rules require for example. Furthermore, and closely related with *risk*, the *trust factor* is negatively implicated as it is unlikely that victims may trust that appliance of the PLD-rules results in a fair distribution of risks between producers and consumers. Conversely, as the complexity of AV-technology increases, the chance of fair risk-distribution between AV-producers and victims decreases, and not in favour of victims, for whom it will become harder to prove defectiveness, causation and damages, whereas the defences for producers remain easy to invoke.

A plausible side-effect of what has been observed to underly the meagre scores of *legal certainty, risk* and *trust*, namely the increasing need (for evidentiary purposes) for the gathering and storing data that may relate to AV-defects and -accidents, implicates *personal data protection* of AV-users. Those data, which are for instance needed to underpin a defectiveness claim, to establish a causal relationship or to invoke a defence, often identify a natural person, and therefore constitute personal data. How those data gathering and -scoring requirements affect the *factors* as encompassed in the regulatory framework on personal data processing, is illustrated further in section 7.4 .

Thus, the lack of *legal certainty* offers room for improvement, as in its current form, the product liability framework likely provides hurdles rather than stimuli for innovation. The level of *trust* will likely not be positively influenced by the currently applicable product liability rules either, as there is a significant *risk* that damages cannot be claimed from the only entity who can influence the occurrence thereof: the producers, who are at the same time not stimulated to make their products as safely as possible. The fact that *risk* and *trust* score a "1" could implicate lower level of acceptability of AV-technology than necessary.

In other words, there seems to be ample room for optimisation of those factors. In the following Chapter, concrete suggestions are made that see to improvement of *legal certainty*, *risk* and *trust*.

7.3 TRAFFIC LIABILITY

7.3.1 INTRODUCTION

The existence of the *factors* within non-harmonised traffic liability frameworks of The Netherlands, France and England have been investigated in sections 6.3.3 (*innovators perspective*)[1661] 6.3.4 (*consumers perspective*). In that respective order, the *factors* are visualised hereafter.

7.3.2 *THE NETHERLANDS*

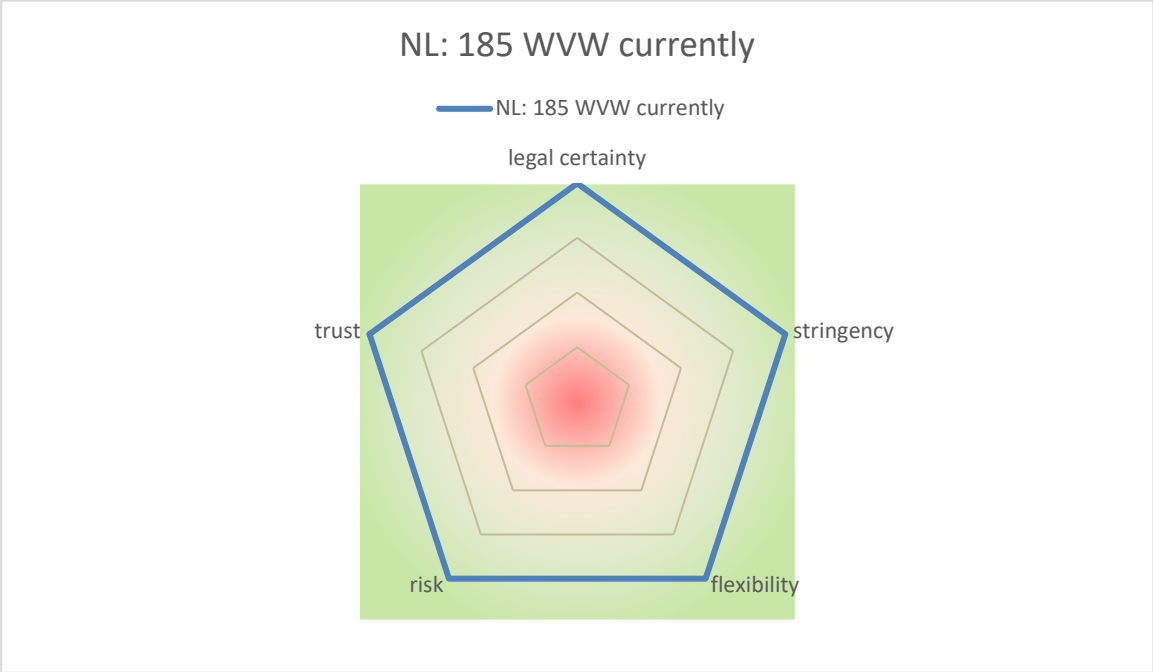
The extra-contractual liability framework that can be applied to AV-accidents as sketched in the case study, consists of three individual regimes, which are scored and analysed below, both in turn and in overview. Article 185 Wegenverkeerswet (WVW) can be applied to accidents between AVs and non-motorised victims. Motorised victims can (try to) claim damages from AV-owners or -keepers on the basis of article 6:162 Civil Code (Burgerlijk Wetboek, BW) – the generic fault-liability regime, or on the basis article 6:173 BW, a risk liability regime addressing the possessor of defective goods.

The *factors* within the article 185 WVW-regime are scored as follows:

Innovators perspective		Consumer perspective	
Legal certainty	4	Risk	4
Stringency	4	Trust	4
Flexibility	4		

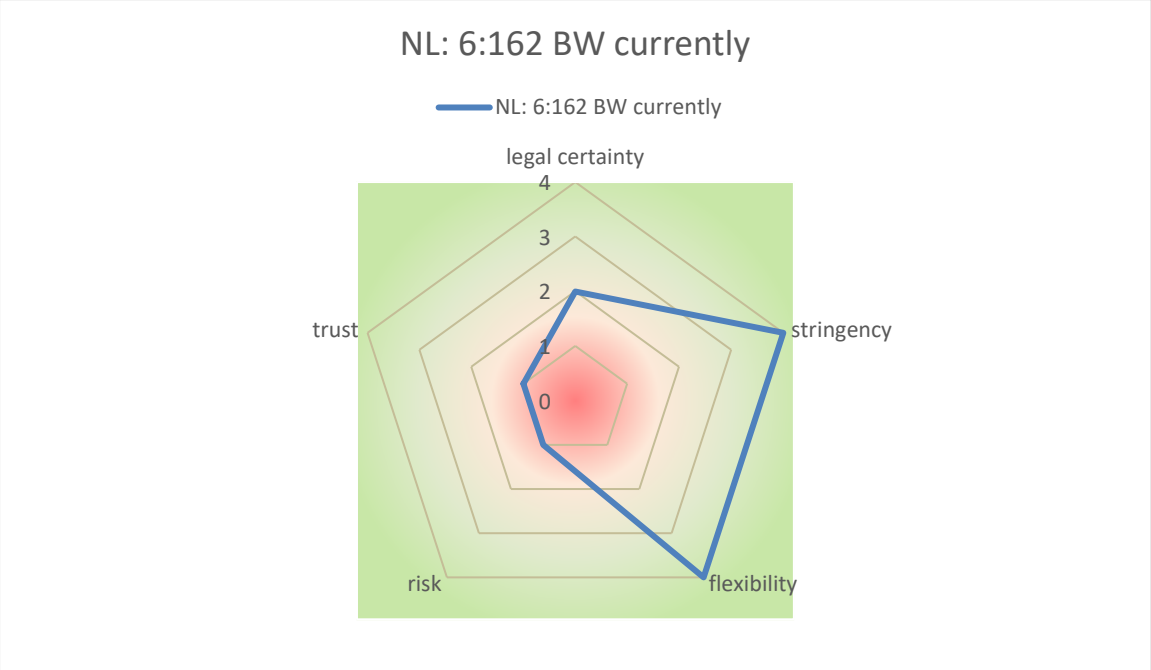
[1661] Please note that the *innovator* sketched in the case study regarding traffic liability is an AV-rental company. This "innovator" is thus of another nature that the *innovator* for the product liability- and the privacy-aspects.

These *factors* are hereafter visualised:



Within its scope, the article 185 WVW-regime scores top results. The only, yet significant, problem, is that the scope is limited to non-motorised victims. As will show hereafter, the means that are provided to motorised victims by the generic fault liability regime of 6:162 BW are of limited use in case of AV-related accidents:

Innovators perspective		Consumer perspective	
Legal certainty	2	Risk	1
Stringency	4	Trust	1
Flexibility	4		

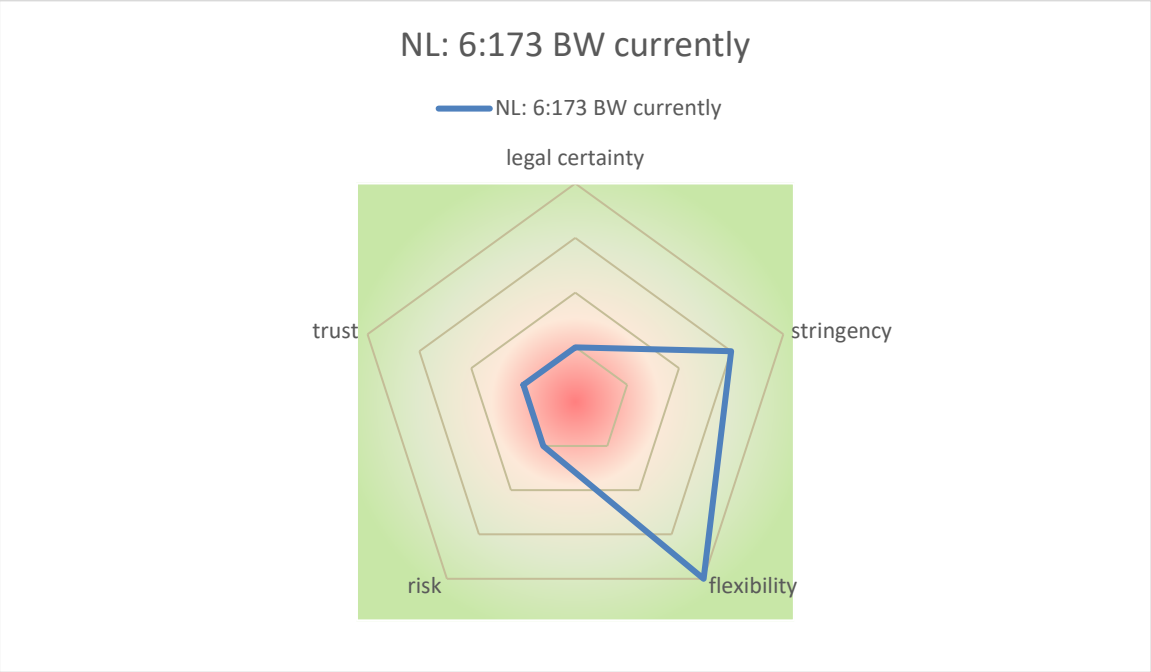


Regarding the *innovators perspective*, it can be observed that there is considerable *uncertainty* ("2") regarding the question under which circumstances innovators can be held liable by (other than motorised) victims of accidents in which AVs are involved, although it is *unlikely* that those innovators can be easily held liable. This is the result of the current rules regarding the establishment of *fault* and *causality*, required to establish liability, which will be hard to prove for victims.[1662] From the *consumers perspective*, there is a high *risk* connected to the foregoing observation that victims will not be successful in a claim directed at AV-innovators. Even if *fault* can be proven, it will be complex – at least without help from a judge - to underpin a causal relationship between the unlawful act and the damage, as this requires expert knowledge for the interpretation of vehicle- and accident data. This relates in turn also to personal data protection as discussed below in section 7.4. These *risks* in turn negatively impact *trust.* That *factor* is negatively implicated as it is highly unlikely that victims may trust that appliance of the 6:162-rules results in a fair distribution of risks between producers and consumers.

[1662] Stringency and flexibility are not considered problematic (see previous chapter), and therefore not further elaborated here.

My review of the third framework (6:173 BW) shows comparable results:

Innovators perspective		Consumer perspective	
Legal certainty	2	Risk	1
Stringency	3	Trust	1
Flexibility	4		



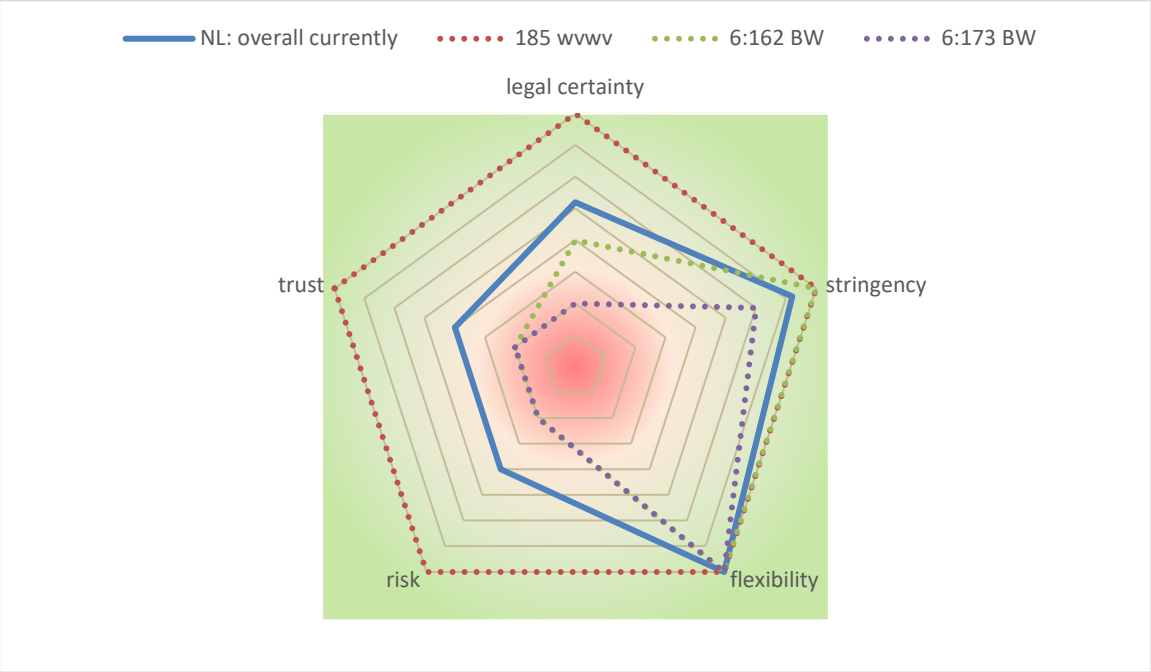
Viewed from the *innovators perspective,* the figures considerable *legal uncertainties* ("2"), comparable to the 6:162 BW-regime, albeit the uncertainties are of a slightly different nature. This is due *inter alia* due to the fact that under the 6:162 BW-regime the uncertainties regarding the parameters for establishing liability are even more uncertain than those under the 6:162 BW-regime, but that this eventually results in a(n even) slightly higher risk of non-remuneration for victims. Uncertain it is for instance when a *good* must be considered *defective* in order to trigger risk-liability for the possessor. Furthermore it is uncertain when the *causation*-requirements are met, and when liability can be *channelled* towards the producer of a certain defective good. When liability *can* however be established, and it is impossible for the innovator to divert the claim towards the producer, the 6:173-regime entails some *stringency* ("3"). In those cases, possessors are made responsible and liable for risks they cannot control or influence. The *consumers perspective* offers similar views as to the 6:162- and the PLD-regime: there is a significant *risk* that damages cannot be claimed under 6:173; establishment of liability would require thorough analysis of the vehicle- and accident data; in order to establish *defectiveness*, procedural aids are necessary, and defending innovators can rather easily invoke defences. This entails *inter alia* a

negative impact on *trust*, as well as yet another necessity for acquiring and storing many (personal) data, related to (potential) accidents and 6:173-claims (see further: section 7.4).

In the following table, the averages are calculated of the *factors* within the individual extra-contractual traffic liability regimes that can be applied to AV-related accidents:

Innovators perspective		Consumer perspective	
Legal certainty	2,6	Risk	2
Stringency	3,6	Trust	2
Flexibility	4		

In the following graph, both the individual scores as the calculated average (in blue) is depicted:



The graph illustrates that the most room for improvement of the *factors* thus regards *legal certainty*, *risk* and *trust*. This is comparable to the observations regarding the product liability framework, for similar reasons: *legal uncertainties* do both directly (i.e. from the *innovators perspective*) and indirectly (i.e. from the *consumer perspective*) influence innovation. In a direct sense, it is not certain when the criteria which are necessary for constituting liability can be deemed to be met, therefore it is difficult to calculate the liability risks for *innovators*. There are at the same time considerable *risks* for victims, on whom the onus of proof rests as regards the establishment of liability and damages. Increased autonomy causes increasing problems for victims to prove for instance *fault* (6:162), *defective goods* (6:173 BW), *defects* in *products* (PLD), causation and damages (all regimes). As the respective innovators potentially have better access to AV- (including the decisions made by the driving-algorithms) and accident data, and – even

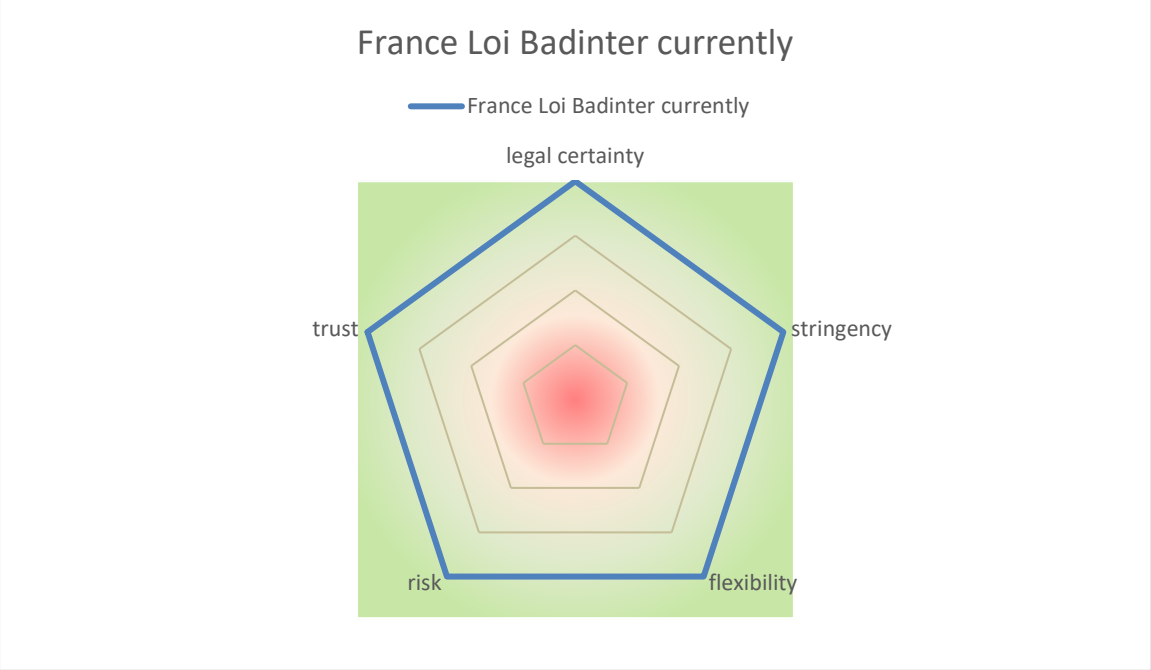
more importantly –interpretation possibilities thereof, they will be better equipped to underpin defences where applicable. Furthermore, it seems virtually impossible for victims to hold innovators liable on the basis of article 6:162 or 6:173 BW, leaving other than non-motorised victims of AV-related accidents in a pitiful position. This would negatively impact consumer's *trust* that victims of AV-related accidents (which happen beyond their control) are compensated in conformity with the objectives of the respective regulatory frameworks – which can be stated to negatively influence the uptake of AV-technology. The circumstance that the current liability rules in fact require massive (personal) data acquisition, storage and other forms of processing, negatively implicates *trust* as well, which is further illustrated below.

7.3.3 FRANCE

From both the *innovators* and the *consumers perspectives*, the French regulatory framework enshrined in the Loi Badinter holds the highest scores:

Innovators perspective		Consumer perspective	
Legal certainty	4	Risk	4
Stringency	4	Trust	4
Flexibility	4		

Which results in the "perfect" web graph:



It follows from my analysis in sections 6.3.3 and 6.3.4, that there are no hurdles in terms of *legal certainty*, as liability risks and damage remuneration obligations are well predictable; there is no *stringency* as the framework does not impose (new) upfront compliance costs for innovators; and

that the Loi Badinter is *flexible* in sense that it does not require that specific compliance-paths are followed, and is, as a result of its *technology neutral* approach, applicable to AV-related accidents in the same way as it applies to non-AV-related accidents. Furthermore, it does not impose (uncertain) liability *risks* on victims, which in turn positively impacts *trust*, as does the fact that the French framework does not necessitate (extra) data processing activities.

From these perspectives, there would not be any need for improvement to make the French extra-contractual liability framework more innovation-friendly. To the contrary: in the next Chapter, it will be evaluated whether the French regime could serve as a model for improvement of some of the other studied regulatory frameworks regarding traffic liability.

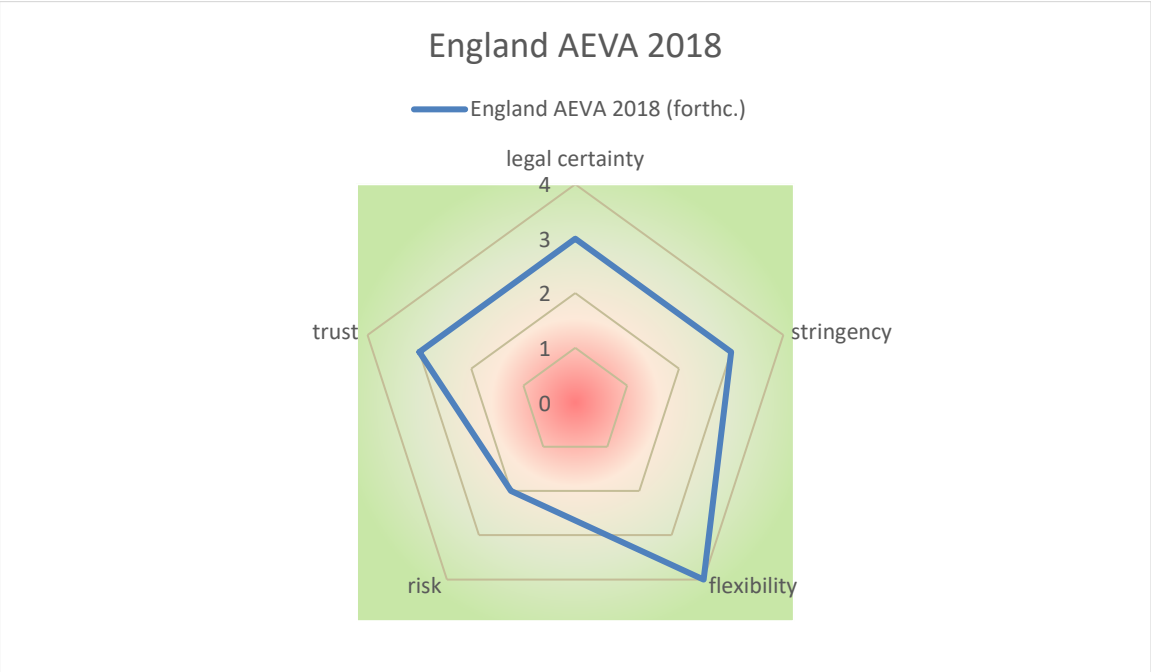
7.3.4 ENGLAND

The traditional English negligence rules that are applied in traffic liability cases, adhere to a *breach of a duty of care* of a *driver.*[1663] As sketched in the case, there is no human driver involved in the traffic accident. Thus, the negligence rules seem to be of no significance in this respect. However, the Automated and Electric Vehicles Act 2018 installs a regime that specifically applies to AV-related accidents.

The AEVA 2018 was also analysed in sections 6.3.3 and 6.3.4. The results thereof are depicted below. A proviso must be made: as the framework has only recently entered into force, it's functioning could not be studied: the textual arrangements of the rules as well as the explanatory memoranda and literature have been used to observe the *predicted* functioning,[1664] as follows:

Innovators perspective		Consumer perspective	
Legal certainty	3	Risk	2
Stringency	3	Trust	3
Flexibility	4		

[1663] See section 6.3.1.3.1.
[1664] Thus, an "extra" uncertainty must be observed regarding the AEVA 2018 compared to the other studied regimes. Where in the other regimes the "past performance" can be weighed in the assessment of the factors in light of a (fictive) case study, that is not the case for the AEVA 2018.



On the basis of the AEVA-rules, it is to a large extent predictable when an *innovator* can be held liable, although it holds a lower level of *legal certainty* ("3") than for instance the French Loi Badinter or the Dutch article 185 WVW-regime. That is because the involvement of a vehicle is as such not sufficient to trigger liability of the insurer or AV-owner, rather, it is necessary to establish that an AV (at least partially) *caused* an accident. Comparable to the causality requirements under the Dutch article 6:162 BW and 6:173 BW, this necessitates technological expertise to be relied upon by the victims of AV-related traffic accidents. *Stringency* is scored with a "3", as this new set of rules will likely require some compliance costs in the form of new insurance that innovators have to take out, and as it necessitates *innovators* to keep their AVs up to date by means of ensuring that for instance safety-critical updates are installed. However, these compliance costs do not seem to be very burdensome (when for instance compared to the GDPR-regime, see section 7.4 below), hence the "3"-scoring. *Flexibility* scores a "4": the AEVA-rules leave plenty options to reach compliance for innovators, and although the framework addresses technology from a certain level of autonomy onwards, it seems to be formulated sufficiently *technology neutral* to remain useful in the future.

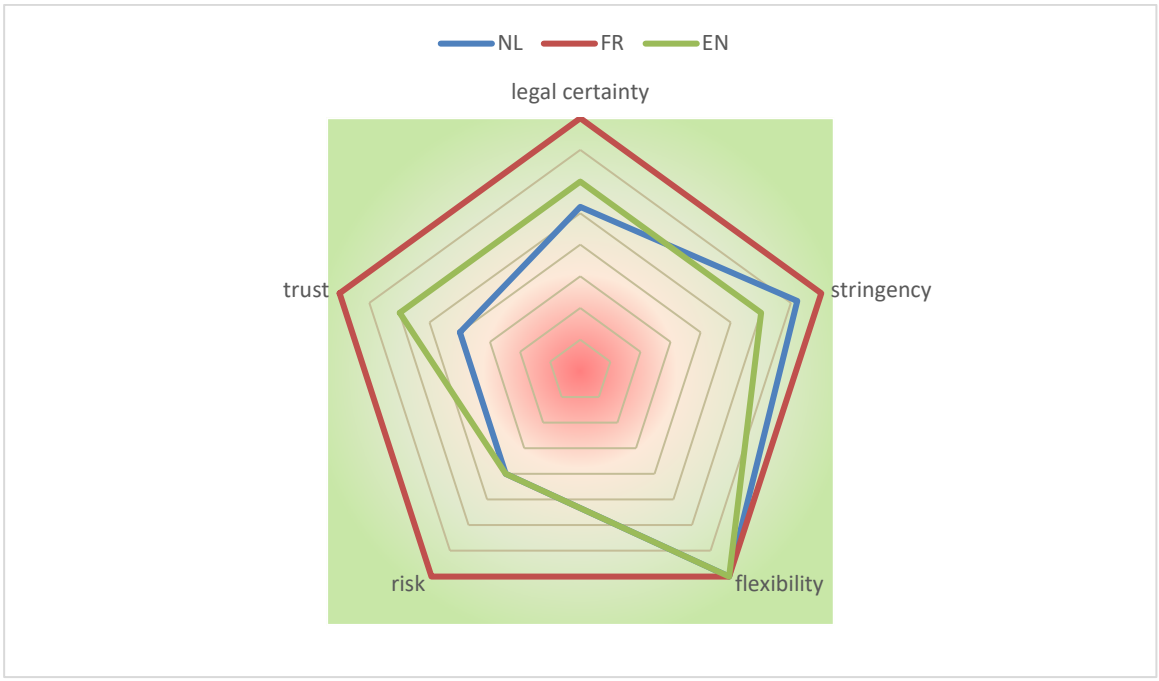
From a *consumers perspective*, it is observed that considerable *risks* ("2") remain for victims who seek compensation on the basis of the AEVA 2018. That is the consequence of the fact that victims have to prove *damages* and *causation*, which in turn needs to be underpinned with AV-data. This approach differs from for instance the French regime and the Dutch 185 WVW-regime (which both score a "4" on these aspects), and can be to a certain extent be compared with the Dutch 6:162 BW-approach, although, differently from 6:162, no *unlawful act* has to be proven. Until further guidance is provided by the English courts regarding for instance presumptions or

perhaps even reversal of the burden of proof (which is not very likely given actual case law), I assume that accident data must be acquired, and expert knowledge is required to interpret these data in order to establish causality Also in regards thereof, the level of *risk* for consumers is stated to be *considerable*. The AEVA-rules only apply to *listed* AVs. Partially, or non-listed AVs are exempted from its scope. When the AEVA *does* apply, it entails less certainty for victims than the French Loi Badinter, or the Dutch article 185 WVW, as it requires victims to prove such causation and damages. However, when liability can be established, the "nature" of the victim (whether or not motorised, or being passenger of the AV itself) is not important; the AEVA does not differentiate between them as the Dutch rules do. Thus, *when* the AEVA 2018 applies, it will implicate less *trust* issues for some "types" of victims than those not addressed by the Dutch WVW, although the French Loi Badinter implicates a higher level of trust for AV-accident victims. Therefore, the *trust*-level is scored with a "3".

Despite the fact that the functioning of AEVA 2018 is not yet in force, some points for improvement can already be observed, in view of "innovation-friendliness". Comparable with the comments regarding product liability, and the Dutch 6:162 and 6:173 BW regimes, *legal certainty* can be improved, as well as *risk* and *trust*, in order to reach a fairer balance between the innovators and consumers, which is in turn beneficial for innovation in general.

7.3.5 SUMMARY

The graph below shows a comparison of the *factors* within the evaluated traffic liability regimes:



Some general observations can be made from summarising the evaluations of the *factors* in the traffic liability frameworks above. The risk-based regimes as instituted by the French Loi Badinter

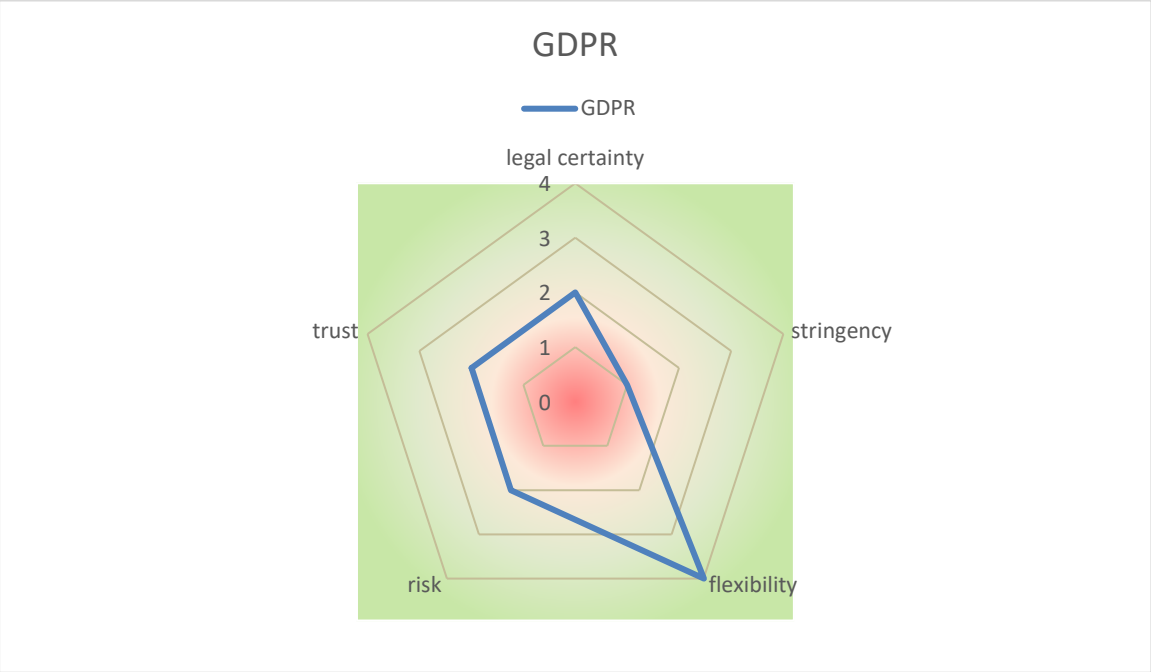
and the Dutch article 185 WVW-regime have the least need for improvement, as they are awarded the highest scores regarding all *factors*. In all other regimes (the Dutch 6:162 and 6:173 regime and the English AEVA 2018), *legal certainty* can be improved: under those regulatory frameworks it is (to varying extents) less easy to calculate liability risks for innovators. Legal uncertainty is also (very) problematic for *consumers*. Not only is it often unclear under which circumstances they can have the innovator's liability established, victim's chances of successful liability claims are poor, especially in The Netherlands (as stated: this *risk* is limited to motorised victims), and to a slightly smaller extent in England. This has a negative implication on the *trust*-scores, as the respective victims may not trust that damages which are related to AV-accidents are easily remunerated, if at all. Furthermore, under all reviewed regimes, except the Loi Badinter and article 185 WVW, the advent of autonomy in vehicles increases the necessity (both for innovators and consumers) to gather, to have access to, and to have means to interpret accident data, including AV-data, which will often include personal data. This also negatively impacts *trust*, related to the protection of the private life of consumers, which is further elaborated in section 7.4.

7.4 PERSONAL DATA PROTECTION

On the basis of the analysis of the regulatory framework regarding personal data protection (of which the GDPR forms the core element) in sections 6.4.2 and 6.4.3, the following observations can be made regarding the *factors*:

Innovators perspective		Consumer perspective	
Legal certainty	2	Risk	2
Stringency	1	Trust	2
Flexibility	4		

These scores are plotted in the web graph as follows:



The GDPR holds poor scores on all factors, except for *flexibility*. It is observed that insufficient *legal certainty* ("2") follows from the rules of the Regulation, as illustrated in the case study. In general, the many open norms of the GDPR, which do form a *technology neutral* and therefore *flexible* and *adaptable* framework, are considered too vague for AV-innovators. Where the European regulator envisaged to create more certainty through (endorsed) codes of conduct, certificates, seals and/or marks, it must be observed that there a very small amount of instruments of that kind (i.e. 3 codes of conduct) officially adopted to date. Further guidance which can be given by the competent data protection authorities (DPAs), is (too) scarce. This results therein, that it will be hard for an innovator to foresee when he is sufficiently complying with the rules regarding *inter alia* the establishment of sufficient lawful bases for processing personal data; whether or not he can legally rely on the provision that lifts the prohibition to process special category data for legal

proceedings purposes; when the Technical and Organisational Measures (TOMs) to secure the personal data he processes, can be deemed appropriate; whether or not a "high risk" for the privacy of AV-passengers results from the envisaged processing activities and the DPA must therefore be consulted; and whether or not sufficient privacy by design and privacy by default measures have been taken. In the same spirit, it must be observed that where extra-contractual liability frameworks such as the (reviewed) product liability rules, and the traffic liability rules of The Netherlands (excluding article 185 WVW) and England, *de facto* necessitate the acquisition, storage and (further) processing of AV-related personal data, it will be often hard if not impossible to bring such activities *de iure* in line with the GDPR-requirements. A similar observation regards the decentralised storage of AV-related data using "blockchain"-like solutions. While such forms of data storage can be beneficial for the development of AV-technology (and therewith the prevention of accidents) and to underpin potential liability claims or defences, these seem to be intrinsically incompatible with the GDPR-norms. Furthermore, it can be observed that the current data protection framework in fact prevents many forms of personal data-export to states as the U.S. that were formerly allowed, and that it will be uneasy to establish which forms of data-exchange between EU and non-EU countries can be considered "compliant". Given these uncertainties, and albeit some steps are taken to provide more clarity by the EDPB, *legal certainty* scores a "2".

Stringency scores a "1", as a result of the large upfront compliance costs for innovators and the corresponding compliance-*uncertainties*, as well as the hefty (mainly public) enforcement risks. As observed, it takes much effort to bring data processing activities in line with the GDPR-requirements. Where compliance is not – or cannot – be reached, innovators risk fines up to € 20 million or 4% of the worldwide annual turnover. This is not a "virtual" risk: high fines have already been imposed on non-complying actors.

Although the GDPR equips *consumers* with certain tools to enforce compliance, the enforceability thereof can be doubted. More specifically regarding *risk*, it will be hard for consumers to successfully hold a non-complying innovator liable, as a result of the fact that a data subject has to prove a *causal relationship* between norm-violation and *damage*, which will often be of an immaterial nature (which are excluded from compensation in England). Comparable to product liability and traffic liability rules (except the article 185 WVW-regime and the Loi Badinter), victims may have to rely on procedural aids such as assumptions of causation and/or damage. Furthermore, immaterial damage is not easily remunerable under the investigated regimes, and the amounts of compensation are rather modest. Thus, the *risk* that victims are not compensated for GDPR-infringements must be considered high. This high *risk*-evaluation can be reduced to some extent, as a result of the public (and collective private) enforcement measures indicated

above. The public-enforcement threat could in theory increase the compliance with the rules, and thus reduce the risks for data subjects as a result of non-compliance. However, also given the stated *uncertainties* and even the potential compliance-impossibilities, it is questionable what the actual "preventive" effects will be of those enforcement mechanisms. Therefore, I assess the *risk* to be *considerable* ("2").

Although the GDPR specifically aims at the creation of *trust*, it is not very likely that such *trust* of AV-consumers can be gained through the application of the current rules. As memorised above, *uncertainties* regarding the contents of the norms may not be beneficial for compliance, and thus the protection of the informational privacy of consumers. This could result therein that controllers such as the AV producers wrongfully assume that they are complying with the (open) GDPR-norms, as certainty regarding ex-ante compliance can hardly be established. This may even lead thereto that compliance is ignored by controllers or processors, or that they take the chance that they will not be 'caught' by the DPAs, or that they risk being held liable by data subjects. Furthermore, the enforceability by consumers seems to be limited, and therefore it must be doubted that victims can successfully claim damages from non-complying personal data controllers or -processors. All in all, *trust* is scored with a "2".

7.5 CONCLUSION

It follows from the foregoing sections that the *legal certainty, risk* and *trust* have the overall lowest scores, which suggests these *factors* should not be overlooked when seeking to improve the conditions for innovation and acceptance in the field of AVs.

Increased autonomy in vehicles leads to increasing *uncertainty* regarding the origination of damage, which is relevant to assess among other things *defectiveness* under the product liability regime and the Dutch regime regarding defective goods in possession, and to assess *fault* under the (generic) liability rules in The Netherlands and England. Also, as autonomy increases, it becomes harder to establish a causal relationship between a norm violation and damage, which is relevant in all studied regimes. Similar problems arise for innovators who want to rely on a (contributory negligence) defence. It is furthermore uncertain when compliance with the GDPR-norms can be established, as a result of the openness of these norms, and a lack of guidance.

Although the indicated *uncertainties* can be problematic for innovators in terms of risk-calculation, even more significant problems arise for *consumers*. Not only are AV-consumers confronted with the same uncertainties, it rather is "their problem" should they fail to establish *defectiveness*, *fault* or other *norm violations, damage* and *causality* between such norm-violations and damage: damages do not qualify for remuneration when liability cannot be established. Despite the fact that innovators, rather than consumers, can control, or ought to be controlling, the damage-inflicting potential that is inherent in AV-technology, the regulatory frameworks that were studied on the basis of the case study, make it, in their current form, uneasy to hold the respective innovators liable when such risks materialise. This would result in a high *risk* of unrecoverable damages for victims of AV-related accidents. Besides this, especially regarding the product liability framework, and the traffic liability frameworks of The Netherlands (with the exception of article 185 WVW) and England, it can be stated that in terms of *compensation, recognition* and *deterrence,* the studied frameworks do not optimally serve their purposes when applied to AV-related accidents.[1665] Moreover, when it is hard for victims to recover damages, this negatively impacts their *trust* in fair distribution of risks. The low *risk* and *trust* scores can be stated to negatively impact the acceptability of AV-technology, and therefore the uptake by consumers. In turn, this is also not beneficial from the *innovators perspective*, as technology-uptake is also crucial for successful innovation.

The other side of the coin, i.e. that despite *uncertainties,* innovators cannot be held liable easily (without procedural aids), is reflected in the observed absence of *stringency* in (most of the)

[1665] See section 4.1.2

studied frameworks. There are little (AEVA 2018) or no (the other regimes) upfront costs involved for innovators in order to comply with the extra-contractual liability norms.

It has furthermore been observed that in order to either underpin a liability claim *or* a defence thereto, acquisition, storage and other forms of processing of AV-data, including personal data, will be necessary, more specifically under the product liability regime, and the traffic liability regimes of The Netherlands (excluding 185 WVW) and England. This 'triggers' the applicability of the data protection framework.

The GDPR forms a high ex-ante compliance burden for innovators. Also because the open norms are often too unclear (*uncertainty*) and sometimes even prohibitive for AV-innovators, whilst non-compliance can be enforced through hefty administrative sanctions, this framework must be considered very *stringent*. The GDPR furthermore does not live up to its aim to create *trust*. As long as it is *uncertain* how AV-innovators can reach compliance, consumers cannot *trust* that their informational privacy is well protected. These uncertainties may have a similar impact on *risk*. *Risk* is furthermore negatively impacted due to the circumstance that it will be uneasy to hold a non-complying innovator liable on the basis of the GDPR-regime.

To end on three more positive notes: all studied regimes score well regarding *flexibility*; and both the French Loi Badinter and the Dutch 185 WVW-regime score full points on all the studied *factors.* This will be taken into account in the following parts. In Chapter 8 and Chapter 9, recommendations will be made that see to making the studied regulatory frameworks more innovation-friendly. The most important "output", i.e. the findings relating to the factors *legal certainty, risk* and *trust* will form the starting point of those recommendations. It will be investigated to what extent these *factors* can be optimised, also taking account of the other factors, in order to render the studied regulatory frameworks as innovation-friendly as possible.

PART THREE – RECOMMENDATIONS FOR IMPROVEMENT OF THE *FACTORS*

Chapter 8. IMPROVING THE FACTORS: WHAT TO IMPROVE?

8.1 INTRODUCTION

In the foregoing Chapter, I concluded that there is ample room for improvement within all three studied regulatory frameworks in order to better stimulate innovation and acceptance thereof in the field of Autonomous Vehicles. The goal of the following two Chapters, is to formulate recommendations in order to improve the *factors* – i.e. at least those with the lowest scores ("1" and "2") in a balanced way. This means that improvement of a factor should preferably not lead to the decrease of one or more other factors in such a way that it would be detrimental for innovation and acceptance – which I further elaborate below. Very briefly put, within the frameworks regarding product liability, traffic liability (as applicable in The Netherlands and England) and personal data protection, especially *legal certainty*¸ *risk* and *trust* deserve attention. Taking account of the factors with the lowest scores, it can be distilled from the previous Chapter that, in very general terms, situations in which victims (*consumers*) of AV-related accidents or improper personal data protection related to AV-deployment run the *risk* that they cannot (easily) claim damages from a producer or another deployer (*innovator*) should be minimised, in order to improve both the *risk* and the *trust* factors. Furthermore, and also from a general point of view, *legal certainty* for AV-innovators has to be improved as it will often be difficult to calculate their (financial) risks that may follow from the studied frameworks.

In the sections hereafter, it will be illustrated <u>which</u> points of improvement could be suggested from both the *innovators* and the *consumers* perspective. Section 8.2.2 regards product liability; section 8.2.3 regards traffic liability; and section 8.2.4 holds recommendations regarding the improvement of the regulatory framework on personal data protection. The question <u>how</u> such improvements could be regulated, against the background of the *better regulation* principles illustrated in section 3.3, is addressed in Chapter 9.

The following proviso is in order here. In my search for improvement-possibilities for the innovation-friendliness of the reviewed frameworks, at least the points above (and further below) could be addressed. I do not claim however that these are the *only* points to be optimised in those frameworks, nor that "fixing" these will necessarily result in a framework that is inherently and under all circumstances optimal for innovators and consumers of AV-technology: my recommendations are limited to the boundaries of the research I have conducted, the choices made therein and the methods I have followed.

A second proviso must be made. As illustrated in section 3.4.4 and later *inter alia* in section 6.5.6, there can be interplays between the *factors*. When one seeks to reduce liability *risks* for consumers in order to reach a fairer distribution between innovators and consumers, this could implicate increased *stringency* for innovators, as the latter could be confronted with "new" potential costs related to compliance, or to being held liable more easily. Improving *legal certainty* may also (positively or negatively) impact *risk* and *trust*, as it will become more clear what a certain norm would also implicate for consumers, and it may sometimes impact *stringency* when it is clarified to what extent certain (compliance) costs have to be made (or not). It will therefore likely not always be possible to reach "perfect web graphs" such as the one for instance illustrated in section 7.3.3. However, my aim is to reach improvement of all *factors* to the best possible extents, in a balanced way. Where, in a proposed situation, it is not possible to improve the scores of all of the individual *factors* at the same time, I will explain the choices made, against the background that in general terms, a proposed change should be "overall" stimulating rather than hindering innovation of AV-technology, and consumer-acceptance of the results thereof.

8.2 FACTORS TO BE IMPROVED

8.2.1 INTRODUCTION

In the following sections, I will indicate which *factors* would need to be improved, in order to optimise the respective regulatory frameworks in terms of stimulating innovation and acceptance. For each reviewed framework, the *factors* scored in Chapter 7 with a "1" or a "2" are – shortly – summarised,[1666] after which suggestions are made for improvement of these factors. The suggestions hereafter are used as "input" for the recommendations in sections Chapter 9, on how to implement the suggested changes.

8.2.2 PRODUCT LIABILITY

Within the product liability framework, *risk* and *trust* received with a "1" the lowest scores. *Legal certainty* was scored a "2".[1667] To start with *risk* and *trust*, it has been observed that there are several mechanisms within the regime that implicate a high *risk* for (consumers as) victims of AV-related accidents that their damages cannot be successfully claimed from the producer of a defective AV(-component). This is in turn may also negatively implicate *trust* in the reparative capacities of the product liability framework – hence the consumer uptake of AV-innovation. Furthermore, the fact that the current product liability rules do not require AVs to be as safe as technically possible, is not beneficial for consumer *trust* either. In order to improve *risk* and *trust*, it can from a general, perspective be suggested, that the product liability framework should

[1666] I refer to Chapter 7 and Chapter 6 for further elaborations.
[1667] See also Engelhard & De Bruin 2018, p. 78-83, where similar topics are addressed, which haven been taken into account as well here.

function such that victims of AV-related accidents may trust that the damage suffered as a result of defective AVs, is effectively remunerable by the producers, and thus that the risk significantly decreases that suffered damage cannot be claimed from the respective producers, resulting therein that the damages have to be borne by the victims. Taking a closer look at the elements within the product liability framework, improvement-recommendations are made hereafter.[1668] As stated above, I argue that victims of AV-related accidents should be effectively protected through the product liability rules. This implicates that the "burdens" for victims that have been indicated in the previous Chapter, should be eliminated as much as possible, which requires action by the European regulator. At the same time, it must be carefully observed that the elimination of such burdens would not implicate too high burdens for innovators. Although it is likely that several routes might lead to the desired improvements in terms of the *factors*, I suggest the following changes to the current rules:

1. The products definition should be adapted resulting therein that also software 'as such', thus irrespective of its relation with hardware, is brought under its scope. That would minimise the risk that a product liability claim is refused on the basis that defective software-components do not fall under the scope of the PLD. This change would be in line with original purpose of the directive to protect consumers from harm inflicted by products they acquire from producers.[1669] Doing so would be a logical next step in its development, given the fact that "embedded" software has already been brought under the scope,[1670] and taking account of the advice resulting from the PLD-evaluation,[1671] the subsequent recommendations from the Expert Group on Liability for Artificial Intelligence and other emerging digital technologies,[1672] as well as the report for the EP regarding Artificial Intelligence and Civil Liability,[1673] and the EP Proposal for a Regulation on a Civil liability regime for artificial intelligence;[1674]
2. It needs to be clarified which safety level may reasonably be expected regarding AVs, whereby it is recommended that "beyond excellent human driving skills" form the

[1668] It must be noted here that the recommendations above and below primarily see to "what" would need to be adapted; the question "how" these changes could be implemented is addressed in sections Chapter 9, 9.3 and 9.4.
[1669] See further section 4.2.2.1.
[1670] See section 4.2.2.2.
[1671] See European Commission 2018, p. 8-9:
[1672] See European Commission 2020, p. 43, where the Expert Group holds that "It is in line with the principle of functional equivalence […], that damage caused by digital content fulfils many of the functions tangible movable items used to fulfil when the PLD was drafted and passed".
[1673] See Bertolini 2020, p. 57.
[1674] European Parliament 2020a, consideration 8.

minimum threshold for determining defectiveness of an AV.[1675] This could facilitate underpinning an argument that an AV was defective, whereby connection is sought with the safety standard that is currently being used in the Dutch traffic liability regime.[1676] It could also be beneficial for consumer's trust regarding the safety of the vehicles.

3. Post-marketing obligations for AV-producers need to be introduced in order to keep AV (component)s safe after they have been sold (or otherwise made available) to consumers. This implicates *inter alia* that safety and (cyber)security updates should be provided for a certain period after an AV was marketed.[1677] This would lead to decreased risks that AVs inflict damage as a result of self-learning capacities or external (cybersecurity related, malicious) alterations of the steering software, and would contribute to the trust that AVs remain safe during that period.
4. In line with the post-marketing obligations to be introduced, the later-existence defence and the development risks defence should not apply in those cases where a producer did not comply with his post-marketing obligations.[1678] Whereas both Bertolini and the EG suggest that those defences should be excluded entirely, this might not be necessary in terms of *risk* and *trust* when the post-marketing obligations are regulated (which should render AVs to be as safe as possible during a certain period).[1679] Furthermore, producers must remain to be able to invoke a *contributory negligence* defence.
5. Introduce procedural aids for victims of (allegedly) defective AVs regarding defectiveness, and the causal relationship between defect and damage, from both a procedural and a material view. This will decrease the risk of non-compensation in case of AV-accident related harm, and increase the trust in the safety of the vehicles as well as the reparative capacities of the PLD-regime.

[1675] In its PLD-evaluation the European Commission (2018, p. 8-9) held that *inter alia* the notion of "defect" might need to be revised in view of recent technological developments. This is acknowledged by the Expert Group (European Commission 2020, p. 28), and Bertolini (2020, p. 57).
[1676] This safety-level has been advocated above in section 6.2.2.2.
[1677] This recommendation is also made by the Expert Group (European Commission 2020, p. 28). As illustrated in section 4.4.4 above, the EP (European Parliament 2020a) has made it a cornerstone of its Proposed regulation to bestow strict liability on a(n backend) operator in article 4 (for high-risk AI-systems – it is likely that AVs would qualify as such) and article 8 (for non-high-risk AI-systems). Be furthermore referred to section 4.2.2.3 and the considered parallels with the Consumer Sales Directive, which already obliges sellers of digital goods to provide updates for a certain period of time; as well as the EDPB, who observes that lifelong security-updates should be provided in their 01/2020 Guidelines; and the CCAV, who recommends the same in CCAV 2017, p. 17 (principle 6 and 8).
[1678] Ibidem, and see also the European Commission 2020, p. 43; Bertolini 2020, p. 58. Also the EG and Bertolini argue to exclude the applicability of the development risk defence in general (and implicate that the later existence defence should be excluded similarly). Also: Vellinga 2020, p. 158, 161, 230-231.
[1679] See also De Bruyne, Van Gool & Gils 2021, p. 388, who argue along similar lines.

a. Procedurally: relieve the burden of proof by regulating a (rebuttable) presumption of defectiveness when an AV is involved in an accident, and assume a (also rebuttable)[1680] causal relationship between defectiveness and damage.[1681]
b. In material sense: regulate logging-by-design obligations for AV (component) producers that enable the reconstruction of events (including automated decisions) prior to (and during) the accident,[1682] with the obligation to provide the logged information to victims. [1683] Failing to log, or to provide relevant, understandable, information should lead to reversal of the burden of proof regarding causation.[1684]

The implementation of the recommendations regarding *risk* and *trust* above, would at the same time be beneficial for *legal certainty*. These points correspond with the findings in section 6.2.3.1 that inter alia *defectiveness, causation* and the *defences* hold room for improvement in terms of legal certainty for innovators. Improving clarity for *consumers* could improve *legal certainty*, or put differently, would likely not lead to (even) less legal certainty.

Implementing the recommendations will implicate more *stringency* for innovators, although it is argued (see section 6.2.3.1) that the current PLD-framework is not stringent enough, as the adequacy of consumer (i.e. AV-victims) protection can be questioned when the current framework would be applied to facts comparable to those of the case study. *Stringency* would likely increase as a result of an extended range of *products* that would fall under the scope of the PLD; the higher safety level (which might in turn be the result of adaptation of the *defectiveness* criteria) to be regarded when putting AVs on the market; the suggested limitation of the *defences*; the *proof aids* and the new obligations regarding *logging by design*. When implemented, these recommendations

[1680] Rebuttable causal relationships may already be assumed by national courts, as was illustrated in section 4.2.2.6, although *reversing* the burden of proof is not allowed according to the *W/Sanofi* case law of the CJEU.
[1681] See European Commission 2020a, p. 20-22; European Commission 2020, p. 49-50; Bertolini 2020, p. 59.
[1682] As further elaborated in section 8.2.4, privacy-by-design has to be incorporated: as little personal data as possible should be processed, and such data should be stored as shortly as possible.
[1683] Both the EG (European Commission 2020, p. 47) and Bertolini (2020, p. 83) underscore the value of logged data. Logging obligations have however not been included in the EP Proposal. Logging-by-design has been incorporated in the Proposed AIR, see mainly Article 12.
[1684] The EG suggests that "[22] the absence of logged information or failure to give the victim reasonable access to the information should trigger a *rebuttable presumption* (emphasis added *RWdB*) that the condition of liability to be proven by the missing information is fulfilled" (European Commission 2020, p. 47). It could in my opinion be fair to *reverse* (thus in line with the 15th recommendation) the burden of proof in such cases, in which only the producer could possibly prove that it had *not* been the system (for which he was responsible) that caused the damage. See in a similar vein Bertolini 2020, p. 84. In line with Bertolini's observation there, I argue that the defendant not only has to provide access to the information, but that this information should be comprehensible, i.e. meaningful and useful for the victim in order to underpin his claim.

may induce higher compliance costs for "existing" innovators, and may also form a hurdle for innovators who would want to access the market. Also, the required improvements may seem to implicate structural changes to the currently applicable product liability rules. However, the expected (disruptive) technological changes might call for "large steps" in order to keep the rules aligned with innovative technology, in order to maintain their fit with the original purposes, including consumer protection and fostering innovation. Such steps have also been suggested by the European legislators, as indicated above. Moreover, should these recommendations or other regulatory changes with similar effects *not* be implemented, the factors *risk, trust* and *legal certainty* would likely not improve. In other words, increased *stringency* is likely necessary in order to improve those factors: doing nothing would result in under-protection of citizens who cannot effectively seek compensation for damages that cannot be attributed to them.[1685] Nonetheless, it must be noted that the recommendations above seek to maintain a balance in the risk-spreading between innovators and consumers, for instance by still allowing the invocation of defences including *contributory negligence*, by not categorically excluding the *development risk* and the *later existence* defence, and the non-absolute proof aids for victims in the form of *rebuttable* assumptions.

Furthermore, implementing these (or comparable) recommendations should lead to a better balance between the *consumer perspective* (by improving *risk* and *trust* the chances of "acceptable" innovative technology is likely to increase) and the *innovators perspective* (as stated, consumer acceptance is necessary for successful innovation, which was elaborated in sections 7.1 and 3.4). However, *logging by design* does entail processing of personal data, which holds an imminent risk for the protection of consumer privacy. Therefore, the personal data protection principles (specifically those regarding data minimisation, privacy by design, and the rules regarding TOMs, as well as the rights of data subjects) of the GDPR must carefully be observed.[1686]

Finally, it should be avoided that implementation leads to avoidable *stringency*,[1687] and that, from the innovators perspective, other factors are implicated where that can be avoided. As will be elaborated further in Chapter 9, material improvement of the said factors should not lead to decreasing *flexibility*: where possible, the improved rules should be adaptable to changes, technology-specificity should be avoided where possible, and innovators must be able to choose as much as possible how to comply with the adapted norms.

8.2.3 TRAFFIC LIABILITY

[1685] Which would implicate an exaggerated application of the principle that "the loss should lie where it falls".
[1686] See further section 8.2.4.
[1687] I.e. forms of stringency that would not see to the improvement of other factors.

Comparable with the product liability regime,[1688] the factors *risk, trust* (both score a "1" for the Dutch 6:162 and the 6:173 BW regimes, and a "2" for the English AEVA-regime) and *legal certainty* (scoring a "1"for the 6:173 BW-regime respectively a "2" for the 6:162 BW-regime) within the Dutch and English traffic liability rules can be improved. From the *consumer perspective*, it was observed that there are significant risks that victims cannot prove *fault* or a *defect* at the side of an AV-deployer, i.e. not without procedural aids, extensive in-depth data-analysis and very lenient interpretations of what may constitute a *fault* or a *defect*. Similar observations were made regarding the need to establishing a *causal relationship* between a norm-violation and damages. Therefore, being successful in a liability claim on the basis of the respective regimes was held to be uneasy, and sometimes hardly even possible. In order to improve *risk* and *trust*, I argue that traffic liability frameworks need to function in such a manner, that victims of AV-related accidents can trust that the damage suffered resulting from accidents in which AVs are involved, is effectively remunerable by those who deploy AVs on the road. Thus the risk needs to be significantly reduced that suffered damage cannot be claimed from the respective innovators (or other deployers). Taking a closer look at the elements within the traffic liability regimes, the following improvement-recommendations are made.[1689]

1. It should not be necessary for victims (irrespective of their "capacity" as driver, passenger or external (non)motorised victim) to prove fault or defect attributable to an AV deployer, in order to establish liability.[1690] The involvement of an AV in an accident should suffice to allocate liability of the deployer of the vehicle (i.e. for example its owner).[1691] This principle is derived from the *Loi Badinter* (see inter alia section 4.3.3.2) and an – albeit in adapted form – the Dutch article 185 WVW-regime(see section 4.3.2.1). This is aimed at reducing the risk for (motorised) victims of non-compensation as in many cases, fault cannot be proven and it will be very complex and costly to prove causation. Reducing *risk* is likely beneficial for *consumer trust* in the reparative capacities of the traffic liability regime.
2. In principle, 100% of the damages resulting from an accident in which an AV was involved should be remunerable, unless *force majeure* can be proven, which may in turn lead to a

[1688] See also Engelhard & De Bruin 2018, p. 78-83, where similar topics are addressed, which have been taken into account here as well.
[1689] It must be noted again that the recommendations above and below primarily see to "what" would need to be adapted; the question "how" these changes could be implemented is addressed in sections Chapter 9-9.4.
[1690] See *inter alia* section 6.3.4 and 7.3 above. See also the European Commission 2020, p. 16-17; and in similar vein Bertolini 2020, p. 108-111.
[1691] It would likely be compatible with the proposed EP provision (European Parliament 2020a) in Article 4(1). With Bertolini (2020 see *inter alia* p. 102-103), and along the same lines of the *Loi Badinter*- and the Article 185 WVW-regime, I argue that involvement must be sufficient in AV-related accidents to allocate liability.

reduction of damages to be remunerated.[1692] Force majeure may include gross negligence (including "inexcusable fault")[1693] at the side of the victim. Gross negligence could exist in situations in which the victim intentionally failed to install safety-critical updates, or where the victim modified the AV's software.[1694] This will contribute to decreasing risks of under-compensation of damage, and thus to trust in the reparative capacities of the regime, although without making an AV-deployer responsible and liable for damage for which solely the victim is to blame.

3. In order to underpin a potential force majeure defence, it may be necessary to acquire and analyse AV- and accident data, which must be available for the defending AV-deployer. Therefore, it should be regulated that logged information (which should be available due to the "logging-by-design" obligations to be introduced for producers, see the previous section) should be made available both to the defending AV-deployers, and to the victims who seek compensation.[1695]

Legal certainty will likely benefit from the suggested changes too, as foreseeability and calculability of the liability risks for innovators would improve compared to the current situation.

Moreover, it can be argued that increased *legal certainty* may be beneficial from an *innovators perspective*, even when this potentially leads to increased *stringency*.[1696] Furthermore, the proposed strictness of both the establishment of liability and the default apportionment of damages may be the most victim-friendly solution of *inter alia* the challenges regarding the

[1692] Given the *Betriebsgefahr* that will always be inherent in the deployment of AVs, it can be argued that the reduction should not exceed a certain percentage of the damages, for instance 50% (which is used in The Netherlands for victims over the age of 14. See section 4.3.2.3. Such a cap on the reduction would deviate from the proposed contributory negligence-defence enshrined in Article 10 of the EP Proposal (European Parliament 2020a), although it would be in line with current systematics under the Dutch (and the French) regimes.

[1693] Cf. the Loi Badinter, see section 4.3.3.3.

[1694] This mechanism can be compared to "contributory negligence" situations under the AEVA 2018, as illustrated *inter alia* in section 4.3.4.4.3. I would argue that damage that is caused by a third party who ought not to have access to the AV's system, but who still succeeded in hacking it, should be borne by the AV-deployer (who may have a product liability claim towards the producer) rather than by the victim, when the victim did not neglect his obligation to install safety-critical updates.

[1695] This would be in line with the system as proposed by the EP (European Parliament 2020a) in Article 10(2). The fact that such information should be available for victims furthermore follows from the rights of the data subjects, and the corresponding information duties for controllers under the GDPR (see *inter alia* section 5.2.6). The obligation to make such data available to defending AV-deployers does currently not follow from (traffic) liability regimes, and should be regulated in order to be in conformity with the obligation for *controllers* in sense of the GDPR to establish a lawful ground for personal data processing, as well as (to the extent applicable) the general prohibition to process special category data (see sections 5.2.4, and 5.2.5 above) and section 8.2.4 below.

[1696] See for example the Expert Group's observation that an alleged "chilling effect of tort law [on innovation, *RWdB*] is stronger as long as the question of liability is entirely unresolved and therefore unpredictable, whereas the introduction of a specific statutory solution at least more or less clearly delimits the risks and contributes to make them insurable". (European Commission 2020, p. 27).

establishment of unlawfulness, and proof-issues that were indicated to exist for consumers under application of the current fault liability regimes. Although "lighter" alternatives might be found, these suggested improvements likely have the best potential to better protect the interests of victims. These solutions seem compatible with the recommendations by the European Parliament

The consequences of the recommendations in terms of *stringency* may be less considerable than they might seem, and they are likely less significant for *innovators* than proposed changes to the PLD could be. Also, as stated in the previous section, significant technological changes may call for corresponding regulatory steps. The resulting innovator-liability for AV-deployers may be however to a large extent comparable with the "traditional" situation, in which the current rules do not have to be applied to AVs, and *fault* can effectively be used to establish liability. However, it is not unforeseeable that *stringency* might increase to a certain extent, for instance in England where 'strictness' of the liability would increase, and the scope of the defences would be slightly limited when compared to the situation under the AEVA 2018. It must however be taken into account that a nuanced approach is suggested (comparable to the AEVA 2018), by *not* making an innovator (entirely) responsible for situations beyond his control, such as (negligent) non-implementation of a safety-critical update, or intentional modification of the AVs software by a victim. As will be elaborated further in sections Chapter 9, 9.3 and 9.4, material improvement of the said factors should not lead to unnecessary decreasing *flexibility*: where possible, the improved rules should be adaptable to changes, technology-specificity should be avoided where possible, and innovators must be able to choose as much as possible how to comply with the adapted norms.

Finally, it must be noted that (comparable to observations regarding the product liability framework), the very objective to bring *consumers* in a better proof-position by installing a *logging by design* obligation for innovators, could also negatively impact the consumer's privacy rights. As stated, *logging by design* does entail processing of personal data, and triggers privacy *risks*, and could negatively impact *trust*. Therefore, the personal data protection principles of the GDPR (specifically those regarding data minimisation, privacy by design, and the rules regarding TOMs, as well as the rights of data subjects) must carefully be observed.[1697]

8.2.4 Personal Data Protection

The product- and traffic liability rules require that personal data are acquired, stored and processed in order to establish a liability claim by victims of AV-related accidents, and the defence thereof by innovators. Personal data processing remains necessary even when the respective frameworks are "improved" in conformity with the recommendations made in the previous

[1697] See further *inter alia* section 8.2.4 and 9.4.4.

sections. Thus, it is relevant to assess how the personal data protection framework may be optimised in both the *innovator* and the *consumer* perspective, where personal data need to be processed regarding the establishment of a product- or a traffic liability claim, or the defence against such a claim.

I concluded in section 7.4 that the factors *stringency* ("1"), *legal certainty* ("2"), *risk* ("2") and *trust* ("2") must be improved in the personal data protection framework in order to better facilitate innovation and acceptance of AVs. The main finding was that the complexity of the personal data framework and the lack of clarity in the open norms of the GDPR, in combination with the serious (public) compliance enforcement measures could lead to high stringency for *innovators*. Innovators are both unable to verify when they comply with the rules, which is sometimes even impossible (for instance when blockchain-solutions are deployed, or transfer to the US takes place), and must fear high penalties for non-compliance . At the same time – and partly for similar reasons – *trust* could be negatively impacted, as it cannot be expected that *innovators* act in conformity with the (unclear) GDPR-rules, which may in turn lead to "under-protection" of the privacy of those whose personal data are processed in the course of AV-deployment. Furthermore, it is uneasy for consumers to claim remuneration from unlawful personal data processing by innovators, which may negatively impact the *risk* factor. Although it may seem a complex puzzle to improve all *factors* and thus optimize the conditions for innovation and acceptance, improving clarity regarding the obligations for innovators would be a good starting point.[1698] Optimizing *legal certainty* for AV-innovators implicates that it gets easier to understand the compliance-obligations, and calculate their enforcement risks in case of non-compliance.[1699] In turn, this could implicate that the norms are better observed by innovators, which may lead to improved *trust*.[1700]

However, improving *legal certainty* will likely not resolve all of the indicated challenges. As concluded, certain (expected) forms of personal data-processing in the course of AV-deployment can simply not be brought in compliance with the currently applicable rules. For instance, the export of personal data outside the EEA and decentralised storage of personal data using

[1698] Blok for instance finds that the development of codes of conduct under the predecessor of the GDPR, the Data Protection Directive, has led to "raising awareness about privacy issues" for innovators within specific sectors, and to "clarification and specification of the abstract legal norms" (Blok 2020, p. 112). With Gray (2020, p. 292-293), he furthermore observes that consumer confidence (i.e. an element of *trust* in view of this study) can be an important stimulus within certain sectors to adhere to the rules, such as those clarified by codes of conduct (Blok 2020, ibidem).

[1699] See the Proposed AIR, p. 3, as *inter alia* addressed above, in section 3.4.2.2: "Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and resect of existing legislation protecting fundamental rights throughout the whole AI system's lifecycle"; and the EP Proposal (European Parliament 2020a) which in a similar vein observes that "legal certainty is also an essential condition for the dynamic development and innovation of AI-based technology" (consideration K).

[1700] See Blok 2020, p. 112.

blockchain (or similar) techniques would require different solutions than just clarifying the norms.[1701] Instead, either the norms should be adapted, or the (expected) processing practices must be altered in those cases (as elaborated below). Furthermore, improvement of the *risk* factor would also necessitate an adaptation of the civil liability regime that is instituted by the GDPR, in such a way that procedural aids can be provided to victims of norm violation to establish the *causal link* between such a violation and *damage*, whereby it needs to be clarified to what extent damages should (at least) be remunerated by a norm-violator. Below, a more detailed overview is provided of *what* could be improved within the GDPR-framework in order to better stimulate innovation and acceptance; *how* that might be done – also taking the other factors (more specifically: *flexibility*) into account – is addressed in Chapter 9.

1. Further clarification and specification of certain open GDPR-norms, regarding at least:
    a. Lawfulness of personal data processing for the purposes of establishment (by victims) of and/or defence (by innovators) against a traffic- or product liability claim. This entails that there should both be a clear lawful basis to process personal data (for the stated purposes, hereinafter referred to as Product- or Traffic Liability Purposes, or PTLP, for instance by means of an Accident Prevention and Registration System (APRS)), as well as an exception to the general prohibition to process special category data such as geolocation data and personal (driving) preferences, in such a way that explicit consent of the data subjects is not required.
    b. Data Protection Impact Assessments (DPIAs); it should be clarified when "high risks" remain after carrying out a DPIA, in which case the respective Data Protection Authority must be consulted before respective data processing activities with regard to PTL PURPOSES by means of an APRS may take place;
    c. Technical and Organisational Measures (TOMs); it should be clarified when the necessary appropriate TOMs have been implemented for personal data flows by AV-innovators, for PTL PURPOSES, by the means of an APRS;
    d. Privacy-by-design & privacy-by-default (PBD); it should be clarified when the privacy-by-design and -by default-obligations can be considered fulfilled by an AV-innovator who is to implement an Accident Prevention and Registration system for *inter alia* legal defence purposes;
2. A solution should be found that would enable the decentralised storage of AV-(accident) data for PTL PURPOSES, using blockchain- or similar technology, which allows for the

[1701] However, it is not realistic to expect that to happen in the short term, given *inter alia* the impact of the CJEU decision in *Schrems II*.

exercise of the rights of data subjects, either by changing the respective GDPR-norms, or adapting the technology in such a way that data subjects rights can be effectuated.

3. International transfers of personal data for PTL PURPOSES for instance through APRS (although not limited thereto), mainly between the EEA and the US should be effectively possible. As indicated, this problem is not limited to AV-data processing, but has a broader relevance, and is of serious concern to all personal data processing activities in which services of providers in the US are used. This calls for a broad and general solution. The current political dead-lock situation after the *Schrems II*-ruling of the CJEU must thus be resolved, in order to re-enable the standing practice of data-exchange between the continents, whilst the rights regarding personal data protection of EU-citizens must be respected.
4. Introduce procedural aids for victims of (alleged) GDPR-violation by AV-innovators (as *controllers*) and the causal relationship between defect and damage, through rebuttable presumptions (at least) when controllers do not comply with their ex-post obligations regarding the execution of data subject's rights; when a personal data breach occurred, or when otherwise damage occurred after a GDPR-norm violation has taken place; and clarify when and which immaterial damages qualify for remuneration under the GDPR-liability provisions.

Clarification of the norms would not only be beneficial for *legal certainty*, it might also positively impact *stringency* (as it becomes clearer for innovators how to avoid unnecessary compliance costs). Also *trust* may benefit from better compliance with clearer norms, as this results in improved observance of the informational privacy rights of consumers.

Enabling de-centralised storage of AV(-accident) data would be beneficial for *legal certainty* and *stringency*, when it is clarified under which conditions decentralised storage may take place. Furthermore, *risk* of non-remuneration for *consumers* could be reduced when the respective data would be stored (and which must be made available to victims – in line with the recommendations above) in a non-manipulable although GDPR-compliant way, and observing the informational privacy of citizens as much as possible (see further section 9.4.4), if these data can be used to underpin a liability claim towards norm-violating innovators. *Trust* could benefit similarly.

Re-enabling international data-transfers between the EEA and the US, under improved conditions, may also lead to improved *legal certainty* (when it becomes more clear to what extent personal and under which conditions personal data may be exchanged with the US) and *stringency* (as it results in less compliance hurdles). At the same time, re-legalisation of intercontinental data processing activities under improved conditions (see further section 9.4.4) for the informational

privacy of EU citizens, may reduce *risk* (as it is not likely that after the *Schrems II*-decision existing processing activities have been re-routed to avoid the US), and increase *trust* that consumer's privacy rights are better observed.

Improving the proof-position of victims of alleged norm-violation will be beneficial in terms of *risk* and *trust*, and may also lead to more *legal certainty*. These improvements could lead to more *stringency*. However, this can be justified on the basis of the observations in the previous Chapter that currently the victim's proof-position is rather poor, and that there are no "less stringent" options to improve this.

8.2.5 CONCLUSION

In the previous sections, recommendations have been made for improvement of the *factors* with the "lowest scores".

Regarding the product liability framework, the general suggestion is, in order to improve *risk* and *trust*, that the product liability should need to function in such a manner that victims of AV-related accidents may trust that the damage suffered as a result of defective AVs, is effectively remunerable by the producers, and thus that the risk significantly decreases that suffered damage cannot be claimed from the respective producers. Therefore, the product definition should be extended to also cover software 'as such'; the minimum safety levels to be expected should be clarified in order to enable easier determination of defectiveness; post-marketing obligations for AV-producers need to be introduced in order to keep AV-(component)s safe after they have been sold (or otherwise made available) to consumers; applicability of defences regarding later-existence and development risk should be excluded, at least when the post-marketing obligations are not complied with; procedural aids should be introduced for victims, regarding the establishment of defectiveness, and the causal relationship between defect and damage. From a procedural view, rebuttable presumptions of defectiveness and causation should be introduced. From a material point of view, logging-by-design obligations should be introduced. This should enable victims, who should have access to understandable, relevant event logs, to reconstruct the relevant (autonomous driving) events prior to an accident. Failing to comply with the logging- and access-provision obligations should lead to reversal of the burden of proof instead of the rebuttable presumptions recommended above.

Regarding the traffic liability framework, the general suggestion is to improve *risk, trust* and *legal certainty* as well. It, it is suggested that traffic liability frameworks need to function so, that victims of AV-related accidents can effectively trust that the damage suffered as a result thereof, that damage is effectively remunerable by those who deploy AVs on the road, and thus that the risk significantly decreases that suffered damage cannot be claimed from the respective innovators

(or other deployers). Therefore, it should not be necessary for victims to prove fault or defect attributable to an AV deployer, in order to establish liability. Involvement of an AV in an accident, should suffice to allocate liability of the deployer of the vehicle; 100% of the damages resulting from an accident in which an AV was involved should be remunerable, unless *force majeure* can be proven, which may in turn lead to a reduction of damages to be remunerated. Furthermore it should be regulated that logged information (in line with the "logging-by-design" obligations to be incorporated in the product liability regime) should be made available both to the defending AV-deployers, and to the victims who seek compensation.

Regarding the personal data protection framework, it is recommended to improve *legal certainty*, which may in turn lead to less *stringency*, improved *trust* and less *risks* that norms are violated with damage as a consequence. Legal certainty (as well as the other mentioned factors) may benefit from specification of the: lawfulness criteria regarding data processing for Product- or Traffic Liability Purposes, (PTLP) for instance by means of an Accident Prevention and Registration System (APRS), as well as an addition to the criteria that enable the processing of special category data for such purposes – without the explicit consent of the data subjects; the criteria regarding DPIAs (more specifically when a "high risk" remains for data subjects, which requires prior consultation of the DPA); appropriateness of TOMs (regarding APRS for *inter alia* PTLP); and PBD-obligations. When improving clarity of the norms does not necessarily lead to an improvement of the factors *stringency, risk* and *trust*, as some (intended) AV-related processing activities are intrinsically non-compliant with the GDPR-provisions, such as data-export to the US, and the use of blockchain-like technologies for decentralised data storage, other solutions must be sought. In order to enable decentralised data storage using blockchain or comparable techniques, either the GDPR-norms need to be adapted, or the technology should be adapted in order to cater for the exercise of data subjects rights. A political solution seems necessary to re-enable the exchange of personal data between the EEA and the US. This would not only be beneficial for the AV-innovation, but for all other transatlantic data-processing practices. Furthermore, to improve *risk* and *trust*, it is necessary to introduce procedural aids for victims of (alleged) GDPR-violation by AV-innovators (as *controllers*) and the causal relationship between defect and damage, in the form of rebuttable presumptions in some situations. Also, it needs to be clarified when and which immaterial damages qualify for remuneration under the GDPR-liability provision.

The question *how* the necessary improvements mentioned above could be realised, is addressed in the following Chapter.

Chapter 9. THREE ROUTES TOWARDS FACTOR-IMPROVEMENT

9.1 INTRODUCTION

In this last Chapter, I will address the regulatory aspects of the improvement of the *factors* as proposed in Chapter 8. I will discuss three main routes towards improving the *factors* within the regulatory frameworks regarding product liability, traffic liability and personal data protection. The three proposed routes are motivated against the background of the research conducted in this study, and will also be discussed in relation to recent regulatory efforts and suggestions made in literature as well by the European institutions, which were introduced and elaborated above in section 4.4. Account will be taken of *inter alia* the Proposed AI Regulation,[1702] the Draft Report of the EP's Committee on Legal Affairs "with recommendations to the Commission on a Civil Liability regime for artificial intelligence",[1703] The Juri-study for the EP regarding "Artificial Intelligence and Civil Liability" by Bertolini,[1704] the report of the EC's Expert Group on Liability and New Technologies regarding "Liability for Artificial Intelligence and other emerging digital technologies", [1705] as well as the evaluations of the Product Liability Directive and the recommendations made therein regarding AI.[1706] Thus, within all three proposed solutions, focus will lie on "material" points of view, for each of the proposed solutions, the potential impact on the *factors* will be illustrated – to the extent possible in the context of recent regulatory developments.

Viewed from the "better regulation process"[1707] point of view, and against the background of the EU Better Regulation Principles,[1708] it will be sketched which ingredients are to be included in the "regulatory mix", and which actors have (at least) to be involved, in order to eventually reach the necessary balance of *factors* which stimulates innovation as much as possible, whilst creating the best opportunities for acceptance and thus uptake of AV technology in the European Union. In that, it is adamant that the other aspects of the better regulation process are carefully observed too. It is necessary that any regulatory activity towards *factor* improvement is and remains embedded in a cycle of forward planning and political validation; stakeholder consultation; evaluation and fitness checks; impact assessments; quality control; and implementation support and monitoring.[1709]

[1702] See *inter alia* section 3.2
[1703] See European Parliament 2020 and European Parliament 2020(a).
[1704] Bertolini 2020.
[1705] European Commission 2020.
[1706] See *inter alia* European Commission 2018 and 2018b.
[1707] See section 3.3.6
[1708] Ibidem.
[1709] See further section 3.3.5 and 3.3.6.

In section 9.2, I explore to what extent binding industry codes of conduct could improve the *factors*, which is inspired by the statements that Volvo, Mercedes and Google already made that this company will accept liability for malfunctioning AV-technology.[1710] The effectiveness of this option largely depends on the commitment of market-parties such as AV-producers and other stakeholders. Binding industry codes could contribute to solving the indicated challenges, however they go not necessarily lead to a harmonised solution of the indicated traffic-liability problems. Therefore, this option likely entails at best minimal improvements of *legal certainty*, *risk* and *trust*, and does not fully decrease the need for more tenable solutions, such as those proposed in section 9.3 and 9.4. In section 9.3, it is suggested, notwithstanding the more structural solutions proposed in section 9.4, to implement a mandatory insurance scheme, in order to relieve the most pressing obstacles to innovation and acceptance, which are related to *legal certainty*, *risk* and *trust*. This scheme should be applicable throughout the European Union in order to equally improve the *factors* within the EU, and in order to prevent differences *inter alia* regarding the protection of consumers as well as market fragmentation between Member States.[1711] Although it would also require significant regulatory effort from both public and private stakeholders to realise such a scheme, it is likely that this *can* in principle be achieved, looking at the – to a certain extent comparable – English example formed by the AEVA 2018. In section 9.4, a "long-term", durable solution is proposed, which involves adaption of the existing frameworks regarding product liability and personal data protection, and suggests to implement a harmonised regulatory framework regarding traffic liability. This solution seeks to directly address the AV-related challenges within the respective frameworks, rather than to create for instance a *sui generis* regulatory (insurance) framework. Although this third solution would be the most tenable of the three, significant regulatory efforts from both public (EU)- and private actors will be required. As it is even suggested that (it should at least be investigated that) the regulatory changes could also address other technology in which autonomy plays an increasing role, it is likely that it will take relatively long time to reach the eventually desired results.

It is therefore that a parallel approach is advisable. It is suggested that regulatory endeavour regarding all three options is started simultaneously in order to realise the desired *factor*-improvements, and in order to prevent unnecessary waiting as much as possible and thus a time-spill for reaching the eventually desirable, tenable end-results.[1712] Due to the complexity that the optimisation of all three regulatory frameworks (instead of creating one *sui generis* regime)

[1710] See for instance https://www.autoexpress.co.uk/volvo/93595/volvo-to-accept-liability-if-autonomous-car-tech-fails; and https://www.cbsnews.com/news/self-driving-cars-google-mercedes-benz-60-minutes/.
[1711] See also European Parliament 2020a, cons. 24; and below footnote 1721.
[1712] This also fits within the better regulation principles regarding *inter alia* forward planning, ongoing political validation and improvement of the regulatory solutions.

implicates, and the lengthy process that will the likely result thereof, the work regarding the third solution can profit from the "lessons learned" from for the first and second improvement routes.

9.2 First Route - Binding Industry Codes of Conduct

As observed in sections 3.3.3- 3.3.5, it is, from a regulatory perspective, encouraged that private actors participate in the regulatory process.[1713] As such, stakeholder participation – which is also mentioned as one of the *better regulation* principles[1714] – could induce a fast, effective and efficient response to rapidly evolving technologies, whereby compliance with (new) norms is better ensured than without private-actor involvement.[1715] It is even indicated that "bottom-up" regulation could enhance the protection of consumer's rights, and *trust*.[1716] From this perspective, it is relevant to address the initiative by Volvo – which has been followed by Mercedes Benz and Google – regarding one of the most pressing issues that needs to be resolved in terms of *risk* and *trust*,[1717] i.e. that under the current product- and traffic liability regimes, victims cannot always trust that their damages resulting from an AV-related accident are (easily) remunerated.

On October 1st 2015, Volvo CEO Håkan Samuelson announced, according to Fortune and AutoExpress, that the "company will accept full liability whenever one of its cars is in autonomous mode".[1718] Mercedes and Google made similar statements, according to CBSNews, who report that "Google and Mercedes told us, if their technology is at fault once it becomes commercially available, they'll accept responsibility and liability".[1719]

Should these statements appear to become practice, this could be qualified as some form of self-regulation,[1720] although without further regulatory embedding (and in fact without implementing the *factor* improvements suggested in the previous Chapter), with limited relevance in terms of *risk* and *trust*. While the victims of AV-crashes in which Volvo, Mercedes or Google cars were involved might trust that their damages can be claimed easier from those companies, *risk* and *trust* may only then improve structurally and generally when the majority - if not all - of the AV-

[1713] See more specifically section 3.3.3, footnote 147.
[1714] See section 3.3.5, and the reference to the second step in the Better Regulation principles, as included in European Commission 2017a, p. 4.
[1715] Ibidem sections 3.3.3- 3.3.5; Baldwin, Cave & Lodge 2012, p. 26-31; De Cock Buning & Senden 2020, p. 4.
[1716] OECD 2015, p 6, as cited in De Cock Buning & Senden 2020, p. 4.
[1717] Which is correspondingly addressed in general in the recommendations formulated in section 8.1: ("in very general terms, situations in which victims (*consumers*) of AV-related accidents and improper personal data protection related to AV-deployment, *risk* that they cannot (easily) claim damages from a producer or another deployer (*innovator*) should be prevented as much as possible, in order to improve both the *risk* and the *trust* factors").
[1718] https://fortune.com/2015/10/07/volvo-liability-self-driving-cars/; see also https://www.autoexpress.co.uk/volvo/93595/volvo-to-accept-liability-if-autonomous-car-tech-fails.
[1719] https://www.cbsnews.com/news/self-driving-cars-google-mercedes-benz-60-minutes/.
[1720] See section 3.3.3.

producers would join in such a practice. This in turn would depend on the voluntary participation of those stakeholders for instance in the form of an *industry code or standard*, which participation can however not be enforced – at least not without the involvement of a public, preferably the European, regulator. Some form of co-regulation would be required then, in which the public regulator mandates to institute the self-made rules throughout the AV-sector. However, this may bring about several problems.[1721]

From a regulatory perspective, "legitimacy and accountability" could then become a serious issue, as indicated by De Cock Buning and Senden, for instance "because of the possibly binding effects which such regimes may have for third parties, the lack of an electoral mandate supporting [such a regime] and of self-interests that might prevail over public interest".[1722] It may be problematic for other stakeholders in the sector than those who were involved in the co-regulatory process to comply with the norms, especially when these norms are easier to comply with for "larger" actors than for smaller companies for instance. Referring to the statements by Google, Volvo and Mercedes, it should be noted that these are very large companies. In order to overcome (some of the) issues in terms of legitimacy and accountability, at least some other, smaller actors would need to be involved as well. Whether the outcome of such a process in which the diverse actors are better represented, would – or should – be comparable to the said statement can be doubted however.

[1721] Besides the potential issues mentioned hereafter, it should be assessed whether or not European regulatory intervention can be legitimated. In that sense, it can be observed that in principle civil liability regulation can be addressed by the EU, on the basis of the principle of conferral, as stated in Article 5 TEU, which may here for instance regard the establishment and functioning of the internal market, as well as consumer protection (cf. article 114 and 169 TFEU). Furthermore, Union legislation should be in conformity with the principles of subsidiarity (see article 5(3) TEU, indicating that in cases of non-exclusive legislative competence of the EU, legislation may only be instituted to the extent that "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") and proportionality (see article 5(4) TEU: "Union action shall not exceed what is necessary to achieve the objective of the Treaties"). In its call on the European Commission to regulate civil liability for artificial intelligence, the European Parliament motivates its proposal as follows: "(24) *Since the objectives of this Regulation, namely to create a future-oriented and unified approach at Union level, setting common European standards for European citizens and businesses to ensure the consistency of rights and legal certainty throughout the Union and to avoid fragmentation of the Digital Single Market, which would hamper the goal of maintaining digital sovereignty, of fostering digital innovation in Europe and of ensuring a high-level protection of citizen and consumer rights, require that the liability regimes for AI-systems are fully harmonized. This cannot be sufficiently achieved by the Member States due to the rapid technological change, the cross-border development as well as the usage of AI-systems and eventually, the conflicting legislative approaches across the Union, but can rather, by reason of the scale or effects of the action, be achieved at Union level. The Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives*" (emphasis added). Along similar lines, it can be argued that a co-regulatory approach such as addressed hereafter, also corresponds with these objectives, the conferral principle as well as proportionality and subsidiarity.

[1722] De Cock Buning & Senden 2020, p. 4-5.

In the stated form, a rule that sees to the "generic acceptance of liability" when AVs are involved in an accident where damage was caused, might provide a high level of *legal certainty* for innovators to whom the rule applies. Furthermore, the rule is likely *flexible* enough to deal with technological changes, and is not prescriptive in terms of which compliance-route to follow. Also, such a rule likely contributes to *citizen's trust* that the innovators are stimulated (in order to avoid liability) to make their AVs as safe as possible, and that their damages are remunerated should accidents nonetheless happen, leaving them with less *risks* of non-remuneration than those under the current product- and traffic liability regimes. Acceptance of liability would likely also decrease the need for the acquisition, storage and analysis of AV- and accident data, which can be stated to be beneficial for privacy protection of *citizens* and thus of their *trust* that the fundamental data protection rights are not unduly disregarded. At the same time however, it may lead to more *stringency*. Having to accept full liability will result in more and higher remuneration obligations for innovators, than would be the case under the liability rules in their current form as well as when the suggested amendments were to be implemented,[1723] which are more nuanced for instance in terms of the requirements for establishing liability, potential defences, apportionment- and redress possibilities. While this might not be a problem for larger companies, it can be problematic for smaller (and start-up) companies, who would have to reserve more means for potential liability claims than would otherwise be the case,[1724] which means they cannot invest in development and deployment of AV-technology, while their overall budget is likely smaller than the budget of larger companies. Furthermore, while the stated rule may provide a solution for the most troublesome issues from a *consumer perspective*, it leaves the indicated problems in the studied regimes in principle intact.[1725] When these problems, in terms of mainly *legal certainty, risk* and *trust* – and to a smaller extent *stringency*, remain unresolved, the opportunity is missed to improve these frameworks, which might not only be relevant for the development and deployment of autonomous vehicles, but also for related and similar (autonomous) technologies.[1726]

Alternatively, and also in line with the *better regulation* principles,[1727] the stated generic liability acceptance can be taken as a starting point for a co-regulatory process (as also suggested regarding the third route in section 9.4) in which a fair representation of the different

[1723] See section 8.2 regarding the material aspects, and hereafter regarding the regulatory aspects.
[1724] At least to the extent that appropriate and affordable insurance would not exist.
[1725] See Chapter 7.
[1726] This is a hypothesis rather than a conclusion that can be drawn from this research.
[1727] I.e. regarding *inter alia*: forward planning and political validation; stakeholder participation; and evaluation and fitness checks, see European Commission 2017a, p. 4-9.

stakeholders participate,[1728] which may lead to more nuanced outcomes. It could for instance be envisaged, among many other options, that the results thereof can be compared with the recommendations above, that AV-involvement in an accident would in principle lead to liability of an innovator (i.e. a producer), which might be reduced in some situations, for instance when a safety-critical update is missed, or when the AV-software is deliberately modified by the AV-consumer. Should that be the case, this might in turn present a better situation in terms of *stringency* compared to the original rule, and to an improvement of *risk* and *trust* when compared to the current situation. However, this may to a certain extent re-trigger the necessity to acquire, store and analyse AV-(accident)related personal data. Then, it would still be required to improve the identified *factors* regarding the regulatory framework on personal data protection. As further elaborated in section 9.4, a co-regulatory approach can be followed to solve some of the problems in conformity with the recommendations indicated in section 8.2.4. Moreover, even when a more nuanced rule would be the outcome of a co-regulatory process, i.e. a better "balanced" liability for innovators on the basis of a binding industry code-of-conduct, this would likely not resolve the indicated issues regarding the *factors* within the current regulatory frameworks.

Nonetheless, the opportunity should not be missed to enter into a close dialogue between the innovators, the public EU regulators and consumers to evaluate – and test – certain bottom-up improvements as indicated in the previous Chapter. Perhaps *regulatory sandboxes* (see further section 9.4.4), in which new rules and technology can be tested in an enclosed environment under direct supervision of the public regulator, can be used to this end. When applying *regulatory sandboxes*, it may be evaluated "in real life" whether or not the problems indicated in Chapter 7 appear to exist in practice. Also, the solutions indicated in Chapter 8 and the potential impacts on the *factors* can be evaluated more realistically. A bottom-up approach (including *regulatory sandboxes*) can be achieved relatively fast, and independently of political processes. Moreover, it can be recommended to combine this with other regulatory efforts as discussed in the following sections, whereby improvement of the *factors* should, from a regulatory perspective, be – as further addressed there – the required end-result. Improving the *factors* within the frameworks would likely be a complex and lengthy process, which may benefit from the "lessons learned" when other routes, including a bottom-up approach as described above, are pursued in parallel with the more tenable improvements within the regulatory frameworks regarding product liability, traffic liability and personal data protection.

[1728] All stakeholders within the AV-liability chain should then be represented, which might (non-limitative) include: AV-producers, component- and software producers, resellers, renters and lessors, insurers, AV-owners, victims (associations), government, NGOs et cetera.

9.3 Second Route – Mandatory Insurance

A second route towards solving one the problems of "under-compensation" of AV-accident victims,[1729] i.e. that under the current product- and traffic liability regimes, victims cannot always trust that their damages resulting from an AV-related accident are (easily) remunerated, could be explored in the form of mandatory insurance.[1730] The route sketched below, draws its inspiration from the AEVA 2018, and should in principle be applicable irrespective of and independent from the product- and traffic liability frameworks in their current form. From a regulatory perspective, this insurance scheme would mainly consist of a "public" regulation to be instituted on the EU-level.[1731] However, there should certainly be a role for private actors,[1732] for instance regarding potential limitation of remuneration-obligations (through contractual exclusions in case of certain behaviour, or caps on damages to be compensated), as further elaborated in the following sections.

Comparable to the AEVA-2018 regime, it could be regulated that an AV-owner should take out insurance, which independent of (fault- or risk) liability insures damage of *any* victim of an accident in which an AV was involved. Differently from the AEVA – and more comparable to the systematics of the Loi Badinter, *involvement* should suffice to trigger a remuneration obligation, which would be bestowed on the insurer of an AV-owner or keeper, and any form of material or

---

[1729] Which is, as stated above, correspondingly addressed in general in the recommendations formulated in section 8.1: ("in very general terms, situations in which victims (*consumers*) of AV-related accidents and improper personal data protection related to AV-deployment, *risk* that they cannot (easily) claim damages from a producer or another deployer (*innovator*) should be prevented as much as possible, in order to improve both the *risk* and the *trust* factors").

[1730] The insurance-option is *inter alia* also evaluated by Bertolini 2020, p. 14; the Expert Group (in European Commission 2020, p. 61-62,; and Engelhard & De Bruin 2018, p. 86-91, of which the observations are taken into account here as well. It must be noted that compulsory insurance is incorporated in the EP proposal (European Parliament 2020a) too: it requires the (backend and frontend) operators of high-risk AI-systems to take out insurance to cover for the liability risks that follow from the proposed regulation in article 4(5).

[1731] The indicated differences in the protection of victims of AV-related accidents are (inter alia) the result of national regimes that sometimes provide diametrically different outcomes (see section 7.3), which leads to different valuation of the *factors* throughout the studied regimes. In order to optimise these and to reach the same level of *risk* and *trust*, as well of *legal certainty, stringency* and *flexibility*, it would be most logical to regulate on the Union-level. See in similar vein Bertolini 2020, p. 11. See also Engelhard & De Bruin 2018, p. 91; and also European Parliament 2020a, consideration 2 and 24, and the observations above in footnote 1721 regarding the principles of conferral, subsidiarity and proportionality. However, a mandatory first-party insurance option is under the current conditions (in which autonomous driving technology is not deployed), will likely not be feasible in for instance The Netherlands. See for instance the letter by the Dutch minister for Rechtsbescherming (legal protection) S. Dekker in his letter to the Tweede Kamer (House of Representatives of the Netherlands): https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z11989&did=2021D25938. That might however change when autonomous driving becomes widely deployed, for the reasons sketched in this study.

[1732] Notwithstanding the "general rule" that is instituted in *inter alia* the EU Better Regulation principles (see section 3.3.3) to involve private actors throughout the whole regulatory process. The stakeholders to be involved, should at least Include *inter alia* insurance companies, AV-producers and -users, and victims-associations.

immaterial damage should in principle be remunerable, as long as this can be reasonably connected to the accident. Comparable to the AEVA-systematics, it may be allowed that insurance companies stipulate in their agreements with AV-owners remuneration-obligations towards the AV-owner as a victim, in case the insured owner intentionally failed to install safety-critical updates, or where the victim deliberately modified the AV's software.[1733] In order to underpin the insurer's claim not having to remunerate damages on the basis of aforementioned provisions or a defence thereto from the owner, it should be regulated that activity-logs may be requested from a producer, or another entity who has made or stored such logs.[1734]

It should be possible for an insurer who remunerated victim's damages under the mandatory insurance scheme, to seek redress from the producer, as long as *factors* within the product liability framework have not been optimised in such a way that the suggested improvements described in section 8.2.2 are effectively implemented. Similarly, a mandatory insurance mechanism could also be required from AV-producers. In that system, AV-producers would also be obliged to take out insurance in case the insurance company of an AV-owner would seek redress. Redress remuneration obligations could be limited, when the insurer would not have contractually exonerated his remuneration-obligation towards the AV-owner in case of intentional failure to implement safety critical updates, or deliberate modification of the AV-software, and one of these issues triggered the damage-inflicting accident.

The proposed mandatory insurance schemes see to the improvement of the *risk* and *trust factors*, as these could significantly reduce the risk that victims are not (sufficiently) compensated after an accident in which an AV had been involved. Also, implementing such schemes would reduce the need for personal data processing, as the assessment of a norm-violation and causation would become less relevant. It is however indicated in literature that compulsory insurance schemes might not necessarily induce an incentive for producers to make their AVs as safe as possible, because remuneration-obligations are "externalised" to an insurance company,[1735] which would

[1733] This mechanism can be compared to "contributory negligence" situations under the AEVA 2018, as illustrated *inter alia* in section 4.3.4.4.3. I would argue that damage that is caused by a third party who ought not to have access to the AV's system, but who still succeeded in hacking it, should be borne by the insured person (who may have a recourse claim towards the hacker, and the producer) rather than by the victim, so long as the victim did not neglect his obligation to install safety-critical updates.
[1734] See further regarding the logging-by-design obligation section 8.2, and section 9.4.
[1735] See European Commission 2020, p. 61, footnote 131, where they refer to Faure, M., "Economic Criteria for Compulsory Insurance", *The Geneva Papers on Risk and Insurance*, 2006, vol. 31, p. 149 ff. See also Engelhard & De Bruin 2018, p. 90.

not be beneficial for *trust* regarding the safety of AV-technology, although such disincentives seem not to be empirically evident.[1736]

However, *legal certainty* may benefit, as implementing these schemes could implicate a simplification of the currently applicable rules, which would lead to better calculability of the risks for *innovators* – where the said simplification should, observing technology-neutrality and the freedom for innovators to choose from different ways of insurance, at the same time not detriment *flexibility*. The fact that *innovators* would be required to take out insurance, could lead to increased *stringency*. As observed by the Expert Group, some producers might want to "compensate victims of their activities out of their own funds",[1737] and may not want to be obliged to take out insurance,[1738] which can be very expensive as it might be "difficult to calculate [premiums, *RWdB*] due to missing experience, which is quite likely with new technologies",[1739] if such insurances would become available at all. Furthermore, insurance premiums could become very high, also due to expectations of false, or overly high claims by victims.[1740] These issues could likely be resolved (or limited), by "capping" the maximum amounts of damages to be remunerated,[1741] in such a way that these would enable insurance companies to a) provide the necessary insurances, and b) calculate the corresponding premiums. These caps should be reconsidered and perhaps removed when required data become available, after deployment of AVs in society. How high the initial (and the reconsidered) caps should be (in order to reach a balance between *risk* for consumers and *stringency* for innovators), may have to be determined in a joint discussion between the relevant stakeholders, including *inter alia* the public EU regulator, AV-producers, insurers, and victims-associations.[1742]

In its Proposal, the European Parliament underscores that (liability) insurance[1743] coverage "is essential for assuring that the public can trust that the new [AV,[1744] *RWdB*] technology despite the potential for suffering harm or for facing legal claims by affected persons".[1745] The EP also

[1736] Ibidem Engelhard & De Bruin, p. 90, and more specifically the remark there that there is no empirical evidence available that "no-fault insurance reduces the level of care or has negative effects for the behavior of insured parties", where reference is made (in footnote 39) to Anderson, J.M. et al., *The U.S. Experience with No-Fault Automobile Insurance – A Retrospective*, Rand-report, Santa Monica (CA): Rand Corporation 2010, and Van Dam 2008, p. 356.
[1737] European Commission 2020, p. 61.
[1738] In line with the Expert Group's observation: I would not suggest to make producer-insurance voluntary, given a potential risk of his insolvency (and thus undercompensation of victims) in case of (multiple) claims that may be filed against him.
[1739] Ibidem, see also Engelhard & De Bruin 2018, p. 90.
[1740] Ibidem.
[1741] European Commission 2020, p. 61; Bertolini 2020, p. 104.
[1742] Ibidem.
[1743] I.e. instead of compensation funds, see consideration 23 of European Parliament 2020a.
[1744] Ibidem, consideration 24.
[1745] Ibidem, consideration 23.

observes that "uncertainty regarding risks should not make insurance premiums prohibitively high and thereby an obstacle to innovation",[1746] despite the lack of historical claims data.[1747] However, the Parliament calls on the European Commission to co-operate with *inter alia* insurers in order to come up with "innovative insurance products that close the insurance gap", referring to comparably new products "that are developed area-by-area and cover-by-cover as technology develops".[1748] Anticipating the fruitful results of a co-operation between public EU regulator and private actors, the EP has proposed that mandatory insurance must be taken out to cover for the liability risks that may result for operators of high-risk AI-systems from the proposed regulation.[1749] Liability, and thus insurance amounts, are capped in the proposal at € 2 million in the event of personal damage (including death), and at € 1 million "in the event of significant immaterial harm that results in verifiable economic loss of or damage caused to property".[1750]

This insurance-obligation proposed by the European Parliament would apply to situations in which an operator is held *liable* towards a victim, which is thus different from the mandatory *no-fault* insurance that is proposed in these sections. However, the underlying issues indicated by the EP regarding *inter alia* the determination of premiums and the lack of historical claims data, as well as the need of co-operation between the public regulator and the stakeholders in the sector, are comparable. In line with the vision of the EP, I argue that an insurance solution should be sought. As stated above, capping liability at certain amounts could be considered an option to be discussed between the public- and private actors.

However, such liability caps may be negative for the *risk* and *trust* factors, when these would result therein that suffered damage exceeds the insured – and thus the remunerated – amounts or types of damage. Considering such cases, it remains relevant to evaluate the (to be) regulated caps regularly, and to adjust these where necessary. Furthermore, there still would be a relevant role to play for "traditional" traffic liability regimes – be it in adapted form.[1751] This role may see to compensating damage that would remain non-remunerable under a mandatory insurance scheme, as it can be observed that "[u]nder no-fault policies, this [level of compensation] will generally be lower than under civil liability law", of which the compensation levels are often "more generous".[1752] Also, it can be envisaged that where the insurer serves as a "one-stop-shop" for

[1746] Ibidem, consideration 24.
[1747] Ibidem, recital 21.
[1748] Ibidem, recital 22.
[1749] Article 4(4) as stipulated in European Parliament 2020b.
[1750] Ibidem, article 5(1).
[1751] See sections 8.2.3 and 9.4.
[1752] Engelhard & De Bruin 2018, p. 91, and the reference to Albert, J., *Compensation of victims of cross-border accidents in the EU: comparison of national practices, analysis of problems and evaluation of options for improving the position of cross-border victims*, Part II. Analysis, Report, European Commission 2009, via https://ec.europa.eu/info/publications/compensation-cross-border-victims-eu_en.

victims, redress from other actors in the chain which were involved in the constitution of the damage, should also be based on the "traditional" traffic liability rules.

Furthermore, the opportunity should, in my opinion, not be missed to improve the current liability regimes, in such a way that – in conformity with their original purposes – they see to the effective compensation of victims of AV-related accidents. In other words, I argue that it would be an undesirable situation to just "apply a regulatory bandage" to compensate AV-accident victims through a mandatory insurance, without "curing the wound" of a traffic liability system that functions sub-optimally. Thus, adaptation of the current traffic liability frameworks in combination with a mandatory insurance scheme,[1753] is preferable over the sole institution of a mandatory insurance scheme *without* adapting the traffic liability rules that are in place already (which currently also co-exist alongside compulsory third-party insurance schemes), albeit perhaps in their currently suboptimal forms regarding the *factors*, which is further elaborated in the following sections.

The proposed sector-specific mandatory insurance for AV-producers may however eventually be phased out, should redress be possible from producers on the basis of improved product liability rules,[1754] and when such claims would be sufficiently covered under "regular" business liability insurance.

9.4 THIRD ROUTE – TENABLE CHANGES TO THE STUDIED FRAMEWORKS

9.4.1 INTRODUCTION

Eventually, the most straightforward option to execute the recommendations regarding optimisation of the *factors* as proposed in section 8.2, will be to implement the required adaptations within the regulatory regimes themselves, also in order to maintain the relevance of the respective frameworks also in the context of advancing technology. This does not preclude the meaningfulness and usefulness of exploring (in parallel) the other routes as outlined in the previous sections, to the contrary. Whereas the "output" of section 8.2 is taken as a point of departure, it may well be that in a further exploration of the other two routes leads to new insights, which should be taken into account in the regulatory changes addressed hereafter. In the following sections, it will be assessed how the material changes suggested in 8.2 could be addressed within the product liability regime (section 9.4.2), the traffic liability regime (section 9.4.3) and the regime regarding personal data protection (section 9.4.4).

[1753] Comparable to the mechanism proposed by the European Parliament, European Parliament 2020a.
[1754] For instance in conformity with the recommendations in sections 8.2.2 and 9.4.

9.4.2 PRODUCT LIABILITY

In order to prevent differences between the Member States when seeking to improve the *factors*, it may be recommended, in line with the suggestions by Bertolini,[1755] and the EP Proposal,[1756] to implement the material changes in the form of a regulation, rather than a directive.[1757] Whether or not the recommendations with regard to AVs could also be extrapolated to other products in which some form of Autonomous Intelligence is incorporated,[1758] is not the object of this study. Thus, the recommended changes should, from this study's perspective, be limited to the development and deployment of AVs. However, it cannot be precluded that the material principles for improvement as addressed in section 8.2 would have relevance beyond the field of AVs, although this would require further investigation.

It is relevant to note that there are differing opinions regarding the question how to regulate different extra-contractual liability regimes regarding the diverse "appearances" of AI within products or services. Bertolini is not in favour of regulating (product) liability for artificial intelligence in a broad sense, and argues for a sector- and technology specific rules.[1759]

Contrarily, the EP does (as does for instance the Expert Group) propose a unitary approach of liability regulation for AI, and seems to have less problems with the heterogeneity of AI appearances, by taking the "output" of AI-systems into account for determining liability.[1760] The proposal distinguishes between high-risk and low-risk AI-systems, depending *inter alia* on the significance of harm to be expected, the number of potential victims who are exposed to the risks, the randomness and the chance for victims to be exposed to these risks which goes beyond "what can be reasonably expected". Establishing the "significance of the harm", should be the result of a weighing of factors, including the severity of possible harm or damage, the degree of autonomy in decision making, the likelihood that risks materialise and the ways and context in which an AI-system is likely to be used.[1761] For the avoidance of legal uncertainty regarding the qualification of AI-systems as such, and to be classified as high-risk (which uncertainty I consider to be likely, given the many factors that should be used for determining *inter alia* intelligence, autonomy, and risk), the EP refers to a list, which is to state in a limitative way high-risk AI-systems.

[1755] See Bertolini 2020, p. 11.
[1756] European Parliament 2020a, consideration 8. The EP "urges the Commission to assess whether the PLD should be transformed into a regulation" – amongst many other things.
[1757] As the main elements of the PLD and the objectives would remain unchanged, should the recommendations be implemented, it can be argued that this would not conflict with the principles regarding conferral, subsidiarity and proportionality. See further footnote 1721.
[1758] See also section 2.2.
[1759] Bertolini 2020, p. 12, 31.
[1760] Ibidem Article 3(b).
[1761] Ibidem, Article 3(c).

Clearly, the EP pursues a different approach than Bertolini, by seeking an overarching set of rules instead of proposing technology- and sector-specific regulation. Taking account of the disadvantages of technology-specific regulation (as illustrated in section 3.4.2.2.2), and the general recommendation to regulate the *outcomes* of certain technology rather than the *technology* itself, the EP's proposal as such is understandable. However, where the determination of a high-risk AI-system is done by the public regulator, one can question the legal certainty for those who are to deploy low-risk AI-systems, as the definitions enshrined in the proposal are very generic, and rather vague. Furthermore, where the Proposal institutes *new* obligations for "operators" of AI-systems, I do not think this should be done in a *sui generis* regime, as in my opinion this would be better placed in the context of existing regimes, which would – or should – otherwise also apply to respective operators.

The Proposal provides rules for "operators" of AI-systems. Frontend-operators (who exercise a certain degree of control over risks connected with the system and who benefit from their operation)[1762] are distinguished from backend-operators (who define on a continuous basis the features of the technology, and who provide data as well as an essential backend-service, and thus *also* exercise control over the risks AI-systems may pose).[1763] Producers in sense of the PLD, may qualify as operators under the Proposal. Thus, there would be a certain overlap in the norms for producers-as-operators, should the Proposal be enacted. As described in Article 11, the proposed regulation prevails over the PLD if the producer in sense of the PLD is the only "operator", or if the producer is the "frontend operator". The PLD prevails in situations in which a producer is (only) a backend operator. This rule in itself may lead to *legal uncertainty* regarding the question which rules must be taken into account by AV-producers. Furthermore, in cases where the proposed regulation is to prevail over the PLD, this implicates a very strict liability for producers in their role as (frontend) operators of high-risk AI-systems: they will, in general terms,[1764] be liable (be it to capped amounts of damage, see Article 5) towards victims when their systems cause harm, unless they can prove *force majeure* (which is not defined in the regulation). Although it must be agreed that the current liability norms for producers in sense of the PLD should be optimised (see section 8.2.2 and this section below), I would to implement the necessary improvements within the PLD-regime, rather than in a new set of *sui generis* obligations.[1765] Furthermore, thinking along the lines of the conclusions and material recommendations of this

[1762] Ibidem, Article 3(e).
[1763] Ibidem, Article 3(f).
[1764] See European Parliament 2020a, Article 4.
[1765] I note again, that in my opinion it is better to "cure a wound" (which is in this case formed by a product liability regime that should *inter alia* see to the effective remuneration of victims who sustained damage inflicted by defective products (in the broad sense), while, as observed in the previous Chapter, this will often not be the case in accidents involving a specific type of products, being AVs), than just to "apply a regulatory bandage" (by creating *sui generis* rules for a "new" type of products).

research, it may be argued, as regards the *stringency factor*, that it will not be necessary to regulate such a strict and unnuanced liability for producers as (frontend) operators of high-risk AI-systems as recommended in the Proposal. At the same time the *risk* and *trust factors* would *inter alia* benefit more from the introduction of procedural aids within the PLD, rather than of a new rule which would still require victims to prove causation between the operation of a high-risk AI-system and damage suffered.

Thus, taking into account the boundaries of this research, the following amendments to the Product Liability Directive(/Regulation) are suggested which would apply to producers of Autonomous Vehicles (whereas I recommend to further research when it comes to extending these to other applications of AI in products):

1. It can be envisaged that a special regime is created for producers of AV(-components), under the general product liability rules. These new provisions,[1766] may (should that appear to be opportune) be extended with producers of other applications containing AI, and adapted when necessary. These provisions should be regulated in close collaboration between the public regulator and private actors, including *inter alia* AV(-component) producers, AV-users, consumer- and victims associations, and insurers, although in conformity with the following principles;
2. These provisions should regulate that:
    a. Software is included under the definition of *product* in sense of Article 2 PLD;
    b. It is clarified in the sense of Article 6(1) PLD that an AV(-component) is defective, when it results in the AV not to possess those driving skills which can be expected from the most excellent human driver, and when the obligations for the producer under the GDPR are not complied with, regarding personal data that have been generated, stored or otherwise processed by or through the AV;
    c. The defences incorporated under article 7(b) (regarding later-existence) and 7(e) (regarding development risk) PLD, may only be invoked when a producer can prove:
        i. that he provided safety-critical updates, during a certain (to be established) period, in order to prevent or repair (potential) defects in his product, and that the injured person deliberately failed to implement these; or

[1766] Rather than a new set of norms. Eventually, I would argue for a consolidated review of the product liability rules, such that the "generic" rules can be applied to both traditional and new (AI-)technology. Given the indicated boundaries of this research, I can however not recommend to do so, just on the basis of this study. However, as stated in the previous footnote: "bandages" in the form of *sui generis* rules should be prevented in my opinion.

ii. that the injured person intentionally modified the AV('s software), which rendered the AV defective;

d. Article 4 PLD is amended as such that when persons sustained injury after an accident in which an AV was involved:
    i. a defect and the causal relationship between the defect and the damage are *assumed*,[1767] which assumption can be rebutted by the producer, unless
    ii. the producer failed to provide the injured person access to AV-logs in terms of the following provision, in which case the burden of proof regarding the defect and the causal relationship are *reversed*. i.e. resulting therein that producer needs to prove that there had been no defect, and that the damage could not have been caused by the defect.
e. A new obligation is introduced in the product liability rules regarding "logging-by-design". Producers shall implement functionality that logs AV-activity, which enables the reconstruction of the course of events prior to an accident, including the automated decisions taken by the AV. These logs should be made available on request of a victim, or on request of an AV-owner in the course of a claims-procedure under the (new) traffic liability rules, as further illustrated in section 9.4.3, and/or a product liability claim. The aforementioned logging-obligations as well as the processing of logged information in a claims (settlement) procedure may serve as a lawful basis for personal data processing in sense of article 6(1)(c) GDPR.

Besides the potential for improvement of the *factors* as elaborated in section 8.2.2, it is stressed again that *flexibility* may profit from a regulatory approach that is as technology neutral as possible, and that it is overall advisable to regulate the provisions above in an iterative way, in which all relevant stakeholders are involved. Such involvement may especially be crucial regarding the implementation of the "logging-by-design" obligation, in sense of point 2(e) above.

By definition, generating AV-activity and -decision logs involves the processing of personal data. Should that not be done in an appropriate, GDPR-compliant manner, this could negatively implicate *risk* and *trust*. As further elaborated in section 9.4.4, and as underscored by the Expert Group who also recommends the introduction of a logging-by-design obligation, privacy rights of data subjects whose data are processed as a consequence, should be carefully obeyed.[1768] Furthermore, the EG recommends that "logging would have to be done in such a way that no interested party could manipulate the data and that the victim/person who compensates the

[1767] Although *without* reversing the burden of proof (at this stage).
[1768] See European Commission 2020, p. 7, 47-48.

victim in the first place, for example an insurance provider, has access to it".[1769] As illustrated in section 5.2.6, blockchain technology could provide just such a solution, however (as addressed *inter alia* in section 6.4.1.2) it is hardly likely that such technology can, in its current form, be brought in compliance with the GDPR-obligations.

Therefore, a dialogue between the public EU regulator and private actors including at least AV(-component) developers, insurers and victims(/consumer) associations is recommended. In that dialogue, it should be investigated:

- to what extent the currently available technology and/or the applicable rules may be adjusted, in order to ensure the "integrity, availability and confidentiality" of the logged data, as well as maximum personal data protection, i.e. for instance through ensuring that a minimum amount of personal data is processed;
- for which period of time such data should be processed;
- in which cases aggregated or pseudonymised data can be processed, and in which cases "personal data in the clear" must (still) be used; and
- and how personal data can only be accessed and/or altered by, or with consent of the data subjects.[1770]

9.4.3 TRAFFIC LIABILITY

In line with the observations by the European Parliament in its proposed civil liability regime for AI,[1771] and those of the European Commission in its Proposed AI Regulation,[1772] I argue that the material recommendations illustrated in section 8.2.3 could best be implemented in the form of a regulation. As this research has shown, there are significant differences between the regimes of the Member States, leading to diverging *risk* and *trust* amongst the regimes, and correspondingly, different levels of *legal certainty* for innovators. From a *factor* improvement perspective, innovation of AVs and acceptance thereof in society may profit the most when the *factors* are equally represented throughout the European Union. The public regulator should play the leading role in the regulatory process, although the other (private) actors should be involved in conformity with the better regulation principles as illustrated in section 3.3.3. The main principles of the traffic liability regulation should at least consist of the following points:

1. The owner of an AV is liable towards victims of accidents in which his AV is involved;

[1769] Ibidem, p. 47.
[1770] See further section 9.4.4.
[1771] European Parliament 2020a, recital 24, as elaborated above in footnote 1721. See also Bertolini 2020, p. 11
[1772] See the Proposed AIR, p. 6.

2. All material and immaterial damages should be remunerated, unless the AV-owner can prove *force majeure* of the victim, which may lead to a reduction of the remuneration-obligation. Force majeure may exist in case of gross negligence of the victim, which could consist of the deliberate failure to install a safety-critical update, or the intentional modification of the AV(-components) including its software;
3. In order to underpin a *force majeure* defence, the AV-owner may claim access to log-files which are to be kept by the producer on the basis of the recommended logging-by-design obligations that need to be implemented in the PLD, as illustrated in section 9.4.2.
4. A lawful basis for personal data processing should be created to enable access to, and the processing of personal data in those log files, in terms of article 6(1)(c) GDPR.

As described in section 8.2.3, implementing the aforementioned recommendations may likely improve *legal certainty, risk* and *trust*, whereas the level of *stringency* would remain acceptable. It is important that in the regulatory process *flexibility* of the regulation to be instituted is maintained.

In this respect, it is relevant to briefly reflect on the civil liability regime for AI proposed by the European Parliament. As stated, the EP Proposal seeks to provide *sui generis* liability rules for AI-systems in general, although without prejudice to additional liability claims for instance on the basis of traffic liability rules.[1773] The Proposal introduces *inter alia* strict liability for high-risk AI-systems operators. A certain overlap between the proposed rules and the (to be improved) traffic liability regime is likely. It is the question how these would – and should – relate. Although it is likely that AVs qualify as "high-risk AI-systems", this does not explicitly follow from the current text of the proposal, whereas these had been listed as such in a previous edition.[1774] From a material point of view, in order to establish liability on the basis of the EP-proposal, victims may likely be required to prove *causation*, which can be burdensome as illustrated in section 7.3. That would imply less improvement of the factors *risk* and *trust* for consumers, as well as less improvement of *legal certainty* for innovators than would be the case when the recommendations above are implemented. Furthermore, the Proposal does not indicate when *force majeure* defence might be invoked. The recommendations regarding force majeure above would implicate more *legal certainty* for innovators regarding this aspect.

Privacy rights must be carefully obeyed, and in a dialogue between public regulator and participants in the sector, it should be investigated how a "blockchain"-like solution, or

[1773] European Parliament 2020a, Article 2(3).
[1774] See European Parliament 2020, Annex I, which lists "Vehicles with automation levels 4 and 5 according to SAE J3016"

comparable technology, could be implemented in order to ensure the availability, integrity and confidentiality of the logged data.

Furthermore, the new traffic liability rules to be regulated, should be accompanied by appropriate liability insurance. This could be regulated (again following a co-regulatory approach, which is also suggested in the EP Proposal),[1775] in a way comparable to the mandatory no-fault insurance as elaborated in section 9.3, be it that this type of insurance is dependent on the establishment of liability of an AV-owner. Also here, an obligation to pay out may be limited in case of deliberate failure of installing safety-critical updates, or intentionally modifications to the AV by the insured AV-owner. Differently from the mandatory no-fault insurance mechanism, there should be no caps on the amounts to be remunerated, in order to ensure that victims do not *risk* underpayment. Regulation of this form of liability insurance, may profit from the 'lessons learned' in the course of the second route, as elaborated above.

9.4.4 PRIVACY

Clarification

In order to implement the recommendations made in section 8.2.4 regarding the necessary clarification of the norms, no new regulatory instruments would have to be drafted: the layered and *flexible* framework that is already provided by GDPR should suffice to improve the *factors*. The necessary clarification can be achieved as follows.

Besides the recommended creation of two "legal obligations" to process personal data in product-[1776] and traffic liability rules,[1777] by means of "logging-by-design" for purposes of (defence against) liability claims,[1778] it should be clarified, preferably using co-regulatory instruments including for instance the (private actor) drafting and (public actor) approval of codes of conduct,[1779] or when this turns out to be unfeasible, through further EDPB guidance:[1780]

1. When controllers may have a legitimate interest regarding the deployment of Accident Prevention and Registration Systems (APRS) for Product- or Traffic Liability Purposes (PTL Purposes), which include logging-by-design functionality;
2. Under which conditions Technical and Organisational Measures (TOMs) will likely be appropriate in order to secure data processing through APRS for PTL Purposes, where **blockchain-like techniques** deserve special attention. In that regard, it can be argued

[1775] See recitals 22 and 23.
[1776] See section 9.4.2.
[1777] See section 9.4.3.
[1778] This may provide for a lawful basis within the meaning of article 6(1)(c) GDPR.
[1779] See section 5.2.7.4.
[1780] See section 5.2.7.4.

that the EDPB Guidelines 01/2020 should in general be used as "minimum threshold" for TOMs to be implemented,[1781] although they would need to be specified further for APRS applications, and also regarding the use **blockchain-like techniques** for the non-manipulable storage of AV-data outside the respective vehicles (see furthermore the following sections);

3. To what extent for PTL Purposes, special category data may be processed under the exception to the general processing-prohibition as stipulated in article 9(2)(f) GDPR, for "the establishment, exercise or defence of legal claims", and which TOMs must be observed as indicated in the previous point;[1782]
4. Which criteria apply to Data Privacy Impact Assessments specifically for APRS-applications for PTL Purposes;[1783]
5. Which specific privacy-by-design and privacy-by-default principles must be implemented within APRS to be used for PTL Purposes (which will overlap with the points regarding TOMs and blockchain-like solutions to a certain extent – as this concerns *inter alia* the processing of AV-data as much as possible within the vehicles, and the (by default) limited storage (periods) of AV-related data, as illustrated the following sections);

New international arrangements

It is a task for European politics, and thus the public regulator, to reach new agreements with *inter alia* – and perhaps most importantly considering the fact that many data-driven services are provided by US based companies – the United States of America in order to effectively re-legalise the export of personal data from EU-citizens to processors or controllers vested under the laws of the US. This is not only relevant for AV-innovation, but more broadly for the effective functioning of the data-driven economy as a whole. In the following section, I shortly reflect on a potential approach for re-enabling the personal data flows between the EU and the US.

Introducing procedural aids

Procedural aids regarding norm violation, causation and damages, could best be introduced by the European legislator, in the form of some (slight) adaptations of the text of the GDPR. Following the better regulation principles, the (private) stakeholders should be able to provide input in the regulatory process, at least by being able to respond to the proposed alterations regarding norm violation and causation. More involvement of the private stakeholders, i.e. at least including the

[1781] See section 5.2.7.1.
[1782] This is not included under the scope of article 40 GDPR, which implicates that clarification of the exception to the special category data processing cannot be achieved through a code of conduct.
[1783] Also regarding this point, EDPB guidance is necessary, as PIA's are not brought under the scope of article 40 GDPR.

insurance sector, AV-(component) producers, insurance associations, consumers- and victims associations would be necessary for the institution of "standardised" lists of (material and immaterial) damages that may be remunerable "by default" after a norm-violation took place.

The introduction of a **lawful basis, and lifting the special category data processing** for the processing of personal data for Product- or Traffic Liability Purposes (PTL PURPOSES) through Accident Prevention and Registration Systems (APRS), could detriment the informational privacy protection of AV-users, as this would enable "new" forms of personal data processing – and thus negatively impact *trust* and *risk* of *consumers*. However, it can be argued that such forms of data processing are (still) necessary in order to be able to defend against a (product) liability claim – which would be beneficial from the *innovators perspective*. Furthermore, these forms of data processing can at the same time positively influence *risk* and *trust*, when such a provision is accompanied by a logging-by-design obligation, and the obligation to provide access to those data for *consumers* who seek remuneration after an AV-related accident, and who need to underpin their claims with proof that can be obtained from the logged (personal) data.

Regarding the **clarification** recommendations indicated above, it is suggested that, from a regulatory perspective, EDPB guidance and/or codes of conduct could be used, in line with the layered rules-regime instituted by the GDPR. First of all, it should be noted that codes of conduct can in principle be used for the clarification of all the indicated points, except for DPIA's, and the exception to the generic prohibition to process personal data in case of (defence against) legal claims.[1784] The competence of the EDPB to provide "guidelines, recommendations and best practices in order to encourage consistent application" of the GDPR, is not limited to those topics.[1785] However, it can be argued that codes of conduct are to be preferred over EDPB guidance in principle, for several reasons. Firstly, codes of conduct may provide the necessary clarification, as it is explicitly regulated in article 40(1) GDPR that through these instruments *specification* of the norms listed under 40(1)(a-k) GDPR may take place,[1786] whereas the EDPB may in principle only generally *explicate* the respective norms to be improved from the perspective of this study.[1787] Secondly, drawing up a code of conduct cannot go without the involvement of the relevant stakeholders (i.e.: "[a]ssociations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of

[1784] See article 40 GDPR.
[1785] Article 70(1)(e) GDPR.
[1786] Which thus includes all the points to be clarified in sense of my recommendations in the foregoing section, except for DPIAs and the generic prohibition personal data in case of (defence against) legal claims.
[1787] The EDPB competence to provide further specifications, is limited to those norms listed under article 70(1)(f-k; and p), which do not include the norms to be clarified in sense of my recommendations as illustrated in the previous section.

specifying the application of this Regulation"),[1788] whereas the EDPB only has to consult the respective stakeholders "consult interested parties and give them the opportunity to comment within a reasonable period" where "appropriate",[1789] which appropriateness is not further specified there: the EDPB seems to have a rather broad margin of appreciation there.[1790] As stated, involvement of actors including at least AV(-component) producers, and consumers associations is mandatory in order to seek maximum awareness and acceptability of the (to be specified) norms by *innovators*, which would in turn be beneficial in terms of consumer *trust* that their privacy rights are duly observed. Thirdly, EDPB guidelines, recommendations or best practices may implicate less *legal certainty* than codes of conduct could. EDPB clarifications, which could in theory be drafted without stakeholder involvement, may be more easily overturned by a court than codes of conduct, especially when such codes have been approved by the DPA's and where applicable the EDBP,[1791] and have gained "general validity" upon an decision by the European Commission.[1792]

This third point however also reveals the "Achilles heel" of the codes of conduct as a regulatory instrument under the GDPR. As indicated in section 5.2.7.4, to date only 3 codes of conduct have been approved, and neither of those is relevant for the AV-sector. As Blok observed, under the GDPR's predecessor (the Data Protection Directive), "[l]little use has been made of the approval procedure because data controllers considered it a 'tortuous' procedure, ie too lengthy, too time consuming and too expensive".[1793] Under the GDPR, the procedure has changed to a limited extent, but, as Blok also observed, it is not likely that this procedure will be broadly used, and to the extent that is will be used, the instrument forms a disincentive for necessary adaptations when technology progresses, due to its complexity.[1794]

Thus, for the mechanism regarding codes of conduct to become more efficient (and *flexible*), it would be necessary to improve the usability, to decrease the costs and the length of the procedure. In line with Blok's observation that the approval-procedures in their current form are rather a race against the authorities who primarily examine "the legality of the codes in full",[1795] it can be

[1788] Article 40(2) GDPR.
[1789] Article 70(4) GDPR.
[1790] However, as Blok observed, the EC urged the EDPB to improve its transparency. See Blok 2020, p. 115, referring to European Commission, "Report from the Commission, First Report in the Implementation of Directive 95/46/EC", COM(2003) 265. Also, the EC later "emphasised the importance of public consultation before the guidelines are finalised": Blok 2020, p. 107, referring to European Commission, "Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018", COM(2018) 43 final.
[1791] See article 40(5-8) GDPR.
[1792] See article 40(9) GDPR.
[1793] Blok 2020, p. 113, and his reference to Korff, D., "EC Study on Implementation of Data Protection Directive 95/46/EC" (2002), p. 187.
[1794] Ibidem, p. 113-114.
[1795] Ibidem, p. 113.

recommended that a bottom-up approach is followed, in which the stakeholders are actively stimulated (also in terms of budget) to codify their "best practices" in conduct-rules (such as the VDA and the ACEA-principles,[1796] which are checked on a more marginal basis against the generic GDPR provisions by the authorities.[1797] Thus, approved codes of conduct would in theory form a better basis for the necessary clarification of the reviewed norms than EDPB guidance where possible, although the approval procedure needs to be optimised for innovators in order to render it (more) effective. Regarding both instruments, it must be noted that it remains necessary that the specified rules are regularly updated,[1798] in order to keep their relevance, and their *flexibility*, which is beneficial in terms of *legal certainty* – and thus *trust* that personal data are and will remain to be processed in conformity with the specified rules.

In line with the recommendation to clarify under which conditions logging-by-design can be implemented, and how the security of the data processing activities through for instance APRS mechanisms can be deemed in line with the obligation to implement appropriate TOMs, it is relevant to assess how **blockchain- or similar solutions** could be used. As also underscored by the Expert Group,[1799] it is of the utmost importance that AV-data which are stored *inter alia* for purposes of reconstructing AV-accidents and to determine liability, and blockchain technology may contribute thereto. However, it had been observed that it is hardly possible to ensure data subject's rights when the currently available blockchain technology is deployed.[1800] In order to seek a solution for this problem, it can be suggested that the public regulator institutes a so-called *regulatory sandbox*. Regulatory sandboxes have *inter alia* been used in the FinTech-sector.[1801] Regulators instituted a "real life" testing environment for innovators in a controlled setting, under direct supervision of the authorities in order to verify under which conditions innovative products or services could be deployed into society.[1802] Testing of the innovation could be done within such a sandbox with "fewer regulatory constraints, less risk of enforcement action and ongoing guidance from regulators".[1803] On the one hand, it can thus be investigated how an innovative product or service could be brought in compliance with the rules, whereas on the other hand it can be examined how those rules should be adjusted in order to (better) fit the type of

[1796] See ACEA 2015; VDA 2014; VDA & German DPAs 2016; and also the CCAV 2017-principles.
[1797] Ibidem.
[1798] Article 40(2) GDPR already contains an "update mechanism" for codes of conduct.
[1799] European Commission 2020, p. 47.
[1800] See further section 9.4.4.
[1801] See for instance https://www.cgap.org/blog/series/regulatory-sandboxes-what-have-we-learned-so-far; see also the Proposed AIR, which contains a sanbox-mechanism.
[1802] See also https://www.afm.nl/nl-nl/professionals/onderwerpen/innovationhub-maatwerk;
[1803] See Allen, H.J., "Regulatory Sandboxes", The George Washington Law Review 2019, vol 87:579, p. 580, referring to Zetsche, D.A. et al., "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", 23 Fordham Journal of Corporate and Financial Law, 2017 vol. 23, (Zetsche 2017) p. 31-103.

innovation.[1804] The Proposed AIR recommends the establishment of AI regulatory sandboxes too. In those sandboxes, Member States, or the European Data Protection Supervisor should set up a "controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time".[1805] A plan should me made (and executed) in order to investigate the functioning of the AI-technology to be deployed on the market, in view of the compliance obligations under the proposed new AI-rules.

The sandbox-approach proposed in the AIR is 'one-directional' in the sense that it sees to getting innovative AI technology compliant with the applicable rules. A bi-directional sandbox can be (more) meaningful for blockchain- and similar technology to be applied in AVs. In a bi-directional setting, the regulator too could learn from the technological innovation, and could implement the measures in order to remain relevant for developing technology. This implicates that it would not only have to be investigated how the technology could be brought in compliance with the GDPR, but also how the GDPR might have to be adapted in order to facilitate the development and deployment of blockchain- and similar innovations, instead of precluding it, as the current rules would. Although, the main objectives (including those regarding strong personal data protection, the free flow of personal data within the Union and facilitating technological developments)[1806] should not be lost out of sight. More concretely, I recommend a dialogue between the EU regulator and private actors including at least AV(-component) developers, insurers and victims(/consumer) associations. In that dialogue, it should be investigated:

- to what extent the currently available technology and/or the applicable rules may be adjusted, in order to ensure the "integrity, availability and confidentiality" of the logged data, as well as maximum personal data protection, i.e. for instance through ensuring that a minimum amount of personal data is processed. This might be achieved through ensuring that data are only "exported" onto blockchain-like data storage systems when these regard AV-accidents. This could for example be limited to the data (triggered by the deployment of an airbag for instance) captured in the moments just before, during an accident;
- for which period of time such data should be processed, which should be limited "by default" to a short period of time, after which the respective data are erased. The erasure could perhaps be prevented, when an actor (including a data subject) requests to keep the data;

[1804] See Zetsche 2017, p. 52-53; also https://www.bbva.com/en/what-is-regulatory-sandbox/.
[1805] Article 53(1) Proposed AIR.
[1806] See section 5.2.2.

- in which cases aggregated or pseudonymised data can be processed (for instance outside the respective vehicles), and in which cases "personal data in the clear" must (still) be used (for instance inside the respective vehicles); and
- how personal data can only be accessed and/or altered by, or with consent of the data subjects.[1807]

In order to investigate which technological applications can be feasible (or not), taking account of the current GDPR norms, a regulatory sandbox could prove to be an ideal "living laboratory" for improving both the technology and the applicable rules.

With regard to the **introduction of procedural aids** for victims of damage resulting from GDPR norm-violation, the following should be noted regarding the involvement of (private) stakeholders[1808] in the regulatory process with regard to the drafting of standards for damages to be remunerated. Not only may involvement of those actors throughout the regulatory process (including the frequent evaluation thereof) contribute to the acceptability of these rules by the *innovators* to whom these shall apply, also *trust* may benefit when (potential) victims are involved in the conceptualisation of standardised damages indications, which likely reduces uncertainty regarding the question if, and to what extent their (immaterial) damages are compensable under the GDPR.[1809]

How **new, compliant international arrangements** should be made cannot be indicated easily. As observed in the *Schrems I & II*-rulings,[1810] it will, among other things, be necessary that the US shall institute better safeguards for the protection of the informational privacy of EU citizens, and that data subjects are equipped with better instruments to enforce their rights for instance against US authorities in order to comply with the GDPR-norms. Alternatively, the bar for personal data protection should be lowered significantly by the EU regulator. That would however not be advisable from *inter alia* a *trust* perspective, as that implicates admitting to a lower level of privacy protection regarding 'exported' personal data. Perhaps, a compromise could be sought, in which at least better safeguards for the informational privacy rights of EU citizens can be agreed than the actual status quo. While it might be complicated to arrange that US intelligence organisations more diligently (ex-ante) observe the informational privacy rights of EU citizens in the near future, it can for instance be envisaged that EU citizens are equipped with (more) effective rights to

[1807] See further section 9.4.4.
[1808] As illustrated in the previous section: these should at least include AV-(component) producers, insurance associations, consumers- and victims associations.
[1809] See also Walree 2021, p. 167-169. He recommends to introduce a system of lump sum damages for certain "substantial" GDPR-infringements, which sees to cover both material and immaterial damages. He expects that "damage scheduling" would have a positive effect on (civil) enforcement of the GDPR.
[1810] See section 5.2.9.

control their data after export to the US, and after (potentially) being subjected to inspection by US intelligence organisations. Therefore, it can be imagined that the ombudsperson which was installed under the Privacy Shield, is placed outside the supervision of the intelligence agencies, and will be endowed with powers enabling *inter alia* the exercise of the access-; rectification- and erasure rights of EU-citizens, and to correct other violations of the GDPR-rules by the US agencies.

9.5 CONCLUSION

There are several ways to improve the factors as recommended in Chapter 8, requiring different kinds of regulatory intervention. I sketched three possible routes, from three different angles. Firstly, I sketched a "bottom-up" approach where improvements are initiated by the industry itself, to be mandated by the public regulator in the form of binding industry codes of conduct. Secondly, it was investigated how mandatory insurance could contribute to *factor* improvement. Thirdly, it was illustrated how the *factors* could be improved in the most tenable way, by means of adaptation of the currently applicable rules within the currently applicable frameworks. It has been observed that the third option would eventually be the preferrable one, although significant regulatory efforts from both public (EU)- and private actors will be required, and overall the third option would likely be the most complex. Therefore, I suggested that regulatory work regarding all three options should start simultaneously in order to realise the desired *factor*-improvements, and in order to prevent unnecessary waiting as much as possible and thus a time-spill for reaching the eventually desirable, durable end-results. Regulating the third solution can profit from the "lessons learned" from for the first and second improvement routes.

Binding industry codes that would see to the "unreserved" acceptance of liability by AV-producers would solve the most acute risk of under-compensation of AV-accident victims (affecting *risk* and *trust*), and would preclude the need for unlimited (personal) data storage for potential underpinning of (defences against) liability claims (which may improve *trust* regarding the privacy aspect). Also, such a general rule could lead to *legal certainty* for innovators. However, it entails several other problems. Accepting full liability, without nuances in terms of defences, apportionment and redress, likely implicates higher remuneration obligations than strictly necessary, which implicates avoidable *stringency*. While liability-acceptance could for instance be an option for large players in industry, this could prove burdensome for smaller companies. Furthermore, the "underlying problems" in the regulatory frameworks remain intact.

Mandatory insurance, leading to compensation of all victims of accidents in which AVs are involved, irrespective of fault or risk-liability, could relieve the most urgent *risks* of under-compensation, and could imply high *legal certainty* for innovators. This could in turn be beneficial for *trust*, especially when this would decrease the need to process personal data (for procedural purposes). Furthermore, I observed that mandatory insurance does not necessarily provide

incentives for producers to make their technology as safe as possible when remuneration-obligations are "outsourced" to insurers – which would not be beneficial in terms of *trust*. When, as suggested, also producers would need to take out a special insurance on the basis of the recommendations, this could implicate *stringency* for innovators, especially when there are no insurance products readily available or when the premiums are very high (due to expected high, or false, claims). These issues could be reduced when the compensation amounts are capped. To determine those caps (and to keep them aligned with the technology and the risks the technology poses), close co-operation is suggested between the public regulator and the private actors including insurers, AV-producers, consumer- and victims associations. However, as damage caps may lead to the situation that not all damages are remunerated under the mandatory insurance scheme, as well as for redress-purposes between potential tort-feasors, it remains relevant to improve the *factors risk* and *trust* in the (liability) frameworks that should see to the compensation of the (remaining) damages. Also from a principle point of view, adaptation of the current traffic liability frameworks in combination with a mandatory insurance schemes (which is also advocated by the European Parliament in its recent Proposal) may be preferable over the sole institution of a mandatory insurance scheme *without* adapting the traffic liability rules.

Eventually, the most straightforward option to execute the recommendations regarding optimisation of the *factors* as proposed in section 8.2, will be to **implement the required adaptations within the regulatory regimes themselves** in order to maintain the relevance of the respective frameworks also in the context of advancing technology. When following this third regulatory route towards improvement of the respective *factors* that deserve most attention, it remains important to involve the stakeholders throughout the process, in order to maximise the relevance of the adapted rules, *legal certainty*, as well as to ensure compliance by the regulatees, which is in turn beneficial for *trust*. Furthermore, in terms of *flexibility*, it is important to build in mechanisms that allow for adaptation of the norms when societal or technological progress would demand so, and that regulatees are left with freedom of choice where it regards compliance.

SUMMARY

This research started from the hypothesis that the currently applicable regulatory frameworks on extra-contractual liability and informational privacy, can influence innovation in the field of Autonomous Vehicles, and that these frameworks do not, in their current forms, provide for optimal conditions for innovation. In the nine Chapters above, this hypothesis was verified, in three parts, that revolved around this main question:

Which factors in regulation may influence innovation in the field of autonomous vehicles in the EU, how do the regulatory frameworks on extra-contractual liability and personal data protection encompass these factors, and how could these factors in the regulatory frameworks be optimized in order to improve the conditions for innovation and acceptance by citizens of AV-technology?

FIRST PART: IDENTIFIED *FACTORS*

The first part had as its goal to *investigate whether or not a set of factors can be identified from academic literature that can be used to assess the possible influences of regulation on innovation in general, which in turn can be applied to the frameworks on extra-contractual liability and informational privacy*,.

In Chapter 3, two perspectives were identified from which I distilled innovation-influencing *factors* which have been used in this study. From the ***innovators*** perspective, these are *legal (un)certainty; flexibility* and *stringency*. *Legal certainty* can impact investments in innovation. When it is difficult or impossible for innovators to reasonably foresee and to calculate risks that may result from a regulatory framework that applies to the development and deployment of novel technology, a negative impact on investment decisions can be predicted. *Stringency* relates to the need for innovators to adapt their behaviour (or technology) in order to comply with regulation. Such changes are particularly evident when new regulation is introduced, which necessitates a behavioural (or technological) change by innovators. Furthermore, when regulation requires upfront compliance efforts for new market players, this could also entail *stringency*. Two aspects of *flexibility* can be found in regulation which may influence the development and deployment of innovation. First, when regulation necessitates certain ex ante compliance, it would be better for innovation when innovators have more manoeuvring space to reach compliance than when the implementation paths are limited. Second, rules that are adaptable to (technological) change and thus as technology neutral as possible, are, from a innovation-stimulating perspective, preferred over technology specific rules, which are less adaptable to changing circumstances.

From the ***consumers*** *perspective*, the factors *risk* and *trust* were identified. It was found that it may negatively impact the adoption of novel technology, when that technology – and the rules that apply thereto – results in (financial and other) *risks* for consumers. *Trust* is, besides the *risk*-factor, important for the acceptance of a novel technology by consumers. Trust regarding *inter alia* the safety of a product is found to be necessary for adoption of technology, as would be trust in the "reparative capacities" of for instance a liability framework when victims suffered damage due to a (nonetheless) unsafe product, and the trust that fundamental rights (including privacy and personal data protection) are well-observed.

The two perspectives are interrelated, as consumer acceptance (which can be "fuelled" when risks are low, and consumer trust is high) is crucial for the uptake, and thus the successful deployment of innovation.

SECOND PART: ASSESSED *FACTORS* WITHIN THE STUDIED REGULATORY FRAMEWORKS

The second research goal related to assessing to what extent the regulatory frameworks on 1) extra-contractual liability and 2) personal data protection that are applicable in the European Union, may influence innovation in the field of Autonomous Vehicles in the EU, in terms of the *factors* identified in this study.

According to the case study introduced in section 3.5, *legal certainty, risk* and *trust* received the "lowest scores", according to the scoring method introduced in section 7.1. This indicates that especially those *factors* should not be overlooked when seeking to improve the conditions for innovation and acceptance in the field of AVs.

Increased autonomy in vehicles leads to increasing *uncertainty* regarding the origination of damage. Establishing where damage originates is crucial in order to assess, among other things, *defectiveness* under the product liability regime and the Dutch regime regarding defective goods in possession, and to assess *fault* under the (generic) liability rules in The Netherlands and (to a certain extent) England, which are necessary to establish a norm violation, which is in turn necessary for establishing liability. These uncertainties also implicate the establishment of causality between a norm violation and damage, which is relevant under all studied regimes. This is problematic for victims who seek compensation, but also for innovators seeking to rely on a (contributory negligence) defence. It is furthermore often uncertain when (non-)compliance with the GDPR-norms can be established, as a result of the openness of these norms, and a lack of guidance.

Those *uncertainties* mainly affect *consumers* when they suffered damage related to the deployment of AVs. In effect, victims will not be able to get damage compensation should they fail

to establish *defectiveness*, *fault* or other *norm violations, damage* and *causality*, while innovators are in a better position to control the damage-inflicting risks inherent in AV-technology than consumers. The studied frameworks, seem to make it in their current form, uneasy for consumers to hold the respective innovators liable when such risks materialise. This implicates a high *risk* of unrecoverable damages for victims of AV-related accidents. Besides, especially regarding the product liability framework, and the traffic liability frameworks of The Netherlands (with the exception of article 185 WVW) and to a smaller extent England, it is stated that the studied frameworks do not optimally serve the victim's interests in terms of the *consumers perspective*. Moreover, when it is hard for victims to recover damages, this negatively impacts their *trust* in the safety of AV-technology and the fair distribution of risks. The low *risk* and *trust* scores can be stated to negatively impact the acceptability of AV-technology, and therefore the uptake by consumers. In turn, this is also not beneficial from the *innovators perspective*, as technology-uptake is also crucial for successful innovation.

At the same time, and despite the indicated *uncertainties,* the fact that innovators cannot be held liable easily (without procedural aids), results in the absence of *stringency* in (most of the) studied liability frameworks. There are little (AEVA 2018) or no (the other regimes) upfront costs involved for innovators in order to comply with the extra-contractual liability norms.

As it stands, large-scale personal data processing is a logical consequence of the currently applicable extra-contractual liability rules. Data are necessary in order to either underpin a liability claim *or* a defence thereto, more specifically under the product liability regime, and the traffic liability regimes of The Netherlands (excluding 185 WVW) and England. This 'triggers' the applicability of the data protection framework.

It was concluded that the GDPR entails *stringency* for innovators. It presents innovators with a high ex-ante compliance burden, and could implicate hefty penalties and liability risks in case of non-compliance. Also because the open norms are often too unclear (*uncertainty*) and sometimes even prohibitive for AV-innovators, whilst non-compliance can be enforced through hefty administrative sanctions and extra-contractual liability, this framework must even be considered unnecessarily *stringent*. The GDPR furthermore might not live up to its aim to create *trust* among consumers. As long as it is *uncertain* how AV-innovators can reach compliance, consumers cannot *trust* that their informational privacy is well protected. These uncertainties may have a similar impact on *risk*. *Risk* is furthermore negatively impacted due to the circumstance that it will be difficult to hold a non-complying innovator liable on the basis of the GDPR-regime.

THIRD PART: IMPROVING THE *FACTORS*

The third and ultimate goal of this research was is to make recommendations that seek to create better conditions for innovation (regarding both the *innovators*- and the *consumers* aspects) in view of the ambitions of the European Union on better regulation of innovative technology.

I distinguished between material recommendations, relating to the question which aspects of regulation could be improved, and formal recommendations, indicating how such improvements might be regulated.

The recommendations regarding which aspects to improve, include the following:

Product liability framework

1. The products definition should be adapted resulting therein that also software 'as such', thus irrespective of its relation with hardware, is brought under its scope.
2. It needs to be clarified which safety level may reasonably expected regarding AVs; it is recommended that "beyond excellent human driving skills" forms the minimum threshold for determining defectiveness of an AV.
3. Post-marketing obligations for AV-producers need to be introduced in order to keep AV-(component)s safe after they have been sold (or otherwise made available) to consumers. This implicates *inter alia* that safety and (cyber)security updates should be provided during a certain period.
4. In line with the post-marketing obligations to be introduced, the later-existence defence and the development risks defence should not apply, at least not in those cases when producer did not comply with his post-marketing obligations. However, producers must remain to be able to invoke a contributory negligence defence.
5. Introduce procedural aids for victims of (allegedly) defective AVs regarding defectiveness, and the causal relationship between defect and damage, from both a procedural and a material view.
    a. In the procedural sense: relieve the burden of proof by regulating a (rebuttable) presumption of defectiveness when an AV is involved in an accident, and assume a (also rebuttable) causal relationship between defectiveness and damage.
    b. In material sense: regulate logging-by-design obligations for AV (component) producers that enable the reconstruction of events (including automated decisions) prior to and during the accident, with the obligation to provide the logged information to victims. Failing to log, or to provide relevant, understandable, information should lead to reversal of the burden of proof regarding defectiveness, damage and causation.

These measures see to the improvement of the *legal certainty, risk* and *trust* factors, and in general terms to the "re-alignment" of the product liability rules in view of the purpose to effectively compensate victims of damage caused by defective products. Unnecessary *stringency* should however be avoided. Therefore, among other things the *contributory negligence* defence should still be applicable.

Traffic liability framework

1. It should not be necessary for victims (irrespective of their "capacity" as driver, passenger or external (non)motorised victim) to prove fault or defect attributable to an AV deployer, in order to establish liability. The involvement of an AV in an accident, should suffice to allocate liability of the deployer of the vehicle (i.e. for example its owner).
2. In principle, 100% of the damages resulting from an accident in which an AV was involved should be remunerable, unless *force majeure* can be proven, which may in turn lead to a reduction of damages to be remunerated. Force majeure may include, besides "inexcusable fault", gross negligence at the side of the victim. Gross negligence could exist in situations in which the victim intentionally failed to install safety-critical updates, or where the victim modified the AV's software.
3. In order to underpin a potential force majeure defence, it may be necessary to acquire and analyse AV- and accident data, which must be available for the defending AV-deployer. Therefore, it should be regulated that logged information (which should be available due to the "logging-by-design" obligations to be introduced for producers) should be made available both to the defending AV-deployers, and to the victims who seek compensation.

Risk and *trust* should profit from the implementation of the recommendations. Legal *certainty* could also benefit from the suggested changes, as foreseeability and calculability of the liability risks for innovators would improve compared to the current situation. It can be argued that increased *legal certainty* may be beneficial from an *innovators perspective*, even when this potentially leads to increased *stringency*. A force majeure defence should be possible in order to prevent unnecessary *stringency*. It is my estimation that the conversion of fault liability rules into strict liability rules in case of AV-accidents does not have a significant impact on *stringency*, where strict liability has traditionally also been used to establish traffic liability.

Personal data protection

1. Clarification is necessary of the following GDPR-norms:
    a. Lawfulness of personal data processing for the purposes of establishment (by victims) of and/or defence (by innovators) against a traffic- or product liability

claim. This entails that there should both be a clear lawful basis to process personal data (for the stated purposes, hereinafter referred to as Product- or Traffic Liability Purposes, or PTLP, for by the means of an Accident Prevention and Registration System (APRS)), as well as an exception to the general prohibition to process special category data such as geolocation data and personal (driving) preferences, in such a way that explicit consent of the data subjects is not required.

   b. Data Protection Impact Assessments (DPIAs); it should be clarified when "high risks" remain after carrying out a DPIA, in which case the respective Data Protection Authority must be consulted before respective data processing activities with regard to PTL PURPOSES by means of an APRS may take place;
   c. Technical and Organisational Measures (TOMs); it should be clarified when the necessary appropriate TOMs have been implemented for personal data flows by AV-innovators, for PTL PURPOSES, by the means of an APRS;
   d. Privacy-by-design & privacy-by-default (PBD); it should be clarified when the PBD-obligations can be considered fulfilled by an AV-innovator who is to implement an APRS for *inter alia* PTL PURPOSES.

2. A solution should be found that would enable the decentralised storage of AV-(accident) data for PTL PURPOSES, using blockchain- or similar technology, which allows for the exercise of the rights of data subjects, either by changing the respective GDPR-norms, or adapting the technology in such a way that data subjects rights can be effectuated.
3. International transfers of personal data for PTL PURPOSES for instance through APRS, mainly between the EEA and the US should be effectively possible. The current political dead-lock situation after the *Schrems II*-ruling of the CJEU must be resolved, in order to re-enable the standing practice of data-exchange between the continents, whilst the rights regarding personal data protection of EU-citizens must be respected.
4. Procedural aids for victims of (alleged) GDPR-violation by AV-innovators (as *controllers*) should be introduced, as well as regarding the causal relationship between defect and damage, through rebuttable presumptions (at least) when controllers do not comply with their ex-post obligations regarding the execution of data subject's rights; when a personal data breach occurred, or when otherwise damage occurred after a GDPR-norm violation has taken place; and it should be clarified when and which immaterial damages qualify for remuneration under the GDPR-liability provisions.

It will be a complex puzzle to improve all *factors* and thus optimize the conditions for innovation and acceptance. Optimizing *legal certainty* for AV-innovators as a starting point, implicates that it gets easier to understand the compliance-obligations, and calculate their enforcement risks in case of non-compliance. In turn, this could implicate that the norms are better observed by

innovators, which may lead to improved *trust*. However, improving *legal certainty* will not resolve all of the indicated challenges. Therefore, it has *inter alia* been suggested that international transfers of personal data are re-legalised, that is must be examined how blockchain-technology can be brought in compliance with the GDPR (which would both lead to less *stringency*), and that procedural aids for consumers are introduced, in order to improve *risk* and *trust*.

There are several ways to improve the factors, requiring different kinds of regulatory intervention. I sketched three possible routes on how to implement the material recommendations, from three different angles. Firstly, I sketched a "bottom-up" approach where improvements are initiated by the industry itself, in the form of **binding industry codes of conduct** to be mandated by the public regulator. Secondly, it was investigated how **mandatory no-fault insurance** could contribute to *factor* improvement. Thirdly, it was illustrated how the *factors* could be improved in the most **tenable** way, by means of **adaptation of the currently applicable rules** within the currently applicable frameworks (instead of the creation of sui-generis rules). It had been observed that the third option would eventually be the preferrable one, although significant regulatory efforts from both public (EU)- and private actors will be required, and overall the third option would likely be the most complex and lengthy. Therefore, I suggest that regulatory work regarding all three options is started simultaneously in order to realise the desired *factor*-improvements, and in order to prevent unnecessary waiting as much as possible and thus a time-spill for reaching the eventually desirable, durable end-results. Regulating the third solution can profit from the "lessons learned" from for the first and second improvement routes.

Binding industry codes that would see to the "unreserved" acceptance of liability by AV-producers would solve the most acute risk of under-compensation of AV-accident victims (affecting *risk* and *trust*), and would preclude the need for unlimited (personal) data storage for potential underpinning of (defences against) liability claims (which may improve *trust* regarding the privacy aspect). Also, such a general rule could lead to *legal certainty* for innovators. However, it entails several other problems. Accepting full liability, without nuances in terms of defences, apportionment and redress, likely implicates higher remuneration obligations than strictly necessary, which implicates unnecessary *stringency*. While liability-acceptance could for instance be an option for large players in industry, this could be too burdensome for smaller companies. Furthermore, the "underlying problems" in the regulatory frameworks remain intact.

Mandatory insurance, leading to compensation of all victims of accidents in which AVs are involved, irrespective of fault or risk-liability, could relieve the most urgent *risks* of under-compensation, and could imply high *legal certainty* for innovators. This could in turn be beneficial

for *trust*, especially when as little personal data are processed as strictly necessary. Personal data might however still have to be processed in order to determine for instance whether or not there had been intentional negligence by the victim who failed to install a safety-critical update, or who modified the AV('s software). Furthermore, it was observed that mandatory insurance does not necessarily provide incentives for producers to make their technology as safe as possible when remuneration-obligations are "outsourced" to insurers – which would not be beneficial in terms of *trust*. When, as suggested, also producers would need to take out a special insurance on the basis of the recommendations, this could spell *stringency* for innovators, especially when there are no insurance products readily available or when the premiums are very high (due to expected high, or false, claims). These issues could be reduced when the compensation amounts are capped. To determine those caps (and to keep them aligned with the technology and the risks the technology poses), close co-operation is suggested between the public regulator and the private actors including insurers, AV-producers, consumer- and victims associations. However, as damage caps may lead to the situation that not all damages are remunerated under the mandatory insurance scheme, it remains relevant to improve the *factors risk* and *trust* in the (liability) frameworks that should see to the compensation of the (remaining) damages. Also from a principle point of view, adaptation of the current traffic liability frameworks in combination with mandatory insurance schemes (which is also advocated by the European Parliament in its recent Proposal) may be preferable over the sheer institution of a mandatory insurance scheme *without* adapting the traffic liability rules.

Eventually, the most logical option to execute the recommendations regarding optimisation of the *factors* as proposed in section 8.2, will be to **implement the required adaptations within the regulatory regimes themselves**, rather than to "regulate around it" by means of sector- or AV-specific rules, in order to maintain the relevance of the respective frameworks also in the context of advancing technology.

Regarding the **product liability** framework, which might best be converted into a regulation, the following (regulatory) suggestions were made:

1. It can be envisaged that a special regime is created for producers of AV(-components), as a *lex specialis* under the general product liability rules. These provisions may (should that appear to be opportune) be extended with producers of other applications containing AI, and adapted when necessary. These provisions should be regulated in close collaboration between the public regulator and private actors, including *inter alia* AV(-component) producers, AV-users, consumer- and victims associations, insurers et cetera, although in conformity with the following principles;

2. It should be regulated that:
    a. Software is included under the definition of *product* in sense of Article 2 PLD;
    b. It is clarified in sense of Article 6(1) PLD that an AV(-component) is defective, when it renders the AV not to encompass those driving skills which can be expected from the most excellent human driver, and when the obligations for the producer under the GDPR are not complied with, regarding personal data that have been generated, stored or otherwise processed by or through the AV;
    c. The defences incorporated under article 7(b) (regarding later-existence) and 7(e) (regarding development risk) PLD, may only be invoked when a producer can prove:
        i. that he provided safety-critical updates, throughout a certain period, in order to prevent or repair (potential) defects in his product, and that the injured person deliberately failed to implement these; or
        ii. that the injured person intentionally modified the AV('s software), which rendered the AV defective;
    d. Article 4 PLD is amended as such that when persons sustained injury after an accident in which an AV was involved:
        i. a defect, the damage and the causal relationship between the defect and the damage are assumed, which assumption can be rebutted by the producer, unless
        ii. the producer failed to provide the injured person access to AV-logs in terms of the following provision, in which case the producer needs to prove that there had been no defect, and that the damage could not have been caused by the defect.
    e. A new obligation is introduced in the product liability rules regarding "logging-by-design". Producers shall implement functionality that logs AV-activity, which enables the reconstruction of the course of events prior to and during an accident, including the automated decisions taken by the AV. These logs should be made available on request of a victim, or on request of an AV-owner in the course of a claims-procedure under the (new) traffic liability rules and/or a product liability claim. The aforementioned logging-obligations as well as the processing of logged information in a claims (settlement) procedure may serve as a lawful basis for personal data processing in sense of article 6(1)(c) GDPR. Privacy should be duly observed (see further below).

The recommendations regarding the **traffic liability framework** should be implemented in an EU regulation, regulating the following principles:

1. The owner of an AV is liable towards victims of accidents in which his AV is involved;
2. All material and immaterial damages should be remunerated, unless the AV-owner can prove *force majeure*, which may lead to a reduction of the remuneration-obligation. Force majeure may exist in case of inexcusable fault, or gross negligence of the victim, which could consist of the deliberate failure to install a safety-critical update, or the intentional modification of the AV(-components) including its software;
3. In order to underpin a *force majeure* defence, the AV-owner may claim access to log-files which are to be kept by the producer on the basis of the recommended logging-by-design obligations that need to be implemented in the PLD, as illustrated in section 9.4.2.
4. A lawful basis for personal data processing should be created to enable access to, and the processing of personal data in those log files, in terms of article 6(1)(c) GDPR.

The improved traffic liability rules should be accompanied by appropriate liability insurance. This could be regulated (again following a co-regulatory approach, which is also suggested in the EP Proposal) in a way comparable to the mandatory no-fault insurance as elaborated in section 9.3, be it that this type of insurance is dependent on the establishment of liability of an AV-owner.

The improvements in the **personal data protection framework** could be regulated as follows:

Clarification of the indicated norms should be done through sector-specific codes of conduct, and where necessary through EDPB guidance. From a *legal certainty* perspective, codes of conduct are to be preferred over EDPB guidance. However, it is likely that the codes-of-conduct-instrument is in its current form too unattractive for the necessary private actors (including for instance AV-producers, consumer- and victims associations and insurers) to participate. Therefore, *inter alia* the costs and length of the procedure to get approval needs to be improved. In that, a bottom-up approach is recommended, in which the stakeholders are actively stimulated (also in terms of budget) to codify their "best practices" in conduct-rules, which are checked on a more marginal basis against the generic GDPR provisions by the authorities.

In line with the recommendation to clarify under which conditions logging-by-design can be implemented, and how the security of the data processing activities through for instance APRS mechanisms can be deemed in line with the obligation to implement appropriate TOMs, the establishment of a regulatory sandbox for blockchain or similar solutions is recommended. In that, it can be investigated how the technology could be brought in compliance with the GDPR, and at the same time it can be examined how the GDPR might have to be adapted in order to facilitate the development and deployment of blockchain- and similar innovations, instead of precluding it, as the current rules would.

The introduction of procedural aids for victims of damage resulting from GDPR norm-violation, should be done within the GDPR-norms, whereby reference can be made of standards for damages to be remunerated. These standard need to be drafted in close collaboration between *inter alia* AV-producers, consumers- and victims associations and insurers.

It is a task for the public regulator to make new international arrangements *inter alia* with the United States in order to re-legalise the exchange of personal data between the EU and the US. In that, it is necessary that the US shall institute better safeguards for the protection of the informational privacy of EU citizens, and that data subjects are equipped with better instruments to enforce their rights for instance against US authorities in order to comply with the GDPR-norms. Alternatively, the bar for personal data protection should be lowered significantly by the EU regulator. That would however not be advisable from a *trust* perspective, as that implicates admitting to a lower level of privacy protection regarding 'exported' personal data.

Thus, in order to reach a well-balanced improvement within al three studied frameworks of the conditions for innovation in the field of autonomous vehicles and consumer acceptance of the results thereof, regulatory action is simultaneously required on different levels. In that, participation of the relevant stakeholders, including *inter alia* AV(-component) manufacturers and other service providers, insurers and consumers is equally important as the regulatory actions to be taken by the EU-regulatory institutions, *en route* towards the optimization of the *factors*, and in turn towards creating better conditions for innovation and acceptance of autonomous vehicles in the European Union.

NEDERLANDSE SAMENVATTING

Het startpunt van dit onderzoek werd gevormd door de hypothese dat de huidige reguleringsraamwerken ten aanzien van buitencontractuele aansprakelijkheid en informationele privacy de ontwikkeling van de innovatie op het gebied van Autonome Voertuigen (AVs) kunnen beïnvloeden, en dat, in hun huidige vorm, deze raamwerken niet voor optimale innovatieomstandigheden zorgen. Deze hypothese is bevestigd in de negen hoofdstukken van het bovenstaande onderzoek dat in drie delen werd uitgevoerd met als hoofdvraag:

Welke factoren in regulering kunnen innovatie beïnvloeden op het gebied van autonome voertuigen in de Europese Unie, hoe kunnen die factoren worden geïdentificeerd in de reguleringsraamwerken ten aanzien van buitencontractuele aansprakelijkheid en bescherming van persoonsgegevens, en hoe kunnen deze factoren zodanig worden geoptimaliseerd dat daarmee de omstandigheden worden verbeterd voor innovatie en acceptatie van AV-technologie door burgers?

De reguleringsraamwerken die ik in dit verband heb onderzocht, betreffen: de geharmoniseerde regels ten aanzien van productaansprakelijkheid en de implementaties daarvan in Nederland, Frankrijk en Engeland; de niet-geharmoniseerde regels ten aanzien van motorvoertuigenaansprakelijkheid in dezelfde jurisdicties; en de regels ten aanzien van de bescherming van persoonsgegevens zoals die zijn geharmoniseerd in de Algemene Verordening Gegevensbescherming (AVG).

EERSTE DEEL: GEÏDENTIFICEERDE *FACTOREN*

Het eerste deel betrof het *onderzoeken of er al dan niet een aantal factoren kan worden geïdentificeerd in de academische literatuur die kunnen worden gebruikt om de mogelijke invloed van regulering op innovatie in het algemeen te onderzoeken, die vervolgens kunnen worden toegepast op de reguleringsraamwerken ten aanzien van buitencontractuele aansprakelijkheid en informationele privacy.*

In Hoofdstuk 3 werden twee perspectieven geschetst van waaruit ik innovatie-beïnvloedende *factoren* heb vastgesteld. Vanuit het ***innovatorsperspectief*** heb ik onderscheiden: *rechts(on)zekerheid; flexibiliteit* en *strengheid*. *Rechtszekerheid* – of het gebrek daaraan – kan investeringen in nieuwe technologieën beïnvloeden. Een negatieve invloed kan worden verondersteld indien het lastig is voor een innovator om te voorspellen en te berekenen welke risico's hij loopt ten gevolge van een reguleringsraamwerk dat van toepassing is op het ontwikkelen en uitrollen van een bepaalde nieuwe technologie. *Strengheid* beschrijft de mate waarin een innovator zijn gedrag (of technologie) moet aanpassen om aan bepaalde regels te voldoen. Dit is met name relevant wanneer nieuwe regulering wordt geïntroduceerd die gedrags-

of technologieaanpassingen vergen. Ook kan sprake zijn van *strengheid* als nieuwe spelers die de markt willen betreden te maken krijgen met hoge voorafgaande kosten om aan de betreffende regels te voldoen. De factor *flexibiliteit* bestaat uit twee aspecten die beide van invloed kunnen zijn op het ontwikkelen en uitrollen van innovatieve technologie. Het eerste aspect betreft de bewegingsvrijheid van innovators als die aan bepaalde regels moeten voldoen: hoe meer ruimte (flexibiliteit) er wordt geboden, des te beter dat is voor innovatie. Het tweede aspect betreft de mate waarin de betreffende regulering kan meebewegen met (technologische) verandering: hoe meer aanpassingsvermogen de betreffende regulering bezit (doordat deze bijvoorbeeld technologie-neutraal is geformuleerd), des te beter dat is. A contrario, regels die technologie-afhankelijk zijn en daardoor *niet* gemakkelijk meebewegen met veranderende omstandigheden, beïnvloeden innovatie negatief.

Vanuit het ***consumentenperspectief*** heb ik *risico* en *vertrouwen* geïdentificeerd. Uit het onderzoek blijkt dat de acceptatie van bepaalde technologie negatief kan worden beïnvloed, indien uit die technologie voor consumenten (financiële of andere) risico's resulteren, voor zover die niet worden weggenomen door de toepasselijke regulering. Ook *vertrouwen* is van belang voor het omarmen van innovatieve technologie door consumenten. *Vertrouwen* kan onder andere betrekking hebben op de veiligheid van bepaalde innovatieve producten en op het "reparerend vermogen" dat uitgaat van toepasselijke (aansprakelijkheids)regels indien die producten onverhoopt toch tot schade hebben geleid. Daarnaast is het van belang dat consumenten erop kunnen vertrouwen dat hun fundamentele rechten (waaronder het recht op informationele privacy) worden gerespecteerd door innovators en door de innovatieve technologie.

De twee perspectieven staan niet op zichzelf en kunnen van invloed zijn op elkaar. Zo is het cruciaal vanuit het *innovatorsperspectief* dat de technologie wordt geaccepteerd door consumenten: zonder die acceptatie is innovatie van weinig belang.

TWEEDE DEEL: DE *FACTOREN* IN DE ONDERZOCHTE REGULERINGSRAAMWERKEN

Het tweede deel van dit onderzoek behelsde het identificeren van de *factoren* in de reguleringsraamwerken ten aanzien van 1) buitencontractuele aansprakelijkheid, en 2) bescherming van persoonsgegevens. Dit gebeurde aan de hand van een casestudy die is geschetst in Hoofdstuk 3.5, en nader uitgewerkt en onderzocht in Hoofdstuk 6 en 7.

De algemene constatering is dat *rechtszekerheid, risico* en *vertrouwen* het slechtst scoren, volgens een scoringsmethodiek die is uiteengezet in Hoofdstuk 7.1. Dit impliceert dat met name *die factoren* moeten worden verbeterd bij het optimaliseren van de reguleringsraamwerken in het licht van innovatie en acceptatie van AVs.

Toenemende autonomie van voertuigen resulteert in toenemende *onzekerheid* ten aanzien van (het kunnen vaststellen van) de bron van schade ten gevolge van een ongeluk waarbij een AV is betrokken. Het vaststellen van een dergelijke bron is essentieel om een succesvol beroep te kunnen doen op aansprakelijkheid van bijvoorbeeld een producent of een AV-verhuurder. Om productaansprakelijkheid (of in Nederland: aansprakelijkheid voor gebrekkige zaken als geregeld in artikel 6:173 BW) te kunnen claimen, is het onder meer noodzakelijk om een *gebrek* te kunnen bewijzen. Ook voor het vaststellen van een *fout* in de zin van de (algemene) onrechtmatige daad (artikel 6:162 BW) ten gevolge waarvan verkeersaansprakelijkheid kan worden vastgesteld in Nederland – en in mindere mate in Engeland – is het nodig dat de schadebron kan worden bewezen door degene die schadevergoeding wenst. Ook het bewijzen van een *causale relatie* tussen een zekere *normoverschrijding* en geleden *schade* (ten gevolge van een AV-ongeluk) wordt lastiger naarmate de autonomie van voertuigen toeneemt – hetgeen van betekenis is voor alle onderzochte aansprakelijkheidsregimes. Dit is met name problematisch voor slachtoffers van AV-gerelateerde ongelukken, omdat het ingewikkelder wordt om aansprakelijkheid van een innovator vast te stellen – terwijl innovators zich relatief gemakkelijk kunnen verweren tegen een claim van AV-slachtoffers. Voor innovators wordt het echter tegelijkertijd ook lastiger om een eventueel (eigen schuld)verweer succesvol in stelling te kunnen brengen, hoewel zij in beginsel wel, en in ieder geval gemakkelijker dan slachtoffers, de beschikking kunnen hebben over de data die zijn opgeslagen in een AV die relevant kunnen zijn voor het vaststellen van de schadebron. Tevens hebben zij betere mogelijkheden dan de slachtoffers om deze data te interpreteren. Ook het reguleringsraamwerk ter zake van persoonsgegevensbescherming herbergt diverse *onzekerheden*. Zo is het vanwege de vele open en vage normen die zijn opgenomen in de AVG en het gebrek aan duiding en nadere normuitleg door de toezichthouders, voor innovators vaak lastig om vast te stellen aan welke concrete eisen zij dienen te voldoen.

De vastgestelde *onzekerheden* lijken met name van negatieve invloed te zijn op de factoren *risico* (dat geleden schade niet kan worden verhaald) en *vertrouwen* (in de compensatiemechanismen van de huidige regels en de veiligheid van AVs in algemene zin) betreffende de productaansprakelijkheidsregels en de verkeersaansprakelijkheidsregels in Nederland (het regime van artikel 185 Wegenverkeerswet uitgezonderd) en in mindere mate de verkeersaansprakelijkheidsregels in Engeland. De omstandigheid dat juist deze twee *factoren* uit het *consumentenperspectief* slecht scoren, impliceert dat de condities van innovatie-acceptatie voor consumenten niet optimaal zijn, hetgeen noodzakelijk is voor het succes van innovatie op het gebied van AVs.

Daarnaast is vastgesteld dat er nauwelijks sprake is van *strengheid* van de onderzochte buitencontractuele aansprakelijkheidsregimes. Dat is echter anders ten aanzien van de AVG, die

als onnodig *streng* kan worden beschouwd. De AVG is van toepassing op de verwerking van persoonsgegevens. Het is waarschijnlijk dat door (middel van) AVs op grote schaal persoonsgegevens zullen worden verwerkt, juist ook voor doelen die zijn gelegen in het vaststellen van product- of fout-gebaseerde verkeersaansprakelijkheid door slachtoffers van AV-ongelukken (of het voeren van verweer daartegen door de innovators). Die mate van *strengheid* is het gevolg van de "regeldruk" voor innovators: voorafgaand aan het uitvoeren van een activiteit die bestaat uit het verwerken van persoonsgegevens, moet aan een groot aantal voorwaarden uit de AVG worden voldaan. Die voorwaarden zijn, als gesteld, vaak niet heel helder, en tegelijkertijd is er een groot (zowel civiel- als publiekrechtelijk) handhavingsrisico in het geval dat niet aan die voorwaarden wordt voldaan door een innovator. Vanwege de eerdergenoemde onzekerheid, en ondanks de handhavingsrisico's, biedt de AVG in zijn huidige vorm te weinig aanknopingspunten voor *vertrouwen* van consumenten: zolang het *onzeker* is aan welke normen innovators dienen te voldoen, kan er niet in redelijkheid door consumenten op worden vertrouwd dat hun informationele privacy voldoende wordt gewaarborgd door die innovators. Dit heeft ook zijn weerslag op *risico*: als de informationele privacy onvoldoende wordt gewaarborgd, bestaat er een kans dat er schade ontstaat voor consumenten vanwege misbruik door derden van persoonsgegevens. Zulke schade kan niet altijd gemakkelijk worden verhaald op een inbreukmakende innovator onder het huidige aansprakelijkheidsregime van de AVG.

DERDE DEEL: VERBETEREN VAN DE *FACTOREN*

Het derde en laatste deel van dit onderzoek zag op het formuleren van aanbevelingen om de *factoren* te verbeteren, en dus om de omstandigheden voor het ontwikkelen en uitrollen van AVs in Europa te optimaliseren in het licht van de ambities van de Europese Unie ten aanzien van het beter reguleren van innovatieve technologie.

Ook in dit deel heb ik twee zaken onderscheiden. Het eerste deel van de aanbevelingen had betrekking op de vraag welke inhoudelijke onderdelen van de betreffende reguleringsraamwerken kunnen worden verbeterd; het tweede deel betrof de vraag hoe zulke verbeteringen zouden kunnen worden gereguleerd.

Ten aanzien van die eerste vraag (wat te verbeteren), kan het volgende worden aanbevolen:

Productaansprakelijkheid

1. Het begrip product dient te worden aangepast opdat ook "software als zodanig" onder de definitie valt, ongeacht de relatie van die software met hardware.
2. Verhelderd dient te worden welke mate van veiligheid men mag verwachten ten aanzien van AVs, waarbij wordt aanbevolen dat verwacht mag worden dat deze tenminste "meer

dan uitmuntende rijvaardigheid" bezitten, bij gebreke waarvan deze als gebrekkig kunnen worden aangemerkt.

3. Er dienen zorgplichten te worden geïntroduceerd voor producenten nadat de producten in het verkeer zijn gebracht, opdat de AV's en of de componenten daarvan veilig blijven, hetgeen onder meer impliceert dat producenten (cyber)security-updates dienen te verstrekken.
4. In het verlengde daarvan kan een producent geen beroep doen op het ontwikkelingsrisicoverweer en het verweer ten aanzien van gebreken die zijn ontstaan nadat de producent het product in het verkeer heeft gebracht, wanneer de producent niet aan de hiervoor bedoelde zorgplichten heeft voldaan. Overigens dient het eigen-schuldverweer wel mogelijk te blijven voor producenten.
5. Er dienen bewijshulpmiddelen te worden gereguleerd voor slachtoffers van (verondersteld) gebrekkige AVs ten aanzien van gebrekkigheid en causaliteit, zowel vanuit materieel als procedureel opzicht:
    a. Procedureel: de bewijslast voor slachtoffers dient te worden verlicht, door middel van het reguleren van een (weerlegbaar) vermoeden van een gebrek indien een AV betrokken is in een ongeluk, alsmede een (eveneens weerlegbare) aanname dat er causaliteit bestaat tussen de gebrekkigheid en de ontstane schade.
    b. Materieel: er dient een "logging-by-design"-verplichting voor AV-(component)producenten te worden geregeld, opdat het mogelijk wordt om de gebeurtenissen te reconstrueren die vooraf gingen aan het ongeluk (met inbegrip van geautomatiseerde voertuigbeslissingen), waarbij het tevens verplicht dient te worden dat de vastgelegde informatie ter beschikking wordt gesteld aan de slachtoffers. Handelen in strijd met deze verplichtingen dient te leiden tot het omkeren van de bewijslast met betrekking tot het aantonen van gebrekkigheid, schade en causaliteit.

Deze maatregelen dienen te leiden tot het verbeteren van *rechtszekerheid*, *risico* en *vertrouwen*. Daarnaast hebben deze voorgestelde maatregelen tot gevolg dat een hernieuwde, verbeterde, balans wordt bereikt die het doel is van het productaansprakelijkheidsraamwerk, namelijk enerzijds het bieden van goede condities voor innovatie, en anderzijds het effectief compenseren van eventuele slachtoffers van gebrekkige innovatieve producten. Onnodige *strengheid* dient echter te worden voorkomen. Daarom dient onder meer het eigen-schuldverweer van producenten in stand te blijven.

Verkeersaansprakelijkheid

1. Het zou niet noodzakelijk moeten zijn dat slachtoffers (ongeacht hun hoedanigheid van bijvoorbeeld "bestuurder", passagier of niet-inzittende) een fout of gebrek moeten bewijzen; de enkele betrokkenheid van een AV in een ongeval dient voldoende te zijn om aansprakelijkheid van die gebruiker (bijvoorbeeld de AV-eigenaar) vast te stellen.
2. In principe dient 100% van de geleden schade te worden vergoed, tenzij *overmacht* kan worden bewezen, hetgeen kan leiden tot een reductie van de vergoedbare schade. Overmacht kan bestaan in opzet of bewuste roekeloosheid van het slachtoffer. Zulke bewuste roekeloosheid kan erin bestaan dat het slachtoffer opzettelijk heeft nagelaten om een kritieke veiligheidsupdate te installeren, of dat het slachtoffer de AV-software heeft aangepast.
3. Teneinde een overmachtsverweer te kunnen onderbouwen, kan het noodzakelijk zijn dat ongeval-gerelateerde AV-gegevens worden verkregen en geanalyseerd. Om die reden dient het te worden gereguleerd dat vastgelegde informatie (die uit hoofde van de te reguleren logging-by-design-verplichting dient te worden vastgelegd) ter beschikking wordt gesteld aan de AV-gebruiker en de slachtoffers in kwestie.

De factoren *risico* en *vertrouwen* dienen te profiteren van de bovengenoemde aanbevelingen,Ookzouden deze een positief effect moeten hebben op *rechtszekerheid*, omdat onder andere de financiële risico's van tevoren beter kunnen worden ingeschat dan het geval zou zijn zonder het implementeren van deze aanbevelingen. Ondanks een mogelijke toename van de *strengheid* (te beteugelen door middel van een overmachtsverweer) van de verkeersaansprakelijkheidsregels, kan de toename in *rechtszekerheid* als overwegend gunstig worden beschouwd vanuit het *innovators-perspectief*, temeer daar ook onder de huidige verkeersaansprakelijkheidsregimes vergelijkbare risicoaansprakelijkheden zijn gereguleerd.

Persoonsgegevensbescherming

1. Verheldering is noodzakelijk ten aanzien van de volgende AVG-normen:
    a. Rechtmatigheid van de verwerking van van persoonsgegevens met als doel het (door slachtoffers) vaststellen en/of het (door innovators) zich verweren tegen product- of verkeersaansprakelijkheidsclaims. Dit brengt mee dat er een heldere rechtmatige verwerkingsgrond dient te worden gereguleerd voor het verwerken van persoonsgegevens voor deze product- en verkeersaansprakelijkheids-doelstellingen (hierna: PVA-doelstellingen), door middel van bijvoorbeeld

systemen ter preventie en registratie van ongevallen (hierna SPRO). Ook dient er een uitzondering op het generieke verwerkingsverbod van bijzondere persoonsgegevens in dit verband te worden geregeld, met betrekking tot geolocatie en persoonlijke voorkeuren van de AV-inzittenden, zonder dat hun toestemming daarvoor noodzakelijk is.

   b. Gegevensbeschermingseffectbeoordelingen (GBOs): verhelderd dient te worden wanneer er "hoge risico's" voor de privacy blijven bestaan voor betrokkenen nadat een GBO is uitgevoerd ten aanzien van PVA-doelstellingen met gebruikmaking van een SPRO, in welk geval een toezichthouder dient te worden geconsulteerd voordat een verwerkingsactiviteit mag worden begonnen.
   c. Technische en organisatorische maatregelen (TOMs): verhelderd dient te worden wanneer een innovator heeft voldaan aan zijn verplichting tot het implementeren van passende TOMs met betrekking tot gegevensverwerking ten aanzien van PVA-doelstellingen door middel van een SPRO.
   d. Privacy-by-design en privacy-by-default (PBD): verhelderd dient te worden wanneer een innovator geacht wordt aan zijn PBD-verplichtingen te hebben voldaan wanneer deze voornemens is gegevens te verwerken voor PVA-doelstellingen door middel van een SPRO.

2. Er dient een oplossing te worden gevonden die innovators in staat stelt om ongeval-gerelateerde AV-data voor PVA-doelstellingen decentraal op te slaan, bijvoorbeeld door middel van blockchain of vergelijkbare technologie, op een zo privacy-vriendelijk mogelijke wijze, en zodanig dat betrokkenen hun rechten effectief kunnen uitoefenen.
3. Internationale doorgifte van persoonsgegevens dient te worden vergemakkelijkt, zodat bijvoorbeeld SPROs kunnen worden ingezet voor PVA-doelstellingen, terwijl niet alle betrokken actoren zich in de Europese Unie (maar bijvoorbeeld in de VS) bevinden. Daartoe dient de huidige patstelling die is ontstaan na het HvJEU-arrest inzake *Schrems II* te worden opgeheven, zonder dat teveel wordt ingeboet op de effectieve privacybescherming van EU-ingezetenen.
4. Er dienen bewijshulpmiddelen te worden gereguleerd voor slachtoffers van (vermeende) inbreuk op de AVG-regels door AV-innovators (in hun hoedanigheid als verwerkings-verantwoordelijke), waarbij die middelen ook dienen te helpen bij het vaststellen van causaliteit. Dit kan geschieden door middel van (weerlegbare) vermoedens ten aanzien van een inbreuk en causaliteit, in het geval innovators in kwestie niet voldoen aan hun verplichtingen ten opzichte van het waarborgen van de rechten van betrokkenen, in het geval van datalekken of wanneer op andere wijze schade is ontstaan na een AVG-inbreuk.

> Daarbij dient te worden verhelderd welke vormen van immateriële schade voor vergoeding in aanmerking komen onder de civiele aansprakelijkheidsregeling van de AVG.

Het zal lastig zijn om alle *factoren* tegelijkertijd te verbeteren. Het optimaliseren van *rechtszekerheid* voor innovators is echter een goed startpunt. Die interventie kan tot gevolg hebben dat het eenvoudiger wordt om de AV-verplichtingen goed te kunnen duiden en dus om deze na te leven. Dit brengt ook mee dat de risico's beter kunnen worden ingeschat ten aanzien van het niet-naleven van de AVG-normen, en zo verbetert de factor *strengheid*. Het beter (kunnen) naleven van de privacyregels impliceert eveneens een verbetering van de factor *vertrouwen*. Desalniettemin lost het verbeteren van de *rechtszekerheid* niet alle andere gesignaleerde problemen op. Daarom dienen ook de andere aanbevelingen, onder meer ten aanzien van het her-legaliseren van trans-Atlantische uitwisseling van persoonsgegevens, en het mogelijk maken van blockchain (of daarmee vergelijkbare) technologie, te worden overgenomen, net als de aanbevelingen ten aanzien van de te introduceren bewijshulpmiddelen.

Er zijn diverse manieren denkbaar om de betreffende *factoren* te verbeteren. Deze gaan gepaard met verschillende vormen van regulering. Ik heb drie verschillende mogelijkheden geschetst ten aanzien van de vraag hoe de gewenste factoroptimalisaties kunnen worden gereguleerd, vanuit drie verschillende invalshoeken.

Ten eerste is het mogelijk om de gewenste veranderingen "van onderaf" te laten plaatsvinden, in de vorm van het implementeren van door de publieke regelgever gemandateerde **bindende gedragscodes voor AV-innovators**. Ten tweede heb ik onderzocht in hoeverre een **verplichte AV-risicoverzekering** kan bijdragen aan het verbeteren van de *factoren*. Ten derde heb ik onderzocht hoe de thans toepasselijke **reguleringsraamwerken zelf** kunnen worden verbeterd, met het oog op zo duurzaam mogelijke, houdbare verbeteringen van de *factoren* – in plaats van het stellen van *sui generis* regels. De derde optie is uiteindelijk te prefereren boven de eerste twee, hoewel die waarschijnlijk de meeste tijd en inspanning van de Europese wetgever zal vergen, omdat in dat geval alle onderzochte reguleringsraamwerken zullen moeten worden aangepast. Om die reden raad ik aan dat de drie routes tegelijkertijd worden ingeslagen, om op zo kort mogelijke termijn tot zo goed mogelijke *factor*verbetering te komen. De ervaringen die de Europese wetgever opdoet tijdens het volgen van de eerste twee reguleringsroutes kunnen worden meegenomen bij het volgen van de uiteindelijk te prefereren derde route.

De **bindende gedragscodes voor AV-innovators** komen in feite neer op het zonder voorbehoud accepteren van aansprakelijkheid door die innovators. Dat lost de meest acute problemen op voor AV-slachtoffers (hetgeen gunstig is voor de factoren *risico* en *vertrouwen*), en voorkomt de noodzaak van ongebreidelde gegevensopslag voor PVA-doelstellingen (hetgeen ook positief zal

zijn voor het *vertrouwen* van consumenten). Ook levert zulke aansprakelijkheidserkenning in feite veel *rechtszekerheid* op voor innovators. Desalniettemin zal dit met zich meebrengen dat innovators zich waarschijnlijk meer aansprakelijkheid en daarmee samenhangende schadevergoedingsverplichtingen op de hals halen (hetgeen onnodige *strengheid* betekent), dan mogelijk het geval zou zijn bij het op genuanceerdere wijze verbeteren van het reguleringsraamwerk inzake buitencontractuele aansprakelijkheid. Ook zal een dergelijke praktijk in financieel opzicht waarschijnlijk beter te dragen zijn door de grotere marktpartijen dan de kleinere spelers, voor wie dit wel eens een te grote belasting zou kunnen betekenen. Daarenboven worden met dergelijke bindende gedragscodes de geconstateerde problemen in de reguleringsraamwerken zelf verder niet opgelost.

De **verplichte AV-risicoverzekering** zou moeten leiden tot compensatie van de schade die alle slachtoffers van AV-gerelateerde ongevallen hebben geleden, ongeacht de verkeers- of risicoaansprakelijkheid van een innovator. Ook een dergelijk systeem lost de meest acute problemen van slachtoffers op, in die zin dat zij hun schade vergoed kunnen krijgen zonder daaromtrent ingewikkelde procedures te hoeven voeren en daarin met lastige bewijsproblemen te worden geconfronteerd. Innovators weten ook direct waar ze aan toe zijn: schade is verzekerbaar, en de verzekering dient te worden betaald. Dat alles is goed voor de factoren = *risico, vertrouwen* en *rechtszekerheid.* Dataopslag blijft overigens tot op zekere hoogte nodig voor verzekeraars, om desgewenst te kunnen onderbouwen dat sprake is van mogelijke uitzonderingen op de regel dat alle schade dient te worden vergoed, bijvoorbeeld omdat er moedwillig een kritieke veiligheidsupdate is overgeslagen, of omdat de software is aangepast door de verzekerde. Een ander effect van deze ruime verzekerings- en daarmee vergoedingsplicht kan zijn dat innovators niet worden gestimuleerd om zo veilig mogelijke AVs op de weg te brengen, omdat die innovators niet direct worden geconfronteerd met een mogelijk schadevergoedingsrisico (hetgeen mogelijk van negatieve invloed is op het *vertrouwen* in de veiligheid van de AV-technologie). Tegelijkertijd kan het ook zo zijn dat de betreffende verzekeringen relatief duur worden voor innovators (met verhoogde *strengheid* tot gevolg). Dat is niet ondenkbaar zolang er nog geen vergelijkbare verzekeringen op de markt zijn, waardoor de premies (te) hoog worden ingestoken. Dat laatste kan worden voorkomen door de uit te keren schadebedragen te maximeren. Hoe hoog die schademaxima dienen te zijn, zou in overleg tussen de diverse actoren (waaronder de Europese wetgever en private actoren zoals verzekeraars, AV-producenten, consumenten en verenigingen van slachtoffers) moeten worden vastgesteld. Schademaxima brengen echter mee dat niet altijd alle schade vergoed zal worden, hetgeen dan een weerslag zal hebben op de *risico*- en *vertrouwens*factoren. Dit impliceert onder andere dat het van belang blijft om de toepasselijke aansprakelijkheidsregels eveneens aan te passen, zodat slachtoffers ook langs die weg aanspraak kunnen maken op de door de verzekering niet-

uitgekeerde bedragen. Ook om meer dogmatische redenen dient men de kans niet te laten glippen om de betreffende reguleringsraamwerken te verbeteren, met het vooruitzicht dat die dan ook effectief kunnen worden ingezet wanneer AVs hun intrede doen op de Europese markt (en anders niet).

Als gesteld is mijns inziens de meest logische en duurzame route erop gericht dat de bestaande reguleringsraamwerken zodanig worden aangepast dat de daarin vervatte *factoren* voor innovatie en acceptatie worden verbeterd. Die route is dan ook te prefereren boven het reguleren van technologie- of sectorspecifieke *sui generis*-normen, die weliswaar een deel van de meest pregnante problemen oplossen, maar niet voor houdbare of toekomstbestendige oplossingen zorgen. Het aanpassen van de bestudeerde raamwerken zou er als volgt uit kunnen zien.

De **Productaansprakelijkheidsrichtlijn** (PAR) die zou moeten worden omgezet in een verordening, dient als volgt te worden aangepast:

1. Ten aanzien van AVs zou er een *lex specialis* kunnen worden gecreëerd (waarvan het toepassingsbereik waar nodig kan worden uitgebreid voor andere technologie waarin AI een rol speelt). Die regels moeten flexibel kunnen worden aangepast aan de voortschrijdende technologische innovatie, door nauwe samenwerking tussen de Europese wetgever en belanghebbende private actoren, waaronder bijvoorbeeld AV(-componenten)producenten; verenigingen van consumenten en slachtoffers; verzekeraars et cetera, waarbij de hierna opgenomen principes tot uitgangspunt dienen te worden genomen.
2. Gereguleerd dient te worden dat:
    a. software onderdeel zal zijn van de *product*-definitie in de zin van artikel 2 van de PAR;
    b. in artikel 6(1) PAR wordt verduidelijkt dat een AV(-component) gebrekkig is, indien deze/die tot gevolg heeft dat het voertuig niet de rijkwaliteiten bezit die mogen worden verwacht van de meest uitmuntende menselijke bestuurder, of indien de producent niet aan diens verplichtingen uit de AVG heeft voldaan ten aanzien van de persoonsgegevens die worden verwerkt door of vanwege de toepassing van de AV;
    c. de verweren die zijn gecodificeerd in artikel 7(b) (ten aanzien van het “later ontstaan” van een gebrek) en 7(e) (ten aanzien van ontwikkelingsrisico) PAR, uitsluitend met succes kunnen worden gevoerd, indien de betreffende producent kan aantonen:

i. dat hij de noodzakelijke kritieke veiligheidsupdates gedurende een bepaalde periode heeft aangeboden die (potentiële) gebreken in zijn product zouden moeten voorkomen of verhelpen, en dat het slachtoffer deze opzettelijk niet heeft geïnstalleerd; of
ii. dat het slachtoffer met opzet de AV-software heeft aangepast waardoor het betreffende gebrek is ontstaan;

d. artikel 4 PAR als volgt wordt aangepast, dat indien een slachtoffer schade heeft geleden na een ongeval waarin een AV betrokken was:
   i. een gebrek, schade en causaliteit (weerlegbaar) wordt aangenomen, tenzij
   ii. de producent niet voldoet aan diens verplichting om het slachtoffer toegang te verschaffen tot de door de AV bijgehouden logbestanden (zie nader onder e), in welk geval de producent dient te bewijzen dat er geen sprake was van een gebrek, en dat de schade niet kan zijn veroorzaakt door dat gebrek;

e. een nieuwe verplichting voor producenten wordt opgenomen in de PAR ten aanzien van "logging-by-design". Producenten dienen AV(-componenten) te equiperen met functionaliteit die het mogelijk maakt om de AV-activiteit in een logbestand op te slaan, op een zodanige wijze dat op basis van die informatie later kan worden vastgesteld welke gebeurtenissen er plaatsvonden voorafgaand aan en tijdens het ongeval, met inbegrip van de geautomatiseerde besluiten die door de AV zijn genomen. Deze logbestanden dienen op verzoek van een slachtoffer of een AV-eigenaar ter beschikking te worden gesteld ten behoeve van een procedure waarin product- of verkeersaansprakelijkheid aan de orde is. Deze logging-by-design-verplichting alsmede het verwerken van de vastgelegde informatie in een juridische procedure dient te worden aangemerkt als rechtmatige grondslag voor het verwerken van persoonsgegevens in de zin van artikel 6(1)(c) AVG, waarbij de privacy van betrokkenen zo goed mogelijk dient te worden gewaarborgd.

De aanbevelingen ten aanzien van het reguleringsraamwerk inzake **verkeersaansprakelijkheid** dienen te worden vervat in een EU-verordening, met inachtneming van de volgende principes:

1. De eigenaar van een AV is aansprakelijk jegens slachtoffers van ongevallen waarbij diens AV betrokken is;
2. Alle materiële en immateriële schade dient te worden vergoed, tenzij de eigenaar van de AV kan aantonen dat er sprake is van overmacht, hetwelk kan leiden tot reductie van de schadevergoedingsplicht. Overmacht kan bestaan in een *faute inexcusable* die kan worden toegerekend aan het slachtoffer, of in bewuste roekeloosheid van het slachtoffer. Er kan

van bewuste roekeloosheid sprake zijn, indien het slachtoffer opzettelijk een kritieke veiligheidsupdate niet installeert, of indien hij met opzet AV(-componenten) waaronder mede begrepen de software aanpast;

3. Een AV-eigenaar dient toegang te kunnen verkrijgen tot de logbestanden van een AV (die ingevolge de te reguleren logging-by-design-verplichting (in de PAR) moeten worden opgeslagen door de producent) teneinde een overmachtsverweer te kunnen onderbouwen;
4. Gestipuleerd dient te worden dat het verkrijgen van toegang tot, en analyse van de betreffende logbestanden een rechtmatige verwerking van persoonsgegevens behelst in de zin van artikel 6(1)(c) AVG voor de hiervoor genoemde doelen.

De bovenstaande verkeersaansprakelijkheidsregels dienen te worden vergezeld van een passende aansprakelijkheidsverzekering. Die verzekering kan op dezelfde voet worden gereguleerd als de hierboven beschouwde verplichte AV-risicoverzekering, zij het dat de hier bedoelde verzekering dus wél ziet op situaties waarin aansprakelijkheid kan worden vastgesteld. Ook in dezen vormt co-regulering de aangewezen methodiek.

De regels inzake **de bescherming van persoonsgegevens** ingevolge de AVG dienen als volgt te worden aangepast:

Het verduidelijken van de geïndiceerde normen dient te geschieden door middel van goedgekeurde sectorspecifieke gedragscodes en waar nodig door middel van EDPB-richtsnoeren. Bezien vanuit de *rechtszekerheid* verdient het de voorkeur dat waar mogelijk gedragscodes worden ingezet in plaats van EDPB-richtsnoeren. Het ligt echter, op grond van de huidige in de AVG vervatte procedures, niet voor de hand dat gedragscodes in groten getale ter goedkeuring aan de toezichthouders worden voorgelegd. Daarom dient (onder andere) de procedure tot goedkeuring te worden vereenvoudigd, en dienen de kosten die daarmee zijn gemoeid, te worden verlaagd. Overigens verdient het aanbeveling de betreffende gedragscodes "van onderaf" te laten ontstaan. Dat dient op zodanige wijze te kunnen geschieden dat belanghebbenden (waaronder bijvoorbeeld AV-producenten, verzekeraars, alsmede verenigingen van consumenten en slachtoffers) op een laagdrempelige wijze de mogelijkheid wordt geboden om de "best practices" die er (wellicht) al bestaan, uiteindelijk om te zetten in ter zake geschikte gedragscodes. Die codes zouden "marginaal" moeten worden getoetst door de betreffende toezichthouders ten behoeve van goed- of afkeuring.

Het verdient aanbeveling om zogenoemde regulatory sandboxes op te zetten, ten aanzien van onder meer de te reguleren logging-by-design-verplichting in de PAR, en de verheldering van de passende technische en organisatorische maatregelen met betrekking tot gegevensverwerkingen

ten aanzien van product- en verkeersaansprakelijkheidsdoelstellingen door middel van systemen ter preventie en registratie van ongevallen, die bijvoorbeeld gebruikmaken van blockchain-technologie. Die regulatory sandboxes kunnen worden gebruikt om te onderzoeken in hoeverre de betreffende technologie in overeenstemming kan worden gebracht met de AVG. Tegelijkertijd kan worden onderzocht in hoeverre de AVG wellicht dient te worden aangepast om de betreffende technologie zo goed mogelijk te kunnen faciliteren in plaats van deze uit te sluiten, zoals thans het geval is, op het moment dat deze niet lijkt te voldoen aan de normen.

Het reguleren van bewijshulpmiddelen voor slachtoffers van AVG-inbreuken dient te geschieden bij de bepalingen omtrent civiele aansprakelijkheid in de AVG. Bovendien kan gebruik worden gemaakt van "standaardbedragen" die passen bij bepaalde normoverschrijdingen. Die standaarden dienen te worden opgesteld door nauwe samenwerking tussen onder meer AV-producenten, verzekeraars, verbanden van verzekeraars en slachtoffers.

De Europese wetgever is aan zet waar het gaat om het maken van nieuwe internationale afspraken ter zake van doorgifte van persoonsgegevens naar derde landen, onder meer met de VS. Daarbij dient de VS betere waarborgen te bieden voor het beschermen van de informationele privacy van EU-ingezetenen, en dienen deze betere middelen tot hun beschikking te krijgen om hun rechten te kunnen handhaven ten opzichte van onder meer de Amerikaanse opsporingsautoriteiten. Het alternatief is dat de EU minder strenge eisen dient te stellen aan privacybescherming van de eigen burgers, hetgeen niet wenselijk is vanuit het perspectief van de consumenten, en met name de factor *vertrouwen*.

Al met al blijkt het nodig dat er actie wordt ondernomen op verschillende wijzen en op verschillende niveaus van regulering. Daarbij is het zaak dat naast de publieke Uniewetgever alle belanghebbende private actoren bij de reguleringsprocessen worden betrokken, *en route* naar een structurele en duurzame verbetering van de *factoren*, en dus onderweg naar het creëren van betere condities voor innovatie en acceptatie van autonome voertuigen in Europa.

LITERATURE

Alheit 2001

Alheit, K., "The applicability of the EU Product Liability Directive to software", *Comparative and International Law Journal of Southern Africa*, vol. 4, issue 1, 2001, p. 188-209.

Allen 2011

Allen, A.L., *Unpopular Privacy*, Oxford: Oxford University Press 2011.

Ashford, Ayers & Stone 1985

Ashford, N.A., Ayers, C., and Stone, R.F., 'Using Regulation to Change the Market for Innovation', *Harvard Environmental Law Review* vol. 9 no. 2 1985, p. 419 – 466.

Ayjam 2010

Ayhan, T., "The Principle of Legal Certainty in EU Case Law". *TODAIE's Review of Public Administration*, vol. 4 no. 3, September 2010, p. 149-183.

Bagshaw 2010

Bagshaw, R., "Traffic Liability in England and Wales", in: Ernst, W. (ed.), *The Development of Traffic Liability*, Cambridge: Cambridge University Press 2010, pp. 12-49.

Balboni 2008

Balboni, P., *Trustmarks: Third-party liability of trustmark organisations in Europe*, Tilburg (diss.) 2008, available online via https://pure.uvt.nl/ws/portalfiles/portal/1063399/Trustmarks.PDF (last accessed 28 October 2018).

Baldwin, Cave & Lodge 2012

Baldwin, R., Cave, M. & Lodge, M., *Understanding Regulation – Theory, Strategy & Practice*, second edition, Oxford (NY): Oxford University Press 2012.

Bauw 2015

E. Bauw, *Onrechtmatige daad: aansprakelijkheid voor zaken*, serie: Monografieën BW, Alphen a/d Rijn 2015.

Baza e.a. 2019

Baza, M. et al., "Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles", *2019 IEEE*

Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-7, via https://ieeexplore-ieee-org.proxy.library.uu.nl/document/8885769 (last accessed 20 July 2020).

Belder, De Cock Buning & De Bruin 2015

Belder, L.P.C. (ed.), Cock Buning, M. de, & Bruin, R.W. de, *CULTIVATE! Cultural heritage institutions, copyright and cultural diversity in the European Union & Indonesia*, Amsterdam: DeLex 2015.

Bell 1976

Bell, D., *The coming of post-industrial society. A venture in social forecasting*, New York: Basic Books 1976.

Berlee 2018

Berlee, A, *Access to personal data in public land registers*, Den Haag: Eleven International Publishing 2018.

Bertolini 2020

Bertolini, A., *Artificial Intelligence and Civil Liability*, report for the European Parliament (Committee on Legal Affairs, Directorate-General for Internal Policies), European Union: Brussels 2020.

Bhorat 2017

Bhorat, Z., 'Do we still need judges in the age of Artificial Intelligence?', Opendemocracy.net, 9 August 2017, available via https://www.opendemocracy.net/transformation/ziyaad-bhorat/do-we-still-need-human-judges-in-age-of-artificial-intelligence (last accessed 12 October 2017).

Black 1996

Black, J., "Constitutionalising Self-Regulation", *The Modern Law Review* 1996, Vol 59, no. 1, p. 24-55.

Black 2001

Black, J., "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World", *Current Legal Problems*, Vol. 54, issue 1 2001, p. 103-146.

Black 2002

Black, J., "Critical Reflections on Regulation", *Australian Journal on Legal Philosophy*, no. 27, 2002, p. 1-36.

Black 2005

Black, J., 'Regulatory innovation', in: Black, J., Lodge, M. & Thatcher, M., *Regulatory Innovation – A Comparative Analysis*, Cheltenham: Edward Elgar 2005.

Blind 2012

Blind, K., 'The Impact of Regulation on Innovation', Nesta Working Paper No. 12/02, January 2012, available on the Internet at

https://www.nesta.org.uk/sites/default/files/the_impact_of_regulation_on_innovation.pdf (last accessed 28 January 2017).

Blind 2012a

Blind, K., "The influence of regulations on innovation: A quantitative assessment for OECD countries", *Research Policy* 2012, no. 41, p. 391-400.

Blok 2002

Blok, P.H., *Het recht op privacy – Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht* (diss.), Den Haag: Boom Juridische Uitgevers 2002.

Blok 2020

Blok, P.H., "The Role of Private Actors in Data Protection Law and Data Protection Practice", in: De Cock Buning, M., de, & Senden, L.A.J. (eds.), *Private Regulation and Enforcement in the EU*, Oxford: Hart Publishers 2020, pp. 95-119.

Boonekamp 2018

Boonekamp, R.J.B., *Groene Serie Schadevergoeding, art. 6:98 BW, aant 1.2, Causaliteitstheorieën*, Deventer: Wolters Kluwer 2018.

Borghetti 2016

Borghetti, J.S., "France", in: Machnikowski, P. (ed.), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies,* Cambride (UK): Intersentia 2016, pp. 206-236.

Borghetti 2018

Borghetti, J.S., "Traffic Accidents in France", *Wake Forest Law Review*, 2018 vol. 53, p. 265 – 291.

Bradley 2014

Bradley, K. St. C., "Legislating in the European Union", in: Barnard, C. and Peers, S., *European Union Law*, Oxford: Oxford University Press 2014, p. 98-140.

Braithwaite 2017

Braithwaite, V., "Closing the gap between regulation and the community", in Drahos, P. (ed.), *Regulatory theory: foundations and applications,* Canberra: ANU Press 2017 (e-book version, via: press.anu.edu.au).

Breemen & Wouters 2020

Breemen, V., and Wouters, A., "Hoofdstuk 5, Casestudy Zelfrijdende auto's", in: Kulk, S., & Van Deursen, S., *Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek*, Den Haag: WODC 2020, p. 71-104.

Bronsword, Scotford & Yeung 2017

Brownsword, R., Scotford, E. and Yeung, K., "Law, Regulation, and Technology: The Field, Frame and Focal Questions", in: Brownsword, R., Scotford, E. and Yeung, K., (eds.), *The Oxford handbook of the law and regulation of technology*, Oxford: Oxford University Press 2017, p. 3-41.

Butcher & Edmonds 2018

Butcher, L., & Edmonds, T., "Automated and Electric Vehicles Act 2018", Briefing Paper for the House of Commons, Number CBP 8118, 15 August 2018, via https://commonslibrary.parliament.uk/research-briefings/cbp-8118/ (last accessed 14 May 2020).

Cane & Goudkamp 2018

Cane, C. & Goudkamp, J., *Atiyah's Accidents, Compensation and the Law*, Cambridge: Cambridge University Press 2018.

Cafaggi 2006

Cafaggi, F., "Rethinking private regulation in the European regulatory space", *EUI Working Paper LAW* No. 2006/13.

Cafaggi & Renda 2012

Cafaggi, F., & Renda, A., "Public and Private Regulation Mapping the Labyrinth", CEPS Working Document No. 370/October 2012, available via http://www.ceps.eu (last accessed 31 Jul. 19).

Carter & Bélanger 2005

Carter L., and Bélanger F., "The utilization of e-government services: citizen trust, innovation and acceptance factors", *Info Systems Journal* (2005), no. 15, pp. 5-25.

CCAM Report 2018

Bolchi, M., et al., "Annex 2, Part B; Scenarios and conditions for the implementation of CAD- CCAM and proactive mapping of policy measures (Task 2)", 165 p., Annex to Van Lieshout et al., "Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected and AI-based vehicles and systems – SMART 2016/0071" Report for the European Commission, by TNO, VVA and SSSA, via: http://publications.europa.eu/resource/cellar/aad6a287-5523-11e9-a8ed-01aa75ed71a1.0001.01/DOC_1 (last accessed 28 August 2021).

Chakravorti 2018

B. Chakravorti, "Trust in Digital Technology Will Be the Internet's Next Frontier, for 2018 and Beyond", *Scientific American* 4 January 2018, via https://www.scientificamerican.com/article/trust-in-digital-technology-will-be-the-internet-rsquo-s-next-frontier-for-2018-and-beyond/ (last accessed 25 May 2018).

Chamberlain & Reichel 2019

Chamberlain, J., and Reichel, J., "The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation", *SSRN Electronic Journal,* January 2019, p. 1-20, via https://www.researchgate.net/profile/Jane_Reichel/publication/335895330_The_Relationship_Between_Damages_and_Administrative_Fines_in_the_EU_General_Data_Protection_Regulation/links/5e27f6eb299bf152167340bb/The-Relationship-Between-Damages-and-Administrative-Fines-in-the-EU-General-Data-Protection-Regulation.pdf (last accessed 28 July 2020).

Channon 2019

Channon, M., "Chapter 3 Insurance", in: Channon, M., McCormich, L., & Noussia, K., *The Law and Autonomous Vehicles*, Oxon: Informa Law from Routledge 2019, pp. 14-33.

Chopra & White 2014

Chopra, S., & White, L.F., *A Legal Theory for Autonomous Artificial Agents*, Ann Arbor: The University of Michigan Press 2014.

Christakis 2020

Christakis, Th., "After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe", *European Law Blog* 21 july 2020, via https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/ (last accessed 24 July 2020).

Cunningham & Goodwin 2013

Cunningham, W. & Goodwin, A., 'Six reasons to love, or loathe, autonomous cars', 8 may 2013, via http://www.cnet.com/news/six-reasons-to-love-or-loathe-autonomous-cars/ (last accessed 12 October 2017).

Custers e.a. 2019

Custers, B., Sears, A.M., Dechesne, F., Georgieva, I., Tani, T. & Vander Hof, S.,, *EU Personal Data Protection in Policy and Practice,* Den Haag: T.M.C. Asser Press 2019.

Davis 1989

Davis, F., "Perceived usefulness, perceived ease of use and user acceptance of information technology", *MIS Quarterly* 13, pp. 319 – 340.

D'Amato 1983(/2010)

D'Amato, A., "Legal Uncertainty", *California Law Review* 1983, 1-55; republished under the same title by Northwestern University School of Law, *Faculty Working Papers* 2010, Paper 108.

Deakin, Johnston & Markesinis 2013

Deakin, S., Johnston, A. & Markesinis B., *Markesinis and Deakin's Tort Law*, Oxford: Oxford University Press 2013.

De Bruin 2016

Bruin, R.W. de, "Autonomous Intelligent Cars on the European Intersection of Liability and Privacy: Regulatory Challenges and the Road Ahead", *European Journal of Risk Regulation* 2016 vol. 7 no. 3 pp. 485-501, https://doi.org/10.1017/S1867299X00006036,

De Bruin 2020

Bruin, R.W. de, "De *Automated and Electric Vehicles Act*, Een Britse oplossing voor aansprakelijkheidsvraagstukken rondom autonome(re) auto's", *NJB* 2020 afl. 11, no. 687, p. 742-753.

De Bruin 2021 (forthcoming)

Bruin, R.W. de. "Informational Privacy and Trust in Autonomous Intelligent Systems", in Aldinhas Ferreira, M.I, and Tokhi, O. (eds.), *Towards Trustworthy Artificial Intelligent Systems*, Intelligent Systems, Control and Automation: Science and Engineering Series, Springer: forthcoming 2021.

De Bruyne, Van Gool & Gils 2021

Bruyne, J. de, Gool, E. van, Gils, T., "Chapter 14 Tort Law and Damage Caused by AI Systems", in: Bruyne, J. de, & Vanleenhove, C., *Artificial Intelligence and the Law*, Cambridge: Intersentia 2021, p. 359-403.

DeCew 1997

DeCew, J.W., *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, Ithaca: Cornell University Press 1997.

De Cock Buning, Ottow & Vervaele 2014

Cock Buning, M., de, Ottow, A.T., and Vervaele, J.A.E., "Regulation and Enforcement in the EU: Regimes, Strategies and Styles", *Utrecht Law Review*, 2014, vol. 10 iss. 5, URN:NBN:NL:UI:10-1-115855.

De Cock Buning & Senden 2020

De Cock Buning, M., de, & Senden, L.A.J. (eds.), *Private Regulation and Enforcement in the EU*, Oxford: Hart Publishers 2020, p. 1-33.

De Cock Buning & De Bruin 2017

Bruin, R.W. de & Cock Buning, M. de., "Autonomous intelligent cars: proof that the EPSRC Principles are future-proof" *Connection Science* 2017, 29:3, pp. 189-199, DOI: 10.1080/09540091.2017.1310181

De Cock Buning, Belder & De Bruin 2012

Cock Buning, M. de, Belder, L.P.C., and Bruin de, R.W., "Mapping the Legal Framework for the Introduction into Society of Robots as Autonomous Intelligent Systems, in: Muller, S., Zouridis, S, Frishman, M, & Kistemaker, L. (eds.), *The Law of the Future and the Future of Law: Volume II*, Den Haag: Torkel Opsahl Academic EPublisher 2012, p. 195-210.

De Cock Buning 1998

Cock Buning, M. de, *Auteursrecht en informatietechnologie* (diss.), Amsterdam: Otto Cramwinckel Uitgever 1998.

De Vey Mestdagh & Lubbers 2015

De Vey Mestdagh, C.N.J., and Lubbers, L., "Nee hoor, u wilt helemaal niet naar Den Haag", *Ars Aequi* 2015 no. 20150276, pp. 267- 280.

De Vor & Van Dijck 2002

De Vor, L., and Van Dijck, G.,, "Zwarte dozen in (deels) zelfrijdende auto's: kan de techniek voorzien in het vaststellen van aansprakelijkheid?", *Aansprakelijkheid, verzekering & schade*, no. 5, 2020, p. 192-199.

Devillé, Sergeyssels & Middag 2021

Deville, R., Sergeyssels, N., and Middag, C., "Chapter 1 Basic Concepts of AI for Legal Scholars", in: Bruyne, J. de, & Vanleenhove, C., *Artificial Intelligence and the Law*, Cambridge: Intersentia 2021, p. 1-22.

Dey et al. 2016

Dey K.C. et al., "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network – Performance evaluation, *Transportation Research Part C* 2016, vo. 68, p. 168-184.

Dimmroth & Schünemann 2017

Dimmroth K., and Schünemann W.J., "The Ambiguous Relation Between Privacy and Security in German Cyber Politics", in: Schünemann, W.J., and Baumann M., *Privacy, Data Protection and Cybersecurity in Europe*, Cham: Springer International Publishing 2017, pp. 97-115.

Drahos 2017

Drahos, P. (ed.), *Regulatory theory: foundations and applications,* Canberra: ANU Press 2017 (e-book version, via: press.anu.edu.au)

Drahos & Krygier 2017

Drahos, P. & Krygier, M., 'Regulation, institutions and networks', in Drahos, P. (ed.), *Regulatory theory: foundations and applications,* Canberra: ANU Press 2017 (e-book version, via: press.anu.edu.au)

Dyson 2018

Dyson, M. (ed.), *Regulating Risk Through Private Law,* Mortsel: Intersentia 2018.

East 2017

East, F., "Chapter 7, England & Wales", in Davis Varner, C. & Pratt, B.W., *The Product Regulation & Liability Review*, London: Law Business Research 2017, pp. 66-77.

EGTL 2005

European Group on Tort Law, *Principles of European Tort Law Text and Commentary*, Wien: Springer-Verlag 2005.

Engelhard & De Bruin 2018

Engelhard, E.F.D. & De Buin, R.W., *Liability for Damage Caused by Autonomous Vehicles*, The Hague: Eleven International Publishing 2018
Based on their contribution to .

English & Hammond 2018

English S. & Hammond, H., *Costs of Compliance 2018,* report by Thomson Reuters, available via the internet: https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2018.html (last accessed 24 August 2018, 17 p.

Evas 2018

Evas. T. ed., *EU Common Approach on the liability rules and insurance related to Connected and Autonomous Vehicles*, for the Directorate for Impact Assessment and European Added Value, with the Directorate General for Parliamentary Research Services (DG EPRS) of the General Secretariat of the European Parliament, February 2018. 129 p., which is available through http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf

Fagerberg & Mowery 2006

Fagerberg J. and Mowery D.C., *The Oxford Handbook of Innovation*, Oxford: Oxford University Press 2006.

Fagnant & Kockelman 2015

Fagnant, D.J., & Kockelman, K., "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations", *Transportation Research Part A*, 77 (2015), pp. 167 – 181.

Fairgrieve 2005

Fairgrieve, D., "'L'exception française? The French law of product liability", in: Fairgrieve (ed.), *Product Liability in Comparative Perspective*, Camridge: Cambridge University Press

Fairgrieve et al. 2016

Fairgrieve D., et al., "Product Liability Directive" in: Machnikowski, P. (ed.), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies,* Cambride (UK): Intersentia 2016, pp. 17-111.

Finn e.a. 2013

Finn, R.L, Wright, D. and Friedewald, M., "Seven Types of Privacy", in Gutwirth, S., e.a. (eds.), *European Data Protection: Coming of Age*: Dordrecht: Springer Science+Business Media 2013, pp. 3-33.

Gawronski 2019

Gawronski, M., "Chapter 8: Legal Remedies, Liability, Administrative Sanctions", in in Gawronski, M. (ed.), *Guide to the GDPR*, Kluwer Law International 2019, pp. 285-294.

Gawronski, Kloc, e.a. 2019

Gawronski, M., Kloc, K., et al., "Chapter 1: Basic Compliance", in Gawronski, M. (ed.), *Guide to the GDPR*, Kluwer Law International 2019, pp. 3-116.

Gawronski, Czarnowski e.a. 2019

Gawronski, M, Czarnowski, A.P. et al., "Chapter 2 DAT Subject's Rights"; "Chapter 3: Security"; and "Chapter 4: Data Processing", in Gawronski, M. (ed.), *Guide to the GDPR*, Kluwer Law International 2019, pp. 117-242.

Gawronski, Chomiczewski, e.a. 2019

Gawronski, M., Chomiczewski, W., et al., "Chapter 5: Managing Incidents and Data Breaches", in Gawronski, M. (ed.), *Guide to the GDPR*, Kluwer Law International 2019, pp. 243-262.

Gawronski & Kibil 2018

Gawronski, M., & Kibil, M., "Chapter 6: Data Protection Officer (DPO)", in in Gawronski, M. (ed.), *Guide to the GDPR*, Kluwer Law International 2019, pp 263-274.

González Castillo 2012

González Castillo, J., "Products Liability in Europe and the United States", *Revista Chilena de Derecho* 2012, vol. 39 no. 2, pp. 277-296.

Giesen 2001

Giesen, I., *Bewijs en aansprakelijkheid* (diss.), Den Haag: Boom Juridische Uitgevers 2001.

Giesen 2005

Giesen, I, *Handle with care! De waarschuwingsplicht in het buitencontractuele aansprakelijkheidsrecht*, Den Haag: Boom Juridische Uitgevers 2005.

Giesen 2009

Giesen, I., "II. The Burden of Proof and other Procedural Devices in Tort Law", in Koziol H., & Steininger, B.C. (eds.), *European Tort Law 2008*, Vienna: Springer Verlag 2009, p. 49-67.

Giesen 2012

Giesen I, "Attribution, Legal Causation and Preventive Effects", in: W.M. Giard (ed.), *judicial decision making in civil law – determinants, dynamics and delusions*, Den Haag: Eleven International Publishing 2012, p. 15-41.

Giesen & Rijnhout 2017

Giesen I., and Rijnhout, R., "Changing the Causation Requirement and Its Impact on Companies Faced with Tort Claims", in: Koster, Pennings & Rusu (eds.), *Essays on Private & Business Law – a tribute to Professor Adriaan Dorresteijn*, Den Haag: Eleven International Publishing, p. 83-107.

Giesen, De Jong & Muslat 2017

Giesen, I., De Jong, E., & Muslat, T., "The State of the Art of Product Liability in The Netherlands", in Kullman, H.J., Stöhr, K., Pfister, B., & Spindler, G., *Produzentenhaftung*, Berlin: Erich Schmidt Verlag 2017, p. 1-86.

Giesen 2019

Giesen, I., "Aansprakelijkheid, de wegbeheerder en het verkeer", *Verkeersrecht* 2019, 1, p. 2-8.

Glancy 2012

Glancy, D.J., "Privacy in Autonomous Vehicles", *Santa Clara Law Review* 2012, vol. 52, no. 4, p. 1171-1240.

Gunningham & Sinclair 1999

Gunningham, N. and Sinclair, D., "Regulatory Pluralism: Designing Porlucy Mixes for Environmental Protection", *Law & Policy* 1999, vol. 21, no. 1., p. 49-76.

Gunningham & Sinclair 2017

Gunningham, N. and Sinclair, D., "Smart Regulation", in: Drahos, P. (ed.), *Regulatory theory: foundations and applications,* Canberra: ANU Press 2017 (e-book version, via: press.anu.edu.au). pp. 711-724.

Guo, Meamari & Shen 2018

Guo, H., Meamari,E., & Shen, C-C, "Blockchain-inspired Event Recording System for Autonomous Vehicles", *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, Shenzhen, 2018, pp. 218-222, via https://ieeexplore-ieee-org.proxy.library.uu.nl/abstract/document/8606016 (last accessed 20 July 2020).

Gray 2020

Gray, O., "Trust through responsibility: Advertising and Self-Regulation in Europe", in De Cock Buning, M., de, & Senden, L.A.J. (eds.), *Private Regulation and Enforcement in the EU*, Oxford: Hart Publishers 2020, pp. 243-294.

Green Paper 2012

Christophe Leroux, Roberto Labruto, Chiara Boscarato and others, "Suggestion for a Green Paper on legal issues in robotics"), December 2012, available on the Internet at http://www.eu-robotics.net/cms/upload/PDF/euRobotics_Deliverable_D.3.2.1_Annex_Suggestion_GreenPaper_ELS_IssuesInRobotics.pdf (last accessed 28 January 2017).

Hartkamp & Sieburgh 2019

Hartkamp A.S. & Sieburgh, C.H., *Asser serie 6-II – De verbintenis in het algemeen, tweede gedeelte, 91 Art. 6:99 BW*, Deventer: Kluwer 2019, nrs. 91-97; 257-272; 273-294.

Hassan & De Filippi 2017

Hassan, S., and De Filippi, P., "The Expansion of Algorithmic Governance: From Code is Law to Law is Code", *The journal of field actions*, 2017 (special issue), no. 3, p. 88-90.

Heldeweg 2009

Heldeweg, M.A., *Smart Rules & Regimes – publiekrechtelijk(e) ontwerpen voor privatireing en technologische innovatie*, (inaugural lecture) Enschede: Universiteit Twente 2009. Available on the Internet at: https://www.utwente.nl/nl/bms/csd/medewerkers/oratie%20Michiel%20Heldeweg.pdf (last accessed 29 May 2018).

Howells 2005

Howells, G., "Defect in English Law", in Fairgrieve, D., (ed.), *Product Liability in Comparative Perspective*, Cambridge: Cambridge University Press 2005, pp. 138-155.

Hijma & Olthof 2017

Hijma, J., and Olthof, M.M., *Compendium Nederlands Vermogensrecht 2017* (digital edition), Wolters Kluwer 2017, nr. 433b.

Hirunyawipada & Paswan 2006

Hirunyawipada, T., & Paswan, A.K., "Consumer innovativeness and perceived risk: implications for high technology product adoption", Journal of Consumer Marketing 2006, Vol. 23 Issue 4, pp. 182 – 198.

Hoffmann-Riem 2006

Hoffmann-Riem, W., "Innovationsoffentheit und Innovationsverantwortung durch Recht, Aufgaben der rechtswissenschaftlicher Innovationsforschung", *Archiv des öffentlichten Rechts*, Band 131 (2006), p. 255-277.

Hosseini et al. 2016

Hosseini, M.H., Delaviz, M., Derakhshide, H. & Delaviz, M., "Factors Affecting Resistance to Innovation in Mobile Phone Industry", *International Journal of Asian Social Science*, 2016, 6(9), pp. 497 – 509.

Kamara 2017

Kamara, I., "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardization 'mandate'", in *European Journal of Law and Technology*, Vol 8, No 1, 2017, p. 1-24.

Kamara & De Hert 2018

Kamara, I., & De Hert, P., "Understanding the balancing act between the legitimate interest of the controller ground: a pragmatic approach", *Brussels Privacy Hub* – working paper, 12 August 2018, via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228369 (last accessed 14 July 2020).

Karner 2018

Karner, E., "A Comparative Analysis of Traffic Accident Systems", *Wake Forest Law Review*, 2018, vol. 53, p. 365-382.

Keirse 2016

Keirse, A.L.M., 'The Netherlands', in: Machnikowski, P. (ed.), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies,* Cambride (UK): Intersentia 2016, p. 311-359.

Keirse 2018

Keirse, A.L.M., "Hoofdstuk 3 – Kwalitatieve aansprakelijkheid (afd. 6.3.2)", in Hartlief et al., *Verbintenissen uit de wet en Schadevergoeding*, Deventer: Wolters Kluwer 2018, pp. 89-162.

Kitching 2007

Kitching, J., 'Chapter 9: Is Less More? Better Regulation and the Small Enterprise', in: Weatherill, S. (ed.), *Better Regulation*, Oxford: Hart Publishing, p. 155-173.

Klaassen & Kortmann 2012

Klaassen, C.J.M., & Kortmann, J.S., *Causaliteitsperikelen* (preadviezen), Deventer: Kluwer 2012.

Koops 2006

Koops, B.J., 'Should ICT Regulation Be Technology-Neutral', in: Koops, B.J., et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners,* IT & Law Series Vol 9, The Hague: T.M.C. Asser Press 2006, p. 77-108.

Koops 2014.

Koops, B.J., "The trouble with European data protection law", *International Data Privacy Law*, Volume 4, Issue 4, November 2014 pp. 250-261 doi: 10.1093/idpl/ipu023.

Kranenborg & Verhey 2018

Kranenborg, H.R. and Verhey, L.F.M., *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief*, Deventer: Wolters Kluwer 2018.

Kulk 2018

Kulk, S., *Internet Intermediaries and Copyright Law – Towards a future-proof EU legal framework*, Dissertation, Utrecht, 2018.

Kuner 2020

Kuner, Ch., "The Schrems II judgment of the Court of Justice and the future of data transfer regulation", *European Law Blog*, 17 July 2020, via https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/ (last accessed 24 July 2020).

Lavrijssen & Weitering 2019

Lavrijssen, N., & Wetering, M., "De zelfrijdende auto en het overmachtsverweer van art. 185 WVW", Verkeersrecht 2019/64, p. 1-7.

Lessig 2006

Lessig, L., *Code, version 2.0*, New York: Basic Books 2006.

Le Vine & Polak 2014

Le Vine, S. & Polak, J., "Automated Cars: A smooth ride ahead?", February 2014 available via http://www.theitc.org.uk/docs/114.pdf (last accessed 12 October 2017).

Lindenbergh 2018

Lindenbergh, S.D., "De wet affectieschade in werking", *Verkeersrecht* 2018/156, p. 1-13.

Lunney, Nolan & Oliphant 2017

Lunney, M., Nolan, D., and Oliphant, K., *Tort Law: Text and Materials*, Oxford: Oxford University Press 2017 (sixth edition).

Luppi & Parisi 2017

Luppi, B., and Parisi, F., "3. Rules versus Standards", in G. de Geest (ed.), *Encyclopedia of Law and Economics*, Cheltenham: Edward Elgar Publishers 2017, pp. 43 -53.

Machnikowski 2016

Machnikowski, P. (ed.), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies,* Cambride (UK): Intersentia 2016.

Machlup 1962

Machlup, F., *The Production and Distribution of Knowledge in the United States,* Princeton, NJ: Princeton University Press 1962.

Marchant & Lindor 2012

Marchant, G.E., and Lindor R.A., "The Coming Collision Between Autonomous Vehicles and the Liability System", *Santa Clara Law Review* vol. 52 no. 4, pp. 1321 – 1340.

Maxeiner 2008

Maxeiner, J., 'Some Realism About Legal Certainty in the Globalization of the Rule of Law', *Houston Journal of International Law*, Vol. 31:1 2008, p. 28 – 46.

Menting 2016

Menting M.-C., *Industry codes of conduct in a multi-layered Dutch private law* (diss.), Tilburg: Prisma Print 2016, available via https://pure.uvt.nl/ws/portalfiles/portal/23090135/Menting_Industry_07_12_2016_emb.pdf, last accessed October 11 2019.

Michalowicz & Lubasz 2019

Michałowicz, A., and Lubasz, D., "Chapter 7: The Regulator", in Gawronski, M. (ed.), *Guide to the GDPR*, Kluwer Law International 2019, pp 275-284.

Mohr 1969

Mohr, L., 'Determinants of innovations in organizations', *The American Political Science Review*, Vol. 63 No. 1, 111-126.

Oliphant & Wilcox 2016

Oliphant, K., and Wilcox, C, "England and Wales", in: Machnikowski, P. (ed.), *European Product Liability – An Analysis of the State of the Art in the Era of New Technologies,* Cambride (UK): Intersentia 2016, pp. 174-204.

Ostlund 1974

Ostlund, L.E., "Perceived Innovation Attributes as Predictors of Innovativeness". *Journal of Consumer Research* 1974, 3(1): 23-29.

Overheul 2018

Overheul, A.M., "Angst voor de dood als schade(post)", *Tijdschrift voor Vergoeding Personenschade* 2018 vol. 4, pp. 119-225

Oxford English Dictionary

Oxford English Dictionary, Oxford: Oxford University Press 2021.

Parker & Braithwaite 2003

Parker, C., and Braithwaite, J., 'Regulation', in: Cane, P. and Tushnet, M., (eds.), *The Oxford Handbook of Legal Studies,* Oxford: Oxford University Press 2003, pp. 119-145.

Pawsey 2013

Pawsey, A., 'Autonomous Road Vehicles', September 2013 via http://www.parliament.uk/briefing-papers/post-pn-443.pdf (last accessed 12 October 2017);

Pearson 2012

Pearson, S., 'Privacy, Security and Trust in Cloud Computing', in Pearson S., Yee G. (eds) Privacy and Security for Cloud Computing. Computer Communications and Networks. Springer, London. Available online via https://link.springer.com/chapter/10.1007/978-1-4471-4189-1_1.

Pelkmans & Renda 2017

Jacques Pelkmans & Andrea Renda, "Does EU regulation hinder or stimulate innovation", CEPS Special Report No. 96/2014.

Raitio 2003

Raitio, J., *The principle of legal certainty in EC law*, Dordrecht: Kluwer Academic Publishers 2003.

Ranchordás 2014

Ranchordás, S.H., *Sunset Clauses and Experimental Legislation: Blessing or Curse for Innovation?*, Zutphen: Koninklijke Wöhrmann 2014.

Rathee e.a. 2019

Rathee, G., et al., "A Blockchain Framework for Securing Connected and Autonomous Vehicles", *Sensors* 2019, vol. 19, no. 1365 p. 1-15.

Rezvani, Jansson & Bodin 2015

Rezvani, Z, Jansson, J., and Bodin, J., "Advances in consumer electric vehicle adoption research: A review and research agenda", *Transportation Research Part D* 34 2015, pp. 122-136.

De La Rochère & Milhac 2007

De La Rochère, J., and Milhac, O., "France", in: Campbell, C., *International Product Liability [2007]*, Yorkhill Law Publishing 2007, pp. 235-272.

Robolaw 2014

Erica Palmerini, Federico Azzarri, Fiorella Battaglia et al., D 6.2, "Guidelines on Regulating Robotics", 22 September 2014.

Rogers 2003, 1995

Rogers E.M. *Diffusion of Innovations*, New York: Free Press 2003 (5th edition), which builds upon the first edition that was published in 1995.

Rössler 2005

Rössler, B., *The Value of Privacy*, Cambridge: Polity Press 2005.

Rouhette, Gallage-Alwis & Houssel 2018

Rouhette, T., Gallage-Alwis, S., and Houssel, G., *Product liability and safety in France*, A Q&A guide to product liability and safety in France, part of the global guide to product liability and safety, Thomson Reuters 2018, available via https://uk.practicallaw.thomsonreuters.com/w-012-7018?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 and (global guide: www.practicallaw.com/productliability-guide, both last accessed 26 November 2019).

Rousseau et al. 1998

Rousseau, D.M., Burt, R.S., Sitkin, S., Camerer, C.F., "Not So Different After All: A Cross-discipline View of Trust", *The Academy of Management Review*, 1998, p. 393-404.

Sappideen & Vines 2011

Sappideen, C. & Vines, P., *Fleming's The Law of Torts*, Sydney: Thomson Reuters Australia/Lawbook Co., 2011.

Scharre 2018

Scharre, P., *Army of None: Autonomous Weapons and the Future of War*, New York: W. W. Norton & Company 2018.

Schellekens 2015
Schellekens, M., "Self-driving cars and the chilling effect of liability law", *Computer Law & Security Review* 2015, vol. 31, pp. 506-517.

Schrijns 2019
Schijns, A.J.J.G., "First partyverzekering voor verkeersongevallen", *Verkeersrecht* 2019/88, p. 1-10.

Schreuder 2014
Schreuder, A.I., "Aansprakelijkheid voor 'zelfdenkende' apparatuur, *Aansprakelijkheid, Verzekering & Schade,* 2014 vol. 5/6, no. 20, pp. 17-24

Schumpeter 1939
Schumpeter, J.A., *Business Cycles. A Theoretical, Historical and Statistical Analysis of the Capitalist Process*, New York, Toronto, London: McGraw-Hill Book Company 1939.

Schulz & Dankert 2016
Schulz, W., and Dankert, K., "'Governance by Things' as a challenge to regulation by law", *Internet Policy Review*, vol. 5 issue 2, p. 1-20.

Senden 2005
Senden, L.A.J., "Soft law, Self-regulation and Co-regulation in European Law: Where Do They Meet?", *Electric Journal od COmparatice Law*, col. 9, 1, January 2005.

Senden 2013
Senden, L.A.J., "Soft Post-Legislative Rulemaking: A Time for More Stringent Control", *European Law Journal* Col. 19, Issue 1, January 2013, p. 57-75.

Senden et al. 2015
Senden L.A.J., Kica, E., Hiemstra, M., and Klinger, K., "Mapping Self- and Co-regulation Approaches in the EU Context" – a study for the European Commission, DG Connect, Utrecht University, Renforce 2015.

Sharma 2020
Sharma, S., *Data Privacy and GDPR Handbook*, Hoboken (NJ): John Wiley & Sons Inc 2020.

Sieburgh 2017
Sieburgh, C.H., *Asser serie 6-II – De verbintenis in het algemeen, tweede gedeelte*, Deventer: Kluwer 2017, nrs. 47-91.

Sieburgh 2019
Sieburgh C.H., *Asser serie 6-IV – De verbintenis uit de wet*, Deventer: Kluwer 2019

Solove 2009

Solove, D.J., *Understanding Privacy*, Cambridge (MA) & London: Harvard University Press 2009.

Spier 2003

Spier, J., (ed). *Unification of tort law* (series): *liability for damage caused by others*, The Hague: Kluwer Law International 2003.

Sportes & Ravit 2019

Sportes, C., and Ravit, V., "France: Product Liability 2019", in: Williams, A. & Fox, T., *Product Liability Laws and Regulations 2019*, London: ICLG 2019, chapter available online via https://iclg.com/practice-areas/product-liability-laws-and-regulations/france (last accessed 26 November 2019).

Stewart 2010

Stewart, L.A., "The Impact of Regulation on Innovation in the United States: a Cross-Industry Literature Review", paper commissioned by the Institute of Medicine Committee on Patient Safety and Health IT, June 2010, available via http://www.itif.org/files/2011-impact-regulation-innovation.pdf (last accessed 2 February 2017).

Street 2016

Street, C. W., "Your pharmacist will soon be a robot", 2 may 2016, via http://www.breitbart.com/california/2016/05/02/pharmacist-will-soon-app-robot/ (last accessed 29 April 2017).

Strickland 2016

Strickland, E., "Autonomous Robot Surgeon Bests Humans in World First", *IEEE Spectrum* 4 May 2016, via http://spectrum.ieee.org/the-human-os/robotics/medical-robots/autonomous-robot-surgeon-bests-human-surgeons-in-world-first (last accessed 29 April 2017).

Takayama, Ju & Nass 2008

Takayama, L., Ju, W., and Nass, C., 'Beyond Dirty, Dangerous and Dull: What Everyday People Think Robots Should Do', conference paper HRI (Amsterdam) 2008, available via file:///C:/Users/Bruin134/AppData/Local/Google/Chrome/Downloads/Beyond_dirty_dangerous_and_dull_What_everyday_peop.pdf (last accessed 27 January 2017) .

Tanghe & Werbrouck 2021

Tanghe, J., & Werbrouck, J., "Hoofdstuk 13. De aansprakelijkheid voor schade veroorzaakt door de gebreken van autonome motorvoertuigen", in: De Bruyne, J., (ed.), *Autonome Motorvoertuigen – Een multidisciplinair onderzoek naar de maatschappelijke impact*, Brugge: Vanden Broele 2021, p. 321-354.

Taylor, Fairgrieve & Wester-Ouisse 2018

Taylor, S., Fairgrieve, D., and Wester-Ouisse, V., "Chapter 12. Medical Accidents and Pharmaceutical Product Liability in France", in Dyson, M. (ed.), *Regulating Risk through Private Law*, Cambridge: Intersentia 2018, pp. 301-322.

Thoe Schwartzenberg 2013

Schwartzenberg, H.W.B., thoe, *Civiel bewijsrecht voor de rechtspraktijk*, Apeldoorn: Maklu 2013.

Tjong Tjin Tai & Boesten 2016

Tjong Tjin Tai, E. and Boesten, S., "Aansprakelijkheid, zelfrijdende auto's en andere zelfsturende objecten", *NJB* 2016, 91(10), pp. 656-664.

Truli 2018

Truli, E., "The General Data Protection Regulation and Civil Liability", in Bakhoum, M., et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law -Towards a Holistic Approach?* Springer, 2018, p. 303-327.

Van Alsenoy 2016

Van Alsenoy, B., "Liability under EU Data Protection Law". *JIPITEC* 2016 vol. 7, no. 3, p. 271-288.

Van Dam 2005

Van Dam, C.C., 'Dutch case law on the EU Product Liability Directive', in: Fairgrieve, D. (ed.), *Product Liability in Comparative Perspective*, Cambridge (MA): Cambridge University Press 2005, p. 126-138.

Van Dam & Van Maanen 2010

Van Dam, C., and Van Maanen, G., "Traffic liability in The Netherlands", in: Ernst, W. (ed.), *The development of traffic liability,* vol 5., Cambridge: Cambridge University Press 2010, pp. 112-150.

Van Dam 2013

Van Dam, C., *European Tort Law* (second edition), Oxford: Oxford University Press 2013.

Van Gerven 2001

Van Gerven, W., *Tort Law – Ius Commune Casebooks for the Common Law of Europe*, Hart Publishing 2001.

Van der Heijden 2017

Van der Heijden, J., "Urban sustainability and resilience" in: Drahos, P. (ed.), *Regulatory theory: foundations and applications,* Canberra: ANU Press 2017 (e-book version, via: press.anu.edu.au). pp. 724-740.

Van der Sloot 2018

Sloot, B. van der, "Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities", in: Gutwirth, S., Leenes, R., & De Hert, P., *Data Protection on the Move*, Dordrecht: Springer 2018, pp. 411-437.

Van Slyke et al. 2004

Van Slyke, C., Belanger, F., and Comunale, C. L., "Factors influencing the adoption of web-based shopping: the impact of trust", *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* Volume 35 Issue 2, Spring 2004, pp. 32-49.

Van Wees 2015

Van Wees, K.A.P.C., "Aansprakelijkheidsaspecten van (deels) zelfrijdende auto's", *Aansprakelijkheid, Verzekering & Schade* 2015, vol 5, no. 28, pp. 170-180.

Van Wijk 2014

Van Wijk, M.A., *Verkeersaansprakelijkheid*, het civiele en strafrechtelijke schuldbegrip bij verkeersongevallen, Tilburg: Celsus 2014.

Veldt & Wissink 2017

Veldt, G.M. and Wissink, A.E.C., "Bewijslastverlichting voor de benadeelde bij productaansprakelijkheid voor onzekere risico's Annotatie bij HvJ EU 21 juni 2017, C-621/15, ECLI:EU:C:2017:484 (W. c.s./Sanofi Pasteur MSD SNC, Caisse primaire d'assurance maladie des Hauts-de-Seine, Carpimko)", *NTBR* 2019/36, pp. 253-263.

Vellinga 2014

Vellinga, N.E., "De civielrechtelijke aansprakelijkheid voor schade veroorzaakt door een autonome auto", *VR* 2014/151 (online edition), p. 1-11.

Vellinga 2020

Vellinga, N.E., *Legal Aspects of Automated Driving* (diss.), Groningen: University of Groningen 2020, via https://doi.org/10.33612/diss.112916838 (last accessed 11 August 2021).

Verhelst 2017

Verhelst, E.W., "Blockchain aan de ketting van de Algemene verordening gegevensbescherming?", *Privacy & Informatie*, vol. 1 2017, p. 17-23.

Viney & Guégan-Lécuyer 2010

Viney, G., and Guégan-Lécuyer, A., "The development of traffic liability in France", in Ernst, W., *The Development of Traffic Liability*, Cambridge: Cambridge University Press 2010, p. 50-75.

Von Bar 2009

Von Bar, C. (ed.), *Non-Contractual Liability Arising out of Damage Caused to Another*, Oxford: Oxford University Press 2009.

Von Grafenstein 2019

Grafenstein, M. von, "Co-regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design", in: Fuster, G.G., Brakel, M. van, & Hert, P. de, *Research Handbook on Privacy and Data Protection Law*, Cheltenham: Edward Elgar Publishing 2019, p. 2-30.

Von Schomberg 2011

Schomberg, R. von, 'Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields', in Schomberg, R. von (ed.), 'Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields', Report from the European Commission Services, Luxembourg: Publications Office of the European Union 2011.

Wadud, MacKenzie & Leiby 2016

Wadud, Z., MacKenzie D., & Leiby P., "Help or hindrance? The travel, energy and carbon impact of highly automated vehicles", *Transportation Research Part A: Policy & Practice* 86, pp. 1-18.

Walker Smith 2013

Walker Smith, B., "Human error as a cause for vehicle crashes", 18 November 2013, via http://cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes (last accessed 12 October 2017)

Walree 2017

Walree, T.F., "De vergoedbare schade bij onrechtmatige verwerking van persoonsgegevens", *WPNR* 25 november 2017/7172, p. 921-930.

Walree & Wolters 2020

Walree, T.F. and Wolters, P.T.J., "Het recht op schadevergoeding van een concurrent bij een schending van de AVG", *SEW* no. 1, January 2020, p. 2-10.

Walree 2021

Walree, T.F., *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens* (diss.), Onderneming & Recht, nr. 126, Deventer: Wolters Kluwer 2021.

Weimer & Marin 2016

Weimer, M. and Marin, L., 'The Role of Law in Managing the Tension between Risk and Innovation – Introduction to the Special Issue on Regulating New and Emerging Technologies', *European Journal of Risk Regulation* 2016 vol. 7 no. 3.

Westerdijk 1995

Westerdijk, R.J.J., *Produktenaansprakelijkheid voor software – Beschouwingen over de aansprakelijkheid voor informatieprodukten*, non-published version used; published edition: Deventer: Kluwer 1995 (Reeks Informatica en Recht, deel 16.

Wiesenfeld 2003

Wiesenfeld, K.G., *Erection of Industry and Alignment of Rights*, (original 1871, reprint in 2003), as edited by Van Veen, A., Heimans, R., Smit Duijzentkunst, B., et al., Utrecht: Inter Pares 2003.

Williams 1951

Williams, G., "7 The Aims of the Law of Tort", *Current Legal Problems*, 1951, vol. 4 no. 1., pp. 137-176, also partially cited in Lunney, Nolan & Oliphant 2017, p. 18-19.

Williams & Scharre (eds.) 2015

Williams, A.P., and Scharre, P.D., *Autonomous Systems – Issues for Defence Policymakers*, The Hague: NATO Communications and Information Agency 2015.

Wuyts 2014

Wuyts, D., "The product liability directive – more than two decades of defective products in Europe", *JETL* 2014, 5(1).

Wyffels 2021

Wyffels, F., "Hoofdstuk 1. Van motorvoertuig tot autonome robot", in: De Bruyne, J., (ed.), *Autonome Motorvoertuigen – Een multidisciplinair onderzoek naar de maatschappelijke impact*, Brugge: Vanden Broele 2021, p. 23-39.

Yeomans 2014

Yeomans, G., "Autonomous Vehicles – handing over control: opportunities and risks for insurance", via https://www.lloyds.com/~/media/lloyds/reports/emerging%20risk%20reports/autonomous%20vehicles%20final.pdf (last accessed on 12 October 2017).

European Commission/European Parliament/European Union/OECD

OECD 2005

Organisation for Economic Co-operation and Development & Statistical Office of the European Communities, 'Oslo Manual, Guidelines for Collecting and Interpreting Innovation Data', third edition, Paris: OECD Publishing 2005.

European Commission 1995

First report on the application of council directive on the approximation of laws, regulations and administrative provisions of the member states concerning liability for defective products (85/374/EEC), 13 December 1995, COM(95)617 final.

European Commission 2000

Report from the Commission on the application of Directive 85/374 on Liability for Defective Products, 31 January 2001, COM(2000) 893 final.

European Commission 2004

European Commission 2001, "European Governance – a white paper", COM(2001) 428 final.

European Commission 2006

Report from the Commission to the Council, the European Parliament and the European Economic and Social Committee, Third report on the application of council directive on the approximation of laws, regulations and administrative provisions of the member states concerning liability for defective products (85/374/EEC of 25 July 1985, amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999), 14 September 2006, COM(2006) 496 final.

European Commission 2010

Communication from the Commission, 'Europe 2020, A strategy for smart, sustainable and inclusive growth', COM(2010) 2020 final.

European Commission 2011

Report from the Commission to the Council, the European Parliament and the European Economic and Social Committee, Fourth report on the application of council directive 85/374/EEC of 25 July 1985 on the approximation of laws, regulations and administrative provisions of the member states concerning liability for defective products amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999, 8 September 2011, COM(2011) 547 final.

European Commission 2012
Communication from the Commission, 'Horizon 2020 – The Framework Programme for Research and Innovation', SEC(2011 1427 & 1428 final, COM(2012) 808 final.

European Commission 2016
Commission Staff Working Document, 'Better regulations for innovation-driven investment at EU level', via https://ec.europa.eu/research/innovation-union/pdf/innovrefit_staff_working_document.pdf (last accessed 28 January 2017).

European Commission 2016a
Report from the Commission to the European Parliament and the Council, '**Saving Lives: Boosting Car Safety in the EU Reporting on the monitoring and assessment of advanced vehicle safety features, their cost effectiveness and feasibility for the review of the regulations on general vehicle safety and on the protection of pedestrians and other vulnerable road users', COM(2016) 787 final, via** http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0787&from=EN **(last accessed 12 October 2017).**
European Commission 2016b
European Commission, Commission Staff Working Document "Better Regulations for innovation-driven investment at EU level, 2016.

European Commission 2017
European Commission, Commission Staff Working Document, "Better Regulation Guidelines", SWD(2017) 350 final.

European Commission 2017a
European Commission, "Better regulation "Toolbox"," complementing Commission Staff Working Document, "Better Regulation Guidelines", SWD(2017) 350 final, available via https://ec.europa.eu/info/sites/info/files/better-regulation-toolbox_1.pdf, and https://ec.europa.eu/info/law/law-making-process/better-regulation-why-and-how_en (accessed 12 August 2019).

European Commission 2018
Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) {SWD(2018) 157 final} {SWD(2018) 158 final}, COM(2018), via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:246:FIN

European Commission 2018a
Communication from the Commission to the European Parliament, the Council, the European Economic

and Social Committee, The Committee of the Regions on "the road to automated mobility: An EU strategy for mobility of the future", COM(2018) 283 Final, via https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf (last accessed 21 December 2018).

European Commission 2018b

Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products, Final Report, doi: 10.2873/477640, available via https://publications.europa.eu/en/publication-detail/-/publication/d4e3e1f5-526c-11e8-be1d-01aa75ed71a1/language-en (last accessed 27 February 2019).

European Commission 2018c

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A renewed European Agenda for Research and Innovation – Europe's chance to shape its future", COM(2018) 306 Final, via https://ec.europa.eu/info/sites/info/files/com-2018-306-a-renewed-european-agenda-_for_research-and-innovation_may_2018_en_0.pdf (last accessed 23 April 2021).

European Commission 2018d

European Commission, European Road Safety Observatory, report "Autonomous Vehicles & Traffic Safety", 2018, available via https://ec.europa.eu/transport/road_safety/sites/default/files/pdf/ersosynthesis2018-autonomoussafety.pdf (last accessed 11 August 2021).

European Commission 2019

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Better regulation: taking stock and sustaining our commitment", COM(2019) 178 final.

European Commission 2020

Report from the Expert Group on Liability and New Technologies – New Technologies Formation, "Liability for Artificial Intelligence and other emerging digital technologies", DOI:10.2838/573689, via https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608 (last accessed 20 May 2020).

European Commission 2021

European Commission, "Horizon Europe Strategic Plan (2021-2024)", February 2021, doi:10.2777/083753, via https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/3c6ffd74-8ac3-11eb-b85c-01aa75ed71a1 (last accessed 31 March 2021).

European Commission 2021a; Proposed AIR

European Commission, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts", COM(2021) 206 final, via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (last accessed 11 August 2021).

European Innovation Scoreboard 2016

European Commission, 'European Innovation Scoreboard 2016', via http://ec.europa.eu/DocsRoom/documents/17822 (last accessed 28 January 2017).

State of the Innovation Union 2014

European Commission, 'State of the Innovation Union Taking Stock 2010-2014', COM(2014) 339, via http://ec.europa.eu/research/innovation-union/pdf/state-of-the-union/2013/state_of_the_innovation_union_report_2013.pdf (last accessed 28 January 2017).

European Parliament 2017

European Parliament, Committee on Legal Affairs, 'Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), A8-0005/2017 (27.1.2017), via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0005+0+DOC+PDF+V0//EN (last accessed 17 July 2017).

European Parliament 2020

European Parliament, Committee on Legal Affairs, 'Draft Report with recommendations to the Commission on a civil liability regime for artificial intelligence' (2020/2014(INL).

European Parliament 2020(a)

European Parliament Resolution P9_TA(2020)0267. 'Civil liability regime for artificial intelligence: European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).

IIA 2003

Interinstitutional Agreement (European Parliament, Council & Commission) on Better Law-making, 13 December 2003, *OJ* 31 December 2003, C 32. Via: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003Q1231(01)&from=EN (last accessed 23 Aug. 19).

IIA 2016

Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Lawmaking, 13 April 2016, *OJ* 12 May 2016, L 123. Via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016Q0512(01)&from=EN.

OECD 2013

OECD, "OECD Factbook 2013: Economic, Environmental and Social Statistics", 2013, via http://www.oecd-ilibrary.org/sites/factbook-2013-en/06/02/03/index.html?contentType=&itemId=/content/chapter/factbook-2013-50-en&containerItemId=/content/serial/18147364&accessItemIds=&mimeType=text/html. (last accessed 12 October 2017).

OECD 2015

OECD, "Industry Self Regulation – role and use in supporting consumer interests", *OECD Digital Economy Papers* No. 247, 2015.

Norms & Standards

SAE J3016_201609

SAE International, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016-201609, available via https://www.sae.org/standards/content/j3016_201609/.

SAE J3016_202104

SAE International, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016-202104, available via https://www.sae.org/standards/content/j3016_202104/.

WP29 and EDPB documents

WP29 (125)

Article 29 Data Protection Working Party, "Working document on data protection and privacy implications in eCall initiative", 26 September 2006, 1609/06/EN WP 125, via https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf (last accessed 13 July 2020).

WP29 (136)

Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, 01248/07/EN WP 136, via https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (last accessed 9 July 2020).

WP29 (196)

Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", 1 July 2012,

01037/12/EN WP 196, via https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (las accessed 31 July 2020).

WP29 (216)

Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques", 10 April 2014, 0829/14/EN WP216, via https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed 9 July 2020).

WP29 (217)

Article 29 Data Protection Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC", 9 April 2014, 844/14/EN WP 217, via https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last accessed 14 July 2020).

WP29 (242)

Article 29 Data Protection Working Party, "Guidelines on the right to data portability", 13 December 2016, revised on 5 April 2017, 16/EN WP 242 rev.01, via https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 (last accessed 20 July 2020).

WP29 (243)

Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers ('DPOs')", 16/EN WP 243 rev.01, via http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 (last accessed 22 July 2020).

WP29 (248)

Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 17/EN WP 248 rev.01, via http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 (last accessed 22 July 2020).

WP29 (250)

Article 29 Data Protection Working Party, "Guidelines on Personal data breach notification under Regulation 2016/679", 3 October 2017, revised on 6 February 2018, 18/EN WP250 rev.01, via https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 (last accessed 22 July 2020).

WP29 (251)

Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profilingf or the purposes of Regulation 2016/679", 3 October 2017, revised on 6 February 2018, 17/EN WP 251 rev.01, via https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826 (last accessed 21 July 2020).

WP29 (253)

Article 29 Data Protection Working Party, "Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679", 3 October 2017, 17/EN WP 253, via https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 (last accessed 27 July 2020).

EDPB 3/2018

European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, 7 January 2020, via https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_0.pdf (last accessed 13 July 2020).

EDPB 1/2019

European Data Protection Board, "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, via https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf (last accessed 22 July 2020).

EDPB 4/2019

European Data Protection Board, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", 13 November 2019, via https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf (last accessed 21 July 2020).

EDPB 05/2019

European Data Protection Board, "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities", 12 March 2019, via https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf (last accessed 14 July 2020).

EDPB 01/2020

European Data Protection Board, "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", v. 1.0, adopted on 28 January 2020, via https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf (last accessed 13 July 2020).

EDPB 05/2020

European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679", version 1.1, 4 May 2020, via https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (last accessed 14 July 2020).

EDPB 07/2020

European Data Protection Board, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", version 1.0, Adopted on 02 September 2020, via https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (last accessed 16 September 2021).

EDPB 2020a

European Data Protection Board, "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 -Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems", 23 July 2020, via https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf (last accessed 28 July 2020).

EDPB 2020b

European Data Protection Board, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", 10 November 2020, via https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (last accessed 5 January 2021).

EDPB 2020c

European Data Protection Board, "Recommendations02/2020on the European Essential Guarantees for surveillance measures", 10 november 2020, via https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (last accessed 5 January 2021).

AP/CBP documents

CBP 2013

College Bescherming Persoonsgegevens, CBP Richtsnoeren: Beveiliging van persoonsgegevens", *Staatscourant* nr. 5174, 1 March 2013, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_beveiliging_van_persoonsgegevens.pdf (last accessed 21 July 2020).

AP 2018

Schermer, B.W., Hagenauw, D., & Falot, N, "Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming", Autoriteit Persoonsgegevens 2018, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf (last accessed 14 July 2020).

AP 2019

Autoriteit Persoonsgegevens, "Normuitleg grondslag 'gerechtvaardigd belang'", 1 November 2019, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf (last accessed 14 July 2020).

AP 2019(a)

Autoriteit Persoonsgegevens, "Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019)", *Staatscourant* nr. 14586, 14 maart 2019, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf (last accessed 27 July 2020).

CNIL documents

CNIL 2018

Commission Nationale de l'Informatique et des Libertés, "Connected vehicles: a compliance package for a responsible use of data", 13 February 2018 (living document), via https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data, (last accessed 13 July 2020.

CNIL 2018a

Commission Nationale de l'Informatique et des Libertés, "Security of Personal Data", *the CNIL'S Guides 2018*, via

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf (last accessed 20 July 2020).

ICO documents

ICO 2019

Information Commisioner's Office, "Guide to the General Data Protection Regulation (GDPR)", 22 May 2019 – 1.0.715, via https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (last accessed 14 July 2020).

Industry standards/proposals

ACEA 2015

European Automobile Manufacturers Association (ACEA), "ACEA Principles of Data Protection in Relation to Connected Vehicles and Services", September 2015, via https://www.acea.be/uploads/publications/ACEA_Principles_of_Data_Protection.pdf (last accessed 21 July 2020).

CCAV 2017

Center for Connected and Autonomous Vehicles, "Guidance The key principles of vehicle cyber security for connected and automated vehicles", 6 August 2017, via https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles (last accessed 21 July 2020).

VDA 2014

Verband der Automobilindustrie "Data Protecion Principles for Connected Vehicles", 3 november 2014, via https://www.vda.de/dam/vda/Medien/EN/Themen/Innovation-und-Technik/Vernetzung/Datenschutz-Prinzipien/vda-data-protection-principles.pdf (last accessed 21 July 2020).

VDA & German DPAs 2016

Verband der Automobilindustrie & Data Protection Authorities of the Federal and State Governments of Germany, "Data protection aspects of using connected and non-connected vehicles", 26 January 2016, via https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf (last accessed 21 July 2020).

CURRICULUM VITAE

Roeland Wieger de Bruin is Assistant Professor of Law and Technology at Utrecht University. He works parttime for the Law Department of the REBO-faculty, Molengraaff Institute for Private Law and the Center for Intellectual Property Law (CIER). He participates in the UCALL- and RENFORCE research groups. In both his research and the courses he teaches, Roeland focusses on the interplays between law and technology in a broad sense, and specialises in the regulation of Artificial Intelligence which started with his contribution to the Eurobotics-forum in 2011. From that moment onwards, he participated amongst other things in the FET-Flagship proposal Robot Companions for Citizens, and co-founded together with Madeleine de Cock Buning and Lucky Belder the Center for Access to and Acceptance of Autonomous Intelligence, which is currently part of CIER.

Besides his academic activities, Roeland works as *advocaat* (attorney-at-law) for KienhuisHoving N.V. in Enschede, where he participates in the PRITIE-team which is specialised in law and technology within *inter alia* the privacy, intellectual property and information technology disciplines. Also there, he focusses on those areas where AI meet law. Furthermore, he runs a – very small – company (Websession) in the business of the design and development of web-technology.

Roeland obtained his LL.B. (with a minor in information science) and LL.M. degrees in Dutch Law at Utrecht University and a second LL.M. in Information Law at the University of Amsterdam.

However, above all, Roeland is a music enthusiast. He has played the violin, viola and piano in many ensembles (the UvA-Orchestra J.Pzn Sweelinck, NSO and NESKO in which he participated as a student, and the current ensembles Collegium Musicum Traiectum and his legendary duet-partners Oksana Ivashchenko and Iris van Gogh must certainly be mentioned here) and endeavours to promote music in a broad sense.

NASCHRIFT EN DANKWOORD

Het hoofdthema van dit promotieonderzoek is *verplaatsing.* Hierboven treft u het verslag van mijn zoektocht aan de hand van diverse variaties rond dat thema. Autonome voertuigen, de voorwerpen van mijn onderzoek, hebben verplaatsing van mens en goed als belangrijkste doel. Om tot betere regulering te komen, concludeer ik dat eveneens verplaatsing nodig is – ditmaal van bepaalde juridische ankerpunten voor innovatoren en consumenten. Daartoe schets ik een aantal mogelijke routes die de wetgever als aanwijzing zou kunnen gebruiken.

Daarnaast heb ikzelf – uiteraard met name vóór SARS-CoV-2 alles ontregelde – diverse verplaatsingen ondergaan door of voor mijn onderzoek. In Västerås, gelegen aan een destijds indrukwekkend bevroren Zweeds meer, raakte ik enthousiast voor het onderwerp. In Hong Kong ging ik in gesprek met deelnemers aan van de Digital Asia Hub, aan de hand van mijn twee minuten (!) durende "lightning speech" over regulering van AVs in Europa en Azië. De ICRES-congressen in Lissabon en – met name Troy, New York – bleken buitengewoon vruchtbare voedingsbodems voor de delen omtrent de wisselwerking tussen recht en innovatie. Spannend was het om in Brussel voor een werkgroep van het Europees Parlement enkele resultaten te presenteren van het onderzoek dat ik samen met Esther Engelhard mocht doen. Voor de afronding van het promotieonderzoek was er geen betere plek dan "het Boshuisje" denkbaar.

Ook op reizen met een ander thema dan het onderzoek in kwestie, sijpelden mijn academische verplaatsingen nogal eens door in het dagprogramma. Přední Labská, Oudega, Feistritz-am-Wechsel en de achtertuin bleken bij uitstek geschikt om toch nog even een paar commentaren te verwerken of wat nieuwe bronnen te raadplegen.

Enfin, de belangrijkste verplaatsingen wat dit onderzoek betreft zitten erop, of ze staan op papier. Deze tour kon ik niet maken zonder de niet aflatende steun van een groot aantal collegae, vrienden en familie, waarvan ik er een aantal langs deze weg wil adresseren. Promotoren Madeleine, Ivo en Elbert: dank voor de strategische, praktische en inhoudelijke tips – tot op de dag van vandaag. Onze ontmoetingen waren zonder uitzondering gezellig en nuttig: ik ga ze missen! Lucky, heel veel dank voor jouw ideeën, het meelezen, helpen opbouwen en faciliteren van mijn boek, en alle gezelligheid daaromheen. Stefan, dank voor jouw ervaringsdeskundigheid en het willen fungeren als inhoudelijke boksbal, en samen met Stijn voor het helpen organiseren van de promotie. KienhuisHoving- en eerder Mitopics-collega's Eduard en Lesley ben ik erkentelijk voor het tolereren van zo'n promoverende eend in de bijt, en voor het becommentariëren van bepaalde stukken van het onderzoek. Jaarclub Inter Pares: dank voor de morele en inhoudelijke ondersteuning. Loes en Kim, dank voor het meelezen van het Nederlandse deel, respectievelijk het broodnodige "uitzoomen" – en voor jullie onvoorwaardelijke vriendschap. Willem, Cisca,

Guido en Allard: dank voor de ruimte die jullie mij boden – ook tijdens de zomer- en winterreizen, en het bieden van de noodzakelijke afleiding bij teveel tunnelvisie. Oksana, zonder onze muzikale verwantschap was dit boek er nooit gekomen.

Tot slot ben ik de allergrootste dank verschuldigd aan Iris, Milan en Olivier. Jullie hielden niet alleen het vuur brandend, maar moesten ook de grootste hitte daarvan doorstaan. Iris, dank voor het meelezen, zeker jouw biologenkijk op mijn teksten is zeer verhelderend gebleken. Ook dank voor de steun en de gelegenheid die je mij bood om mij op belangrijke momenten even te laten begaan. Milan en Olivier waren uiteindelijk dé drijfveren om dit onderzoek zo snel mogelijk te voltooien. Dit boek draag ik met trots op aan jullie!