FACULTY OF LAW
Lund University

Gustav Juhlin

To err is human; but to drive, or not to drive, that, is the question

A Comparative Study of Artificial Intelligence, Crime and Liability Especially in Relation To Autonomous Traffic

LAGM01 Master Thesis

European Business Law
30 higher education credits

Supervisor: Aurelija Lukoseviciene

Term: Spring 2022

Abstract

As progress is rapidly made in the spheres of computation and artificial intelligence the implementation of new artificial intelligence technologies becomes a more and more significant part of our everyday lives. One application that garners a lot of attention, making promises in the forms of lessened congestion, increased safety and a line of other benefits to society is the autonomous car. While testing of autonomous cars is well underway in many parts of the world, they still have not been fully let into traffic - this, however, is something that experts believe will be a reality shortly. Despite this there are already multiple accidents that have already been caused by these vehicles, as well as instances of crimes committed by these autonomous vehicles, mainly due to some form of third party interference.

The risks that are brought forward by the potential full scale implementation of autonomous vehicles beg the question of who is to be liable for damages arising in the events of an accident, or be liable for crimes committed by a car operating autonomously. This is what this thesis is set out to investigate. The focus of the thesis will lay on a string of proposals made by the European Parliament on general principles and concepts to be applied in the question of liability in relation to artificial intelligence, and comparing these to a more concrete proposal for the specific regulation of autonomous road traffic laid out by the Swedish Government.

The solutions are identified and discussed weighing benefits and drawbacks against each other, and one particularly controversial solution in the shape of a legal personhood for AI-agents is discussed, especially in relation to the attribution of criminal liability to these agents.

The thesis concludes as the author presents his own opinions, suggesting a solution that draws heavily on a combination of both the European Parliament and the Swedish Proposals, with some improvements and clarifications in areas where the proposals were found to be lacking.

Sammanfattning

Allteftersom stora framsteg görs i datorernas värld och inom artificiell intelligens ser samhället en allt större implementering av artificiell intelligence-teknologi i människors vardag. En sådan implementering är autonoma, självkörande, fordon. Detta är en teknologi som lovar stora framsteg inom fordonssäkerhet, lägre utsläpp till följd av mindre köbildning och en rad andra samhällsvinster. Det utförs redan idag tester av dessa fordon, men de har inte ännu släppts ut i allmän trafik, detta är emellertid något experter tror kommer ske inom kort. Trots detta har en rad olyckor orsakats av fordonen. Även trafikbrott har begåtts av dessa fordon, ofta till följd av inblandning från tredje part.

Riskerna för att fler olyckor och trafikbrott sker i samband med användningen av autonoma fordon, till följd av en storskalig implementering av dessa, bringar med sig frågan om hur ansvar skall fördelas, både det civilrättsliga ansvaret vid exempelvis ett olycksfall, och det brottsansvar vid exempelvis trafikbrott. Detta är frågan som ämnar undersökas i denna uppsats. Arbetet kommer fokusera på en rad förslag som framlagts av Europaparlamentet, dels allmänt hållna förslag kring fördelningen av civilrättsligt ansvar vid användning av artificiell intelligens, dels förslag för autonom trafik i stort. Dessa kommer jämföras med de lösningar för ansvarsfördelning som framlagts av Sveriges Riksdag, specifikt för autonom vägtrafik.

De lösningar som identifieras kommer diskuteras, för- och nackdelar kommer vägas mot varandra, och ett särskilt kontroversiellt förslag kring att attribuera artificiell intelligens med en elektronisk juridisk personlighet diskuteras, särskilt i samband med möjliga lösningar för att tillskriva artificiell intelligence med brottsansvar.

Uppsatsen avslutas med en presentation av författarens egna uppfattningar och förslag kring hur ansvarsfrågan med hänsyn till autonom vägtrafik bör hanteras. Denna uppfattning faller i stort i linje med förslagen både från Europaparlamentet, och Sveriges Riksdag, men vissa förbättringar och förtydligande föreslås för de områden där författaren uppfattat brister i befintliga förslag.

Abbreviations

AI - Artificial Intelligence

EU - European Union

GPS - Global Positioning System

NHTSA - National Highway Traffic Administration

SAE - Society of Automotive Engineers

SFS - Svensk Författningssamling

SUV - Sport Utility Vehicle

Table of Contents

1. Prelude

1.1 Introduction

Computers and man made intelligence have long been a subject of fascination not only in science but in society at large, countless are the movies where humanity battles an artificial entity capable of humanlike or superhuman intelligence. Today computers have become more than a tool to be controlled by humans, it has become an entity of its own, capable of feats previously unknown to man. There are warehouses operating almost entirely under the guidance of artificial intelligence, AI, AI-guided missiles, autonomous cars, along with a myriad of other products powered by AI.

This surge of use of AI affects a plethora of fields, notably customer support in the form of chat bots, smart homes, as well as the medical sector, where AI is used in diagnosing, treatments, and decision making.[1] The world also sees rapid advancements in the world of driver assistance systems and fully autonomous vehicles; both personal vehicles, taxis and large scale transportation.

Seeing how the world may soon regularly see multiple tonne machines rolling in public streets, without the control of a human, the question of what happens when mistakes are made, either on behalf of, or by, these AI Systems arises. What if an autonomous vehicle suddenly turns off the road, accelerates, brakes, commits an act that would fall within the definitions of traffic crimes or otherwise causes an accident leading to property damage, injury or even death? Who is to blame for the mistakes of AI? This all might sound like a potentiality, something for future concern, but these situations are already here. Furthermore, they will, without a doubt, become more and more common as an increasing number of makers adapt others', or adapt their own, solutions for autonomous traffic.

[1] PwC 'No longer science fiction, AI and robotics are transforming healthcare', <https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html> accessed 2 March 2022.

AI aspects of vehicles, frm simpler driver like assistance tools, e.g. lane assists, that take action when the car seems to be swerving out of lane and adaptive cruise control that keeps an even speed but is able to adapt to sudden changes in the traffic flow, to full scale autonomous vehicles are viewed by many experts as a way of increasing safety in traffic.

Autonomous vehicles are largely viewed to be the next step in increasing safety, a view that is supported National Highway Traffic Safety Administration of the United States, NHTSA, looks favourably on both the current safety systems available to customers, as well as the potential future safety benefits of high automation level autonomous vehicles, seeing it as one of the biggest promises of the technology.[2]

However, As early as 2018 we saw the first pedestrian death involving an autonomous vehicle, a Volvo SUV owned by Uber hit a pedestrian on a four lane crossing in Arizona, killing her. This car was part of Uber's fully autonomous vehicle tests, and the car was equipped with a safety driver in the front seat. In this case the driver was fully capable, and there to, control the car in case it would malfunction or otherwise not behave as intended, and the safety driver was later charged with negligent homicide. Uber and Volvo were both excluded from any criminal prosecution.[3] In the matter of civil liability Uber secretly settled with the family of the victim, leaving the question of liability open.[4]

These auto-pilot systems have also been shown to be susceptible to both physical and digital third party interference. Israeli cybersecurity firm Regulus Cyber, in 2019, was able to disturb the autonomous software of a car by feeding it faulty GPS coordinates, causing it to switch lanes, turn off the road, brake heavily and speed up

[2] NHTSA, Automated Vehicles for Safety
<https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>
Accessed 2 March 2022.

[3] Timothy B. Lee, ‘Safety driver in 2018 Uber crash is charged with negligent homicide’, ARS Technica (16 September 2020).
<https://arstechnica.com/cars/2020/09/arizona-prosecutes-uber-safety-driver-but-not-uber-for-fatal-2018-crash/>
Accessed 2 March 2022.

[4] Conny Loizos, ‘Uber has settled with the family of the homeless victim killed last week’, TechCrunch (30 March 2018).
<https://techcrunch.com/2018/03/29/uber-has-settled-with-the-family-of-the-homeless-victim-killed-last-week>
Accessed 2 March 2022.

and even honk the horn, all outside of the control of the driver.[5] In an experiment conducted by McAfee researchers it was also shown that a car on auto-pilot could be fooled by a small sliver of tape being placed on a sign signaling thirty-five miles per hour, to then instead interpret it to be a sign for eighty-five miles per hour, accelerating to more than twice the speed limit.[6] Who is to be held accountable for these traffic crimes, when they are committed completely at the discretion of the autonomous vehicles? This needs to be addressed by lawmakers, both at an international and a national level.

The European Parliament has made a line of proposals on principles for the attribution of civil liability, as well as a civil law for AI and a resolution on autonomous driving. In the proposals the European Parliament set out principles and guidelines that, while unbinding in their current form, could shape how regulations on the subject are formulated, adapted and applied throughout the European Union going forward. In these proposals a multitude of different models for liability are discussed, including the highly controversial possibility of creating a whole new legal class, or legal personhood for capable AI-agents. The proposals divide AI-agents into high-risk and non high-risk - and autonomous vehicles fall into the high-risk category.

In the light of these issues, there are countries that are on the forefront of regulating the area of autonomous traffic, paving the way for vehicles with a higher degree of automation to enter traffic amongst regular vehicles. In this group of vanguardian countries we find Sweden who proposes a law for the complete introduction of these vehicles into traffic. In the light of this legislative proposal it is of great interest to comparatively study and discuss the allocation of both civil and criminal liability in cases involving autonomous vehicles in both the Swedish and European Parliament proposals, as a fully adopted legislation at European Union level would likely become binding on Member States in the future.

[5] Felix Björklund, ‘Lurade Tesla att köra fel: ”Ett alarmerande svar”’, NyTeknik (25 June 2019) <https://www.nyteknik.se/fordon/lurade-tesla-att-kora-fel-ett-alarmerande-svar-6962918> Accessed 2 March 2022.

[6] Steve Povolny ‘Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles’, McAfee Labs (19 February 2020) <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/> Accessed 2 March 2022.

1.2 Purpose And Research Question

In the light of the novelty of autonomous vehicles, the implications they have on existing principles of liability and the rapid advancements made in the sphere of AI and autonomous vehicles, the purpose of this thesis is to comparatively study alternative principles and models proposed by the European Parliament for the attribution of liability in relation to AI, and the more concrete and specific legislative proposal for the regulation of autonomous traffic made by the Swedish government.

The thesis deals with the issue of civil and criminal liability in relation to self-driving vehicles, a type of artificial intelligence. The intention is to investigate principles and possible solutions for the attribution of such liability. In investigating this the author intends to answer;

1. *‘What EU-level proposed principles and possibilities exist for the attribution of civil and criminal liability in relation to autonomous vehicles?’,*
2. ‘*What concrete solutions for the attribution of civil and criminal liability are suggested in the Swedish draft legislation on autonomous vehicles?’* and;
3. *‘’Is it realistically possible to attribute an artificial intelligence agent with civil or criminal liability qua some sort of legal personality?’*

Additionally the author intends to finally present his opinion on what he considers the most reasonable way forward to be.

1.3 Material and Methodology

This is an investigative comparative study focusing on discussing and comparing legislative proposals on issues relating to liability, AI and autonomous vehicles. These proposals will be the main concern of the thesis. In fulfilling the purpose of the essay, as stipulated in the previous section, research will first focus on AI in general, to provide the reader with an understanding of basic concepts of AI, drawing information mainly from secondary sources. In illustrating issues regarding artificial intelligence and autonomous vehicles various news articles have been consulted, as the novelty of the subject garners a large amount of publicity in the event of an accident.

The thesis also touches upon the general concepts of criminal and civil liability, discussing these concepts with the support of doctrinal research in the shape of both literary works and research articles, public print, as well as other secondary sources such as technical articles and other materials chosen with respect to their relevance to the subject. The attribution of civil liability is discussed at length, mainly based on the legislative proposals, but also in the light of external opinions on the different solutions for the attribution that are proposed within them. This discussion extends both to the more generally held discussion of attributing liability to artificial intelligence, as well as the more specific and concrete attribution of liability in relation to autonomous traffic.

The attribution of criminal liability is discussed largely on the basis of research and opinions of Gabriel Hallevy, but also in the light of the proposals both on the attribution of criminal liability to AI in general, and in relation to autonomous vehicles, as well as opinions contradictory to those of Hallevy.

The analysis is strengthened through the reliance on a multitude of expert sources, discussing aspects of the material critically to form opinions on the topic. The author intends to remain critical of the material as to be able to draw conclusions *de lege ferenda*.

1.4 Scope and Delimitations

The thesis focuses on the issues of legal personhood, criminal- and civil liability in relation to autonomous vehicles in particular, but will extend to more generally held proposals on AI and liability, as autonomous vehicles intersect the sphere of AI. While there are many aspects to be considered in relation to artificial intelligence the thesis will remain focused on this, refraining from commenting on purely ethical considerations as well as other forms of liability.

The thesis is limited to comparing the proposals for the attribution of liability in relation to AI, as applicable to autonomous vehicles, and the more concrete Swedish legislative proposal for autonomous traffic. I will refrain from discussing any other eventual legal orders on the subject. Aside from the focus on general AI-liability and the focus on liability and autonomous vehicles there will be no deep diving discussion on any other type of artificial intelligence.

1.5 Disposition

Following the introductory prelude the reader will be given an introduction to AI, focusing on the definition, categorization, and schooling, of AI. Hereinafter follows an introduction to the application of AI in autonomous vehicles, to give an understanding of the inner workings of AI in autonomous vehicles.

The following section will give an overview of the, by the European Parliament proposed solutions for a general civil liability regime for AI, touching upon civil liability, attributing a legal personality to AI, the fundamentals of a crime and their relation to AI, as well as attributing criminal liability on AI.

This is followed by a review of the Swedish legislative proposal, and a comparative discussion on the Swedish and European stances on liability and AI, especially in autonomous vehicles. The thesis concludes in a conclusionary section where the research questions are answered and author opinions presented.

2. Introduction to Artificial Intelligence and its application to Self-Driving Vehicles

To further the understanding of issues discussed in later chapters, this section gives a brief introduction to AI, presenting an overview of the categorization and schooling of modern AI, as well as AI in autonomous vehicles.

2.1 Defining and Categorizing Modern Artificial Intelligence

John McCarthy, in answering a layman's questions about AI defines AI as;

> *"[...] the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable."*[7]

And intelligence as;

> *" [...] the computational part of the ability to achieve goals in the world."*[8]

Stuart Russel and Peter Norvig briefly describe AI as the science of making machines intelligent, giving them the ability to perform an array of tasks that otherwise would require human intelligence, exemplifying e.g. driving a car and trading stocks.[9] McCarthy's description of AI is related to its comparability to human intelligence, the ability to think and act like humans. This, however, is not the sole definition of intelligence that has been brought forward in the discussion of AI. There is also the idea of an 'ideal' AI, whose thinking and actions would be based entirely on rationality, as well as many ways to categorize AI in order to more clearly understand what type of AI is being dealt with in any given situation.

[7] John McCarthy, 'What is Artificial Intelligence?', Stanford University (24 November 2004). <https://borghese.di.unimi.it/Teaching/AdvancedIntelligentSystems/Old/IntelligentSystems_2008_2009/Old/IntelligentSystems_2005_2006/Documents/Symbolic/04_McCarthy_whatisai.pdf> Accessed 8 March 2022.

[8] *Ibid*.

[9] Stuart Russell, Peter Norvig. *Artificial Intelligence - A Modern Approach (4th Edition)* (Pearson 2020) 1.

2.1.1 Strong and Weak Artificial Intelligence

Strong AI, artificial general intelligence, or artificial super intelligence is a type of AI that only exists in theory. This type of AI aims to possess the same level, or a higher level, of intelligence than humans, being self aware, having an ability to solve problems, learn from them and make plans for the future.[10] Once the intelligence surpasses that of a human it would be considered super intelligent. Strong AI would also be capable of passing an extended Turing test[11], thereby fooling humans into believing that they are speaking to another human being.

There are those that believe that this type of intelligence can never be achieved in a machine, with a prominent critic being John Searle. In Searle's '*The Chinese Room Argument'*, where he brings forth the argument that if a non-chinese speaker is able to respond to a sequence of Chinese symbols correctly through inputting them into a computer program and then passing on the output, he still does not speak chinese, Searle boils the argument down completely to;

> *"Computation is defined purely formally or syntactically, whereas minds have actual mental or semantic contents, and we cannot get from syntactical to the semantic just by having the syntactical operations and nothing else…A system, me, for example, would not acquire an understanding of Chinese just by going through the steps of a computer program that simulated the behavior of a Chinese speaker."*[12]

While there are parts of the computer science society that have high hopes of achieving strong AI, or even super intelligence, the concepts remain entirely theoretical. In the meantime examples of artificial superintelligence can instead be collected from Science fiction, with prominent examples being HAL from 2001: A

[10] IBM Cloud Education, 'Strong AI', IBM (31 August 2020)
<https://www.ibm.com/cloud/learn/strong-ai>
Accessed 8 March 2022.

[11] Jack Copeland et. al, 'Alan Turing and the beginning of AI', Britannica (20 July 1998)
<https://www.britannica.com/technology/artificial-intelligence/Alan-Turing-and-the-beginning-of-AI>
Accessed 5 March 2022.

[12] John Searle, 'The Chinese Room Argument', Stanford Encyclopedia of Philosophy (2020)
<https://plato.stanford.edu/entries/chinese-room/>
Accessed 8 March 2022.

Space Odyssey[13], or more recently Just A Rather Very Intelligent System, J.A.R.V.I.S of Marvel's Iron Man, whose filmatization has been a large success in recent times.

Weak AI, on the other hand, surrounds us all in our everyday life. This type of AI is what powers a large array of applications that we use in everyday life. The name "weak" AI may be misleading, as it is not a reference to how powerful the AI is, but rather to the variance of tasks it can perform. As such, it is oftentimes called narrow AI, rather than weak.[14]

Rather than taking a general approach, as the theoretical strong AI would do, narrow, or weak, AI instead focuses on performing one task very well, making many applications of the technology rather robust. This type of AI powers applications such as e.g. virtual assistants, like Google Assistant, Apple Siri and IBM Watson, as well as chess-bots, customer service bots and is often used for medical purposes in e.g. analytics and diagnostics. Furthermore this is the type of AI that powers autonomous vehicles and driver's assistance systems.[15]

2.1.2 Human or Rational? Thought and Action

As mentioned previously there is a distinction between AI that thinks and or acts human, and AI that thinks and or acts out of rationality. Authors Stuart Russell and Peter Norvig bring up this distinction, and the confusion that sometimes arises between AI, and machine learning.[16]

The human approach means that the intelligence of an AI system is assessed on the basis of its ability to think and formulate itself in a human-like way. This was assessed through a test called the Turing Test, which tests capabilities linked to human behavior. The original version of the test did not consider physical touch or interaction to be necessary in assessing or displaying intelligence; but this has been suggested as an addition to the test, making for a 'total' Turing Test. Such a test would further need the system to possess computer vision, and robotics. These six

[13] IBM Cloud Education, (n 10).
[14] IBM Cloud Education (n 10).
[15] *Ibid*.
[16] Russell, S and Norvig P, 2020 (n 9) 1.

abilities are essentially what encompasses AI today, i.e.; natural language processing, knowledge representation, automated reasoning, machine learning, computer vision and robotics.[17]

Rational thought and action, on the other hand, is based around AI acting in accordance with what would yield the best result, and when there is uncertainty around what result will be achieved, acting in accordance with what should yield the best result. Rational thoughts are based on logic, a concept derived in ancient Greece, and a way of arguing that always gives a correct result, given correct conditions. For this to work at all times, the world is required to be certain, it must always behave in a manner that is to be expected. This is not the case, and in such cases an AI-system would instead rely on probability to assess what is correct. This, however, only constitutes thought - intelligent behavior requires both reasoning and action.[18] Acting rationally would mean action following a rational thought process, which requires the agent to perceive and understand its environment, have the ability to not only adapt to change, but to act in a way as to maximize the benefits of its actions in a changing environment.[19]

For a behavior to be considered intelligent, from the perspective of human rationality, however, the agent would also need to have an understanding of human values, as to discern what separates a good outcome from a bad one. This approach is beneficial as taking the right action is entirely based on probability, numerical values, and the right action is defined by what goal has been fed into the system. This is perfect rationality, something that is almost impossible to achieve in the real world. As such agents would likely act from limited rationality, taking action when there might not be enough time to compute all possibilities.[20] This is comparable to human reflexes.

The artificial intelligence controlling an autonomous vehicle must operate under a limited rationality, trying to make the best decision possible from a statistical

[17] *Ibid* 1-3.

[18] Russell, S and Norvig, P, (n 9) 5-6; IOP Publishing, Experts debate the possible paths to human-like AI, Physics World <https://physicsworld.com/a/experts-debate-the-possible-paths-to-human-like-ai/> Accessed 10th of March.

[19] Russell, S and Norvig, P (n 9) 6.

[20] *Ibid 6-7.*

viewpoint - even when not possessing all the data.[21] Algorithms of the AI systems in autonomous cars need to be thoroughly trained to perceive their environment, i.e. detecting, identifying and following objects in traffic, to uphold traffic safety.

2.2 Artificial Intelligence Learning

There are a multitude of different ways to school AI. In order to further the understanding of certain liability issues discussed in later sections it is beneficial to have a basic understanding of how AI, and in extent, autonomous vehicles, process and learn from information.

2.2.1 Machine Learning

The main way of teaching AI is through machine learning. Machine learning, simply put, is the science of making machines interpret, understand, and learn from data in the same way that humans do, more technically put it is a way to teach AI through the use of mathematical data models, without being instructed directly.

Machine learning is a four step process. The first step is to collect and prepare data. The second step is to train the model using this data. The third step is to verify the model precision, and the final step is to interpret the results.[22] There are three main categories of machine learning; supervised-, unsupervised and reinforced machine learning.

Supervised machine learning is done through the use of labeled data, where the data itself becomes the teacher of the machine, making adjustments until the model works as intended.

Unsupervised learning uses machine learning algorithms to discover hidden patterns in larger datasets and data groupings that are completely unlabeled, without any need for human intervention. This type of AI is good for e.g. segmentation work and

[21] *Ibid 8*.

[22] Michael Tamir, 'What Is Machine Learning (ML)?', Berkley School of Information (26 June 2020) <https://ischoolonline.berkeley.edu/blog/what-is-machine-learning/>
Accessed 10 March 2022.

pattern- or image recognition. Furthermore there is semi-supervised learning, which falls in as a medium of unsupervised and supervised learning.[23]

The last category is reinforcement machine learning, a trial and error concept where the machine learns by doing and is rewarded when doing the right thing, or punished when doing the wrong thing. Successful outcomes are then reinforced to produce a pattern for the machine to follow when facing other problems.[24]

2.2.2 Deep Learning and Neural Networks

Deep learning is a subcategory of machine learning in which the machine is fed data to learn from, without being introduced to any human rules or algorithms. The datasets and processing power required for this are enormous, and the higher the amounts of data fed to the machine the more the predictive model will improve.[25]

Neural networks are built to mimic the structure of a human brain, it consists of layers of nodes, with one layer handling input of information, one or multiple hidden layers that handle the main processing of information, and one layer that outputs the result from the former layer. Each node in the network is supplied with its own weights and thresholds for what information it will pass on through to the next node. Deep, in deep learning, refers to the depth, or multitude, of the layers in a neural network.[26] The AI-systems in autonomous vehicles are powered by massive datasets collected through image recognitioning systems, processed through systems for deep learning in neural networks.[27]

The neural network in an autonomous vehicle is used to identify patterns in the images, to be able to let the AI-system powering the vehicles recognize other

[23] IBM Cloud Education, 'What is machine learning?', IBM (15 July 2020) <https://www.ibm.com/cloud/learn/machine-learning#toc-machine-le-K7VszOk6> Accessed 10 March 2022.

[24] Michael Tamir (n 22).

[25] *Ibid.*

[26] *Ibid*.

[27] Ben Lutkevich, Self-driving car (autonomous car or driverless car), TachTarget (October 2019) <https://www.techtarget.com/searchenterpriseai/definition/driverless-car> Accessed 15 March 2022.

vehicles, traffic lights, signs, curbs, trees, etc. Data processing conducted in the manner described previously is called data annotation. Data annotation is a type of supervised machine learning, a human based system of labeling images, videos and text in a way for a computer to grasp and to then give context to these labels to assist AI in making its decisions in any given situation.[28]

There are many different types of data annotations, with some of the main ones being semantic annotation, image annotation, video annotation and text categorization. Semantic annotation is a process that helps machine learning categorize new concepts in text, through labeling different concepts in a text-based dataset for the machine to learn from. Image annotation is the process in which the machine is taught to identify one object from another in an image; e.g. a car from the road, etc. Video annotation is a similar process, which analyzes video content on a frame by frame basis. Text categorization is the process of categorizing certain sentences or paragraphs within a text on a given system. This can be helpful in training autonomous vehicles in understanding traffic regulations and traffic information.[29]

Deep learning neural networks lets the car teach itself rather than having a human manually put in rules, such as to stop when seeing red - in reference to a stop sign - thus allowing for a more efficient processing of the data collected by sensors and cameras on the vehicle, each element, or task of driving would require its own deep learning neural network for the car to function safely while autonomous driving is conducted. These types of deep learning algorithms have been the driving factor behind a substantial decrease in pedestrian misidentification at Google's autonomous vehicles section Waymo.[30]

[28] Melanie Johnson, Powering Self-Driving Cars with Data Annotation (December 15 2021) <https://tdan.com/powering-self-driving-cars-with-data-annotation/28890>
Accessed 15 March 2022.

[29] *Ibid.*

[30] IHS Markit, Artificial intelligence driving autonomous vehicle development (30 January 2020) <https://ihsmarkit.com/research-analysis/artificial-intelligence-driving-autonomous-vehicle-development.html>
Accessed 15 March 2022.

The application of deep learning systems further means that, as the vehicle is being driven around, the dataset on which decisions are based will grow and change, through the process of self learning, leading to more advanced ability to make complex and nuanced decisions in traffic.[31] This includes systems for detecting potholes as well as systems for localization, i.e. systems that can determine precisely where the vehicle is positioned in relation to other vehicles and otherwise its positioning in traffic.[32]

2.3 The Society of Automotive Engineer Classification System

AI systems in autonomous vehicles operate at varying levels of automation. The Society of Automotive Engineers, SAE, has developed a six-tier, level 0 through 5, classification system for the systems. Level 0 means that there is no driving automation whatsoever, but may still include systems such as automatic emergency braking or blind spot warning systems.

Levels 1 through 3 require a human driver to drive the car, and are meant only to assist in this task. Level 1 implies driving assistance, such as lane-centering or adaptive cruise control. Level 2 are systems that provide both acceleration, braking and steering - *inter alia* a combination-system for both adaptive cruise control and lane centering. In levels 3 through 5 the car will generally not need human assistance in driving, though level 3 systems may need assistance at times. Levels 3 and 4 cover systems that are capable of driving a vehicle under limited conditions and only when certain requirements are met; these systems include traffic-jam chauffeur systems, and automatic parallel parking systems in tier 3, while driverless taxis that are confined to a certain area fall under level 4. Level 5 covers all vehicles that are able to operate without human interference at any location and conditions.[33] The

[31] *Ibid*.

[32] *ibid*.

[33] The Society of Automotive Engineers, SAE J3016

same system of classification is used by the NHTSA[34], as well as the Swedish Government.[35]

2.4 Safety and Autonomous Vehicles

In a 2017 joint American Department of Transportation and NHTSA study of fatal traffic accidents it was found that, where more than 37.000 people died in traffic, 94% of the deaths were due to human error and sub-par decisions, such as driving under the influence or distracted driving.[36] The NHTSA further suggests that safety will be one of the largest benefits of autonomous traffic, as autonomous driving systems will remove the human element from driving.[37]

While safety may be projected to be one of the large benefits of autonomous vehicles, there are concerns raised in relation to the subject. The notion of fully autonomous cars may cause over-reliance on the in-vehicle systems, as it did when a Tesla SUV crashed into a highway lane divider, where the driver was not in control of the car as his hands were not on the wheel, despite being instructed to assume control both audibly and visually. [38]

The sensors on autonomous vehicles may also misread a situation, misidentify a pedestrian or other obstacle, as was the case when, during an Uber test drive with an autonomous vehicle, with a safety driver inside, failed to identify a woman with a bicycle, crashing into her with a fatal outcome.[39] Another system for autonomous driving misidentified the side of a large truck as the sky, driving full speed into, and under the truck, killing the driver.[40] Sensors have also been tricked into speeding by the placement of a small piece of tape on a sign, manipulating the systems into interpreting the speed to be much higher than it actually was.[41]

[34] NHTSA (n 2).

[35] See e.g. Sveriges Riksdag, SOU 2018:16 243.

[36] Lutkevich, 2019 (n 27).

[37] NHTSA (n 4).

[38] Lutkevich, 2019 (n 27).

[39] See e.g. Timothy B. Lee, 2020 (n 3).

[40] Lutkevich, 2019 (n 27).

[41] Björklund, 2019 (n 5).

2.4 Summarizing Discussion on Artificial Intelligence and Autonomous Vehicles

It is safe to say that there are many challenges when it comes to safety and autonomous vehicles, there is a need for the system to act instantaneously to objects in traffic, as well as technically complex issues such as ensuring safe operations in tunnels, where a global positioning system may not function properly, as well as issues of priorities in traffic, such as when and how to let emergency vehicles pass a autonomous vehicle in traffic.

While a rational AI propelling an autonomous vehicle may act on the most probable way in which to reach the desired outcome, and while the AI propelling autonomous vehicles will partake in a constant learning process, it is not guaranteed to always make a correct decision, just like a human being. Aside from mistakes. The autonomous vehicle may also completely misidentify a part of its surroundings, leading it to act erratically, or downright dangerously. Aside from internal factors of the autonomous vehicles themselves, there is the possibility for external factors such as an icy, or otherwise slippery, road, or even cybersecurity threats, to influence the autonomous vehicle in a way so that an accident arises.These safety concerns bring with them the issue of liability, the question of who is to be held accountable in a case of misbehavior by an autonomous vehicle.

The vehicles are already able to navigate around a city in busy streets completely void of human control, acting on their own volition and learning as they go. Who shall be held accountable when it’s an inherent flaw, when there is external influence from an unknown source - or in cases where the vehicle is completely empty? This is the main concern of the thesis, and what will be investigated in the upcoming sections.

3. European Union Proposals on AI Liability Solutions and Self-Driving Vehicles

This section will present key contents of three proposals at an EU-level for liability and AI as well as the applications on self-driving vehicles as this relates directly to the purpose of the thesis. The first of the documents was a report with recommendations on a civil law for robotics of 2017; the key takeaway of which is the proposal for an establishment of an electronic legal personhood - as will be discussed in section 3.4. The Parliament further released a proposal for liability for operation of AI-systems in 2020, to which they attached a proposed civil liability regime, which mainly focuses on control based liability at different stages of the operation of AI-system, as discussed in section 3.2.1. Additionally the Parliament made a resolution on autonomous driving in 2019, and it is of interest to see how this resolution relates to the later legislative proposals, as well as if and how the principles discussed in the resolution are incorporated in the proposal. As such these proposals and the main solutions proposed will be discussed and illustrated throughout this chapter. The conclusions drawn will later be used to fuel the comparative analysis of the more concrete Swedish proposal as discussed in section 4.

The Parliament proposes no solutions for the attribution of criminal liability in relation to AI, something that could possibly become crucial in the context of autonomous vehicles, due to the criminal nature of certain behaviors in traffic of which an autonomous vehicle would be perfectly capable. It is, however, identified that the aforementioned proposal for the attribution of an electronic legal personhood could possibly allow for AI-agents to be indicted with criminal liability in the same manner in which other legal persons are. The possibility for criminal liability to be attributed to AI-agents and the idea of a fundamental capability of AI-agents to commit crime is therefore discussed, in the interest of highlighting a possible solution for the attribution of criminal liability in relation to AI, in section 3.5.

3.1 General Considerations

The European Parliament considers the challenges posed by a broad introduction of AI into our society as one of the most significant questions in politics today. The introduction of these systems can, however, bring many benefits. In order to cease these benefits it is important that the regulatory environment remains unified and non-fragmented, and thus there is a need for a broad spectrum, principle based, cross border, regulatory framework to ensure legal clarity, equal standards and efficient protection. With this said there is still a need for sector specific regulations in e.g. the transport sector.[42]

The Parliament further underlines that the digital single market must be fully harmonized, due to the cross-border nature of data flows and dynamics in the digital environment. This, the Parliament believes, is the only way to remain digitally sovereign, and to boost innovation in the digital sphere. It's also noted that the race to reach new levels of AI is already underway, and that it is an international race. Protecting users from damages through liability frameworks encourages the protection to become an international standard, with liability being one of the main considerations of a new regulation.[43] The European Parliament also recognizes the potential implications of intelligent and autonomous machines that deploy self-learning and have the capacity to adapt to situations and make various decisions completely independent of human intervention.[44]

On the behalf of the rapid innovation and evolution of technological aspects in the field of robotics and AI and the growing ability of AI agents to learn and make independent and semi-independent decisions, the European Parliament recognizes the importance of the questions of liability arising from any harmful action taken by such an agent. The Parliament further questions the applicability of current rules on liability, and whether new ones need be written to deal with the considerations that

[42] European Parliament, 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) (20 October 2020) 1-2.

[43] *Ibid* 3-5.

[44] European Parliament, Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL) (27 January 2017) 4.

are brought forth by the use of AI, and ultimately whether robots can fall into any current legal categories or whether a new category is needed.[45]

The European Parliament additionally discusses the fact that under current European liability regulations there is no manner in which an AI agent can be held responsible for its actions, and the current legal framework can only administer liability when the cause of the damage can be traced back to any single person, and where the person in question could reasonably foresee the damage, as well as have the possibility to stop it. In a scenario where the agent is able to make independent decisions the current legal framework is not enough for legal liability to arise, as no direct link can be found to a person. As such there is a discussion on possibly holding users, owners, operators or manufacturers strictly liable for any damages.[46]

Furthermore the Parliament recognized the impact autonomous transport will have on the daily life of citizens of the European Union, the detrimental nature of autonomous traffic on the transport and mobility sector as a whole, and the increased needs of the transport and freight sectors. [47] It is further pointed out that the need for regulation is urgent, with fully autonomous vehicles expected to come to market during the next two decades, with roll-out beginning already in 2020.[48] It is pointed out that a large majority of all traffic accidents are due to human error, something that is largely eliminated in the use of autonomous traffic. The increase in road safety has declined in speed in recent years, while AI powered driving assistance is already proving to be a tool in increasing safety.[49] The Parliament especially stresses that a clear regime with regards to liability needs to be in place in relation to autonomous vehicles.[50]

[45] *Ibid* 6-7.
[46] *Ibid* 7.
[47] European Parliament, Autonomous driving in European transport; European Parliament resolution of 15 January 2019 on autonomous driving in European transport (2018/2089(INI) (15 January 2019) A, B, F, G.
[48] *Ibid* J, M, R.
[49] *Ibid* D-I.
[50] *Ibid* 14-19.

The Parliament further denotes that current EU-regulations on product liability and automotive insurance are not equipped to handle the issues posed in relation to autonomous traffic. It is noted that there is a need to clarify who bears the damage in the event of an accident involving a vehicle operating in full automotion. In cases where the vehicle can operate either in full automation, or under driver control, systems must be in place to show who the responsible party is. Furthermore the Parliament discusses whether any of the technical malfunctions that have historically caused crashes, without any other links to operator-negligence, can justify manufacturer based liability. It is also discussed whether obliging the owner and driver with certain instructions can be a reasonable compensation for this shift in liability.[51]

In terms of autonomous vehicles specifically the European Parliament suggests that a regulation covering all modes of transport be regulated. The Parliament further recognizes that the autonomous traffic sector is one of the sectors in most dire need of a functioning cross-border regulation that ensures that autonomous vehicles function, so that the benefits of autonomous traffic can be collected. It further underlines that fragmentary regulation on the field would stifle implementation of autonomous transport.[52] The European Parliament also recognizes the impact of moving from manually controlled vehicles to autonomous vehicles in fields like, *inter alia*, civil liability and insurance, and road safety.[53]

The Parliament believes that a complete overhaul of the current liability regimes is not necessary, but the evolving and changing nature of AI systems, self-learning and potentially autonomous systems makes it necessary to periodically adjust liability regimes, both at Union levels and at national level, in order to accomodate this changing nature and ensure that someone who suffers damage does not go without compensation. It is further noted that the way AI operates may make it impossible to find a person responsible through the construction, deployment, interference or use of the artificial intelligent agent, but that this issue can be circumvented through the direct assignment of liability in a liability regime.[54]

[51] *Ibid* 21.

[52] European Parliament (n 44) 12.

[53] *Ibid* 12.

[54] *Ibid* 7.

It is instead suggested that current product liability laws be modified to include persons in different stages of the AI sphere, from the producer, to backend operators, front end operators, software engineers etc. This would then let the regulation handle questions of damage and liability following faulty AI. Furthermore the Parliament believes that the protection offered by existing tort law in Member States already offer sufficient protection in terms of damages suffered due to third-party interference with AI, such as hacking. It is however noted that it may be hard to find a person on which to pin the liability, and as such the laws need to be complemented. On the basis of this the Parliament shifts the focus to the operator of the AI, as he ultimately holds the control over any risk associated with its use.[55]

The recommendation was motivated by the important role of liability in ensuring that a person or persons who suffer harm or damage are entitled to claim and be compensated from a liable party. The Parliament further notes that a new framework must give confidence in the safety, reliability and consistency of products and services to create a balance between protecting the citizens and still leaving room for innovation and product development. The ultimate goal is described to be the creation of legal certainty for all interested parties.[56]

It is also suggested that there is room for Member States to alter the rules for certain actors in the question of liability, as well as stricten the rules for certain activities, making it possible to hold parties liable despite no fault, in so-called strict liability situations. Strict liability is pointed out to be common in many national tort-laws, such as in relation to dangerous activities, like the propulsion of a vehicle, or activities with risk-filled elements outside our control, such as handling animals.[57]

The goal of a regime on civil liability for AI is to explicitly allocate liability, the issue should still be subject to public scrutiny and debate, leaving room for all interested parties to have their say in order to avoid misunderstandings. It is argued that AI, as well as the inter-connectivity between different AI and non-intelligent systems, as it stands today, poses a significant challenge for existing systems of liability, especially

[55] European Parliament (n 42) 6-10.
[56] European Parliament (n 42)
[57] *Ibid* C.

in terms of identifying a responsible party. Concerns stem also from cybersecurity vulnerabilities and deep learning techniques.[58]

The Parliament speaks on the need for a functioning compensation procedure, ensuring the same level of compensation in cases where AI is involved as it would if there was no AI involved, in order to address the aforementioned challenges, and to eliminate any unwillingness among the users to accept the new technology. It is however pointed out that similarly to cases where AI is not involved, there is a need for the consumer to ensure that he is correctly insured and that there is a defined route to redress.[59]

3.2 Civil Liability and the Proposed Solutions for the Attribution of Civil Liability and Artificial Intelligence

Civil liability can come in many shapes. It is a legal obligation that obliges one party to take responsibility for damages as well as to follow any other court-enforcements in a lawsuit brought against the party. One example is that of a traffic accident, where one party usually becomes liable to pay the damages of the other party. These liabilities oftentimes arise from contractual- or tort law, and bear with them no threat of a prison sentence.[60]

With the recognition of the importance of clarifying liability in relation to AI the European Parliament suggests that it is a subject which needs to be addressed at a Union level, to uphold fundamental values such as legal certainty, transparency and clarity in the application of liability regimes in relation to AI.[61] Further the Parliament suggests that the proposal, no matter what means of compensation, the civil liability remains untethered by the fact that the damages are caused by a non-human agent.[62]

[58] *Ibid D-I*

[59] *Ibid* I-L.

[60] Legal Information Institute, Civil Liability, Cornell Law School <https://www.law.cornell.edu/wex/civil_liability>
Accessed May 5 2022.

[61] European Parliament (n 44)16.

[62] *Ibid 16-17*.

3.2.1 A Control based Regime of Alternative Strict and At-Fault Operator Liability

The Parliament is of the opinion that operational liability should cover all modes of operation, be they physical or remote, remarking that operation in public spaces not only exposes the operator to risk, but many other people around. This, however, may be hard to prove as they have any contractual liability claims to aim towards the operator, and as such they would need to prove fault, which may prove difficult, as such any such claims may fail.[63]

The term operator is suggested to concern both front- and backend operators, given that the latter is not already covered by product liability. Furthermore the Parliament suggest the frontend operator to be the natural or legal person who exercises control over a risk connected to the AI, while the backend operator is a person who, continuously defines the features of the technology, providing it with different services etc. and thereby exercises a degree of control over the functionality, operation and risks connected to these. Control is to be defined as any interference which impacts the operations, output or result of the AI system, or changes processes within the system.[64] The Parliament further notes that a system can have multiple operators, and that one operator can operate many systems. In the case of multiple operators the degree of liability should be determined in proportion to their respective degree of control.[65]

The European Parliament attaches a detailed proposal for regulation, of which the subject matter, stated in the first article, is the rules for the civil liability claims of natural and legal persons against AI operators.[66] The second and third articles deal with the scope of application and definitions of key terms, *inter alia* AI-system, operator, front- and backend operators and high risk.[67] The fourth article covers the strict liability that is suggested to be connected to the operation of high-risk AI systems. The operator shall be held strictly liable for any harm or damage caused by any AI operation. All high-risk systems, autonomous vehicles included, are proposed

[63] European Parliament (n 42) 11.
[64] *Ibid* 12.
[65] *Ibid* (n 42) 13.
[66] European Parliament, Proposal For a Regulation of the European Parliament and of The Council on Liability for the Operation of Artificial Intelligence Systems (October 20 2020) 1(1)
[67] *Ibid* 1(2)-1(3)

to be listed in an annex to the regulation, and the Commission is proposed to be empowered with the ability to adopt delegated acts to amend the exhaustive list. Operators of high-risk systems shall not be able to escape liability through arguing that due-diligence was observed, or that the damage was caused by autonomous activities, but shall not be held accountable in cases of force majeure.

There is also a responsibility imposed on frontend operators to ensure that the system is covered by liability insurance, while backend operators must ensure that the same system is covered by product or business liability insurances. The fourth article also establishes that the regulation, if adopted, would reign supreme over any national liability regimes.[68]

Articles five and six cover the amount and extent of compensation, setting a cap of EUR two million and EUR one million respectively, depending on the type of damage sustained. It also establishes that the cap is applicable to cases with multiple persons claiming damages, and that the total in such a case must not exceed the cap.[69]

The proposal also includes a limitation period, which states that civil liability claims are subject to periods of ten and thirty years respectively, depending on the surrounding circumstances. It is also established that national laws on the same topic shall take priority over this.[70] Chapter four of the legislative proposal deals with the adjustment of damages due to contributory negligence and joint and several liability. Furthermore it contains rules regarding the operators' possibilities for recourse for compensation.[71] The final chapter covers the administrative aspects of the proposed regulation, such as exercise of delegation, review and entry into force.[72]

The Parliament recognizes that different types of systems pose different amounts of risk to the public, and as such AI systems should be divided into high risk and non-high risk systems, where only high-risk systems are connected to strict liability. It is emphasized that a risk-based approach should be furnished with a clear list of

[68] *Ibid* 2(4).
[69] *Ibid* 2(5)-2(6).
[70] *Ibid* 2(7).
[71] *Ibid* 4(10)-4(12).
[72] *Ibid* 5(13)-5(15).

criterias and definitions in the name of legal certainty. Any AI systems that fall outside this list are to remain within fault-based liability regime.[73] It is also suggested that systems that prove problematic, insofar as causing multiple incidents, without yet being assessed and classified as high-risk already, should be connected to the same type of strict liability by means of exception.[74]

Due to the dynamic evolution in the field of AI the Parliament stresses that new introductions in the field need be analyzed quickly with regards to their risks, and that the process for this be as simple as can be. Potential high risk systems should be assessed for product safety at the same time as the risk assessment, to avoid high-risk products being cleared for market without mandatory insurance.[75] The European Parliament points out that, in likeness to the strict liability systems already in place in Member States, the proposed regulation should also cover violations of rights to life, health, physical integrity and property, specifying amounts and extent of compensation.[76]

3.2.2 A Limited Product, Owner, and User Liability

The European Parliament also suggests that one possible solution for the coverage of damages in relation to civil liability claims is an obligatory insurance system, like what encompasses motor vehicles, and that this system be supplemented by a fund for situations where there is no insurance coverage. This fund, it is suggested, could possibly be connected with limited liability for producers, owners and users if they contribute to the fund or jointly take out insurance to guarantee compensation for any damages caused by an autonomous intelligence agent.[77]

[73] European Parliament (n 42) 20.
[74] *Ibid* 21.
[75] *Ibid* 17.
[76] European Parliament (n 42)19.
[77] European Parliament (n 44) 17-18.

3.2.2 A No-Fault Liability Regime, Insurance, and Redress

The Parliament views liability coverage as to be one of the keys to a successful introduction of new technology. It also views the coverage as necessary in ensuring the public's trust in new technology, despite potential risks of harm. At the same time it notes that the regulation focuses on the needs of furthering the technology, balancing this against robust safeguards. As such the Parliament suggests a mandatory insurance system for any and all systems falling under an annex to the proposed regulation, under the category of high risk systems. This system would operate similarly to that in place for traditional vehicles. It is also suggested that a no-fault insurance framework be set up to cover damages resulting from autonomous vehicles, and that any such damages should not be limited on the basis of autonomous operation, to ensure adequate protection of victims.[78] The Parliament reckons, however, that a Union level mechanism for compensation is not the way to go, but that work should be done closely between the Commission and the insurance sector to analyze potential risk and develop insurance solutions.[79]

[78] European Parliament (n 48) 33-34, 42-43.
[79] European Parliament (n 42) 23-25.

3.4 Giving Artificial Intelligence with an Electronic Legal Personhood as a Solution for the Attribution of Civil Liability

The European Parliament also makes a suggestion that there be a specific legal status, an electronic personhood, created for capable AI-entities and robots. This personhood, or legal persona, is suggested to be connected with an obligation to compensate for any damage caused, although it is left open who this obligation should apply to.[80] This suggestion was met with massive criticism at the time of its conception. In an open letter more than 150 European experts on AI, robotics, ethics, law and medicine opposed the idea.

The experts argue that the creation of a specific legal status for robots or AI agents is not only based on incorrect grounds, but also deems it inappropriate from an ethical and legal perspective. Instead they argue that a legal framework needs to be in place as the interactions between humans and AI or robots become part of our daily lives. The framework needs to reinforce democracy and fundamental values of the European Union, the experts argue. They emphasize that the framework would require exploration not only in terms of legal and economic aspects, but through ethical, societal and psychological aspects as well.[81] Furthermore the group points out that the basis for the creation of such a personality, that it would be impossible to prove damage liability, is incorrect in of itself. They argue that there are many troubles with the creation of a legal electronic personality for robots, both in terms of ethical, and legal aspects.[82] They assess that such a personality can not be derived from a legal entity model, as there is no person behind it, like there would be a company or other legal person, and similar is the situation for a trust-, fiducie- or treuhand situation, which also implies a person to be behind it.[83]

[80] European Parliament (n 47) 18.

[81] Various Authors, Open Letter to the European Commission - Artificial Intelligence and Robotics, Politco.eu (April 2018) <https://www.politico.eu/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf> Accessed 2 May 2022.

[82] *Ibid.*

[83] *Ibid.*

There are supporters of the system, however. Professors Vagelis Papakonstantinou and Paul de Hert argue that the refusal to provide AI systems with a legal personality is wrong, and that the Parliament should embrace change rather than shy away from it, in the proposals. They argue that, in fact, the liability is enhanced rather than reduced in giving AI a certain legal personality. This is due to the fact that, since AI will become part of most parts of society they will need to operate under cross-border agreements between multiple parts of the liability chain, developer, deployer and end user, and as such it will, Papakonstantinou and De Hert argue, be nigh impossible to establish the liability of any one person, and that it would instead be clearer for the end user if the AI entity be given its own personality.[84] They argue further that a human conscience is unneeded in the process of granting legal personhood, in response to reasoning around this by the European Parliament. They continue, stating that giving AI a legal personality similar to that of a legal person; as it is today granting the persons controlling the company liability, it would grant the persons controlling the AI liability.[85]

The Professors emphasize two advantages of such a solution. First is the flexibility, allowing for a case by case assessment of liability in a similar way as has been the case for legal persons, something they view as crucial for a field in evolution. Second is proximity; granting the personhood would leave the claimant with a local legal entity towards which claims can be directed.[86] Papakonstantinou and de Hert also recognize that this would not be a solution for all issues, and that a legal personality could be used to escape liability in e.g. situations involving autonomous vehicles.[87]

[84] Vagelis Papakonstantinou, Paul de Hert. Refusing to award legal personality to AI: Why the European Parliament got it wrong, European Law Blog (25 November 2020)
<https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/>
Accessed 5 May 2022.

[85] *Ibid.*

[86] *Ibid*.

[87] *Ibid*.

The European Parliament proposals only consider civil liability in relation to AI, and leave no guidance on the attribution of criminal liability to Artificial Intelligence or its operators. It is not possible to hold an object or product criminally liable for any actions. With the proposal of the attribution of an electronic legal personality to AI-agents, however, could bring forward the question of criminal liability, potentially offering the possibility to hold the AI-agent liable for a criminal act in the same way as one would other legal or physical persons.

Establishing this possibility, however, also begs the question of whether it is fundamentally possible for AI to commit crime, if there is any reason in holding an AI agent liable for a crime, and if the fact that the agent potentially could be held liable really means that it should.

3.5 Electronic Legal Personhood as a Solution for the Attribution of Criminal Liability to Artificial Intelligence

Gabriel Hallevy recalls a situation where a factory plant worker was deemed a threat to the mission of an AI entity operating a hydraulic arm in the same plant. The arm pushed the worker into a nearby production machine - killing him, to stop him from interfering with the mission. Hallevy ponders who is to be held accountable for such a premeditated, and lethal act.[88]

If AI-agents are given electronic legal personhood this question may have been given an answer by the European Parliament, enabling the criminal liability to be attributed to Artificial Intelligence qua a legal person.

In asserting criminal liability generally two criteria generally need to be fulfilled; the intent, or frame of mind - *mens rea* and the guilty act - *actus reus*, or a failure to act if a duty is imposed. In establishing criminal liability it is important to understand these concepts, what they entail and the possibility to apply these to an artificial intelligence agent.

[88] Gabriel Hallevy, The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control, Akron Intellectual Property Journal (Akron Law Journals, 2016), 171-72.

3.5.1 *Mens Rea* - A guilty state of mind

Mens rea entails the mental, or internal element of a crime, in extension meaning the intention, motive or planning of a crime. In traditional criminal judgements it is not the act in itself, but rather the intention, or culpability, that decides whether a crime has been committed or not. *Mens rea* generally also includes assumptions or wishes towards a certain outcome, as well as culpous behavior.[89]

Mens rea is a central concept to anglo-saxon penal theory.[90] The concept can, however, be found also in civil systems, *inter alia* in the Swedish penal code, Brottsbalken. Brottsbalken clearly states that a crime, except in specially regulated cases, shall only be considered a crime if an intent can be established. This also rings true in cases where the perpetrator of the act is under a self-inflicted changed state of mind, such as the influence of drugs or alcohol. Such a changed state of mind shall not prohibit the acts to be seen as a crime due to lack of intent.[91]

Swedish courts have established three main categories of intent through case law. premeditated intent, or direct intent, meaning the suspicion and wish to achieve a criminal end goal of an act, if the culprit has had the intent to achieve this goal, or as a means to achieve another end goal, as well as perceiving the effect as practically achievable. There is also intent through disregards; meaning that when a perpetrator suspects an outcome, yet disregards this in his actions. Furthermore there is insightful intent, meaning that there is a direct correlation between action and outcome, but the intent is to achieve something else, e.g. if someone were to place a bomb at a speakers podium with the intention to kill the speaker, that intention will extend to any bystanders as well.[92]

[89] Bertram F Malle, Sarah E. Nelson. "Judging mens rea: The tension between folk concepts and legal concepts of intentionality." Behavioral sciences & the law 21 May 2003, 563-580. <https://www.researchgate.net/publication/9085796_Judging_Mens_Rea_The_Tension_Between_Folk_Concepts_and_Legal_Concepts_of_Intentionality>
Accessed 23 March 2022.

[90] Albert Levitt. "Origin of the doctrine of mens rea." Illinois Law Review 17 (1922): 117. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/illlr17&div=14&id=&page=>
Accessed 23 March 2022.

[91] Sveriges Riksdag, Brottsbalk (1962:700) 1(2).

[92] Högsta Domstolen (Swedish Supreme Court), B 379-16; Högsta Domstolen (Swedish Supreme Court), NJA 2004 s. 176

The notion of *mens rea* is, furthermore, generally connected to that of transferred intent; where a person intends to harm one person but ends up harming another, say by missing a shot intended for the first person. In such a case the person has not intended to harm the person that was harmed, but the intent to harm remains with the act and actor, and is then transferred to the person who actually falls victim to the act.[93]

Mireille Hildebrandt argues that the imposition of *mens rea* on an AI agent would be similar to imposing it on an animal, due to the lack of possibility for an AI to formulate *mens rea*.[94] It is an argument made in a state of mind that views AI only as a machine, or tool, operating under the instructions of its masters. Hallevy argues instead that AI is fully capable of forming *mens rea*, be it through knowledge, intent or negligence.[95] He argues that AI systems generally are well equipped for knowledge, defined as the sensory reception of factual data and understanding of this - this data is then sent to be processed, a task at which AI often supersedes the human mind. He further argues that for specific intent to be established it is enough that the aim of an action is the outcome, which very well could be the case of an AI.[96]

This ties back to the factory robot that deemed it necessary to terminate a human worker it perceived to threaten the mission - the intent was to eliminate the person - and thus intent should be possible to establish. Hallevy goes on to argue that human feelings might not possibly be imitated by AI, but that these feelings are rarely necessary to establish *mens rea*. He further argues that, as it is possible to attribute the highest form of *mens rea*, specific intent, to an AI entity, it should follow that it is possible for the entity to fulfill all lesser *mens rea*, e.g. negligence, recklessness etc.[97]

[93] Hall, D.E. Criminal Law and Procedure, (Cengage Learning 2015) 64.

[94] Mireille Hildebrandt, Ambient Intelligence, Criminal Liability and Democracy, 2 Crim L. & Philos. 163, 164-170 (2008).

[95] Hallevy, G. Dangerous Robots - Artificial Intelligence vs. Human Intelligence (21 February 2018) 24-25
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3121905>
Accessed 5 May 2022

[96] *Ibid* 26.

[97] *Ibid* 27.

John Searle, on the other hand, argues that all an AI entity does respond mechanically either to the rules that have been put in, or in accordance with what it has learned through self-learning. It acts without comprehension of the consequences of its actions, and as such it could be argued that AI can not fully satisfy a *mens rea* requirement.[98]

3.5.2 Actus Reus - The Act

In addition to the internal element of *mens rea* one must consider the external, or objective element of *actus reus*, the guilty act; for what is a thought without action? Once again *actus reus* alone generally will not constitute a crime without the existence of *mens rea*. Generally the term only incorporates acts committed voluntarily. Voluntariness is an ambiguous concept. An early attempt to define the same was made by Wendell Holmes, stating that; a spasm is not an act. and that the contraction of the muscles must be made at will for there to be any liability associated with the action.[99] This would exclude involuntary actions, such as reflexive actions, actions committed while sleepwalking or actions committed in the defense of one's own life.

The *actus reus* can achieve criminal status through the act or itself, such as rape, speeding or robbery, or through a specific behaviour such as possession of illicit substances. Furthermore the *actus reus* can arise through failure to act, if there is a duty to do so, which is the case in the case of omissions.[100] Similarly to the element of *mens rea* the *actus reus* is central to the crime, especially in common law theory, it still, however, appears in many civil law penal- or criminal codes, such as the Brottsbalk of Sweden, as it is established that only an act can be punished[101], and only under the circumstance that it was committed with intent, unless otherwise prescribed.[102]

[98] John Searle (2020) (n 12).

[99] O. Wendell Holmes, The Common Law (1st edition) (Macmillan, 1882) 54.

[100] Legal Information Institute, Actus Reus, Cornell Law School
<https://www.law.cornell.edu/wex/actus_reus>
Accessed April 2 2022.

[101] Sveriges Riksdag (n 91) 1(1).

[102] *Ibid* 1(2).

The element of actus reus should be rather easily satisfied for any AI entity, self-driving cars included. An AI entity that, under its own control, voluntarily, performs an action, should be able to fulfill the criteria. Under the circumstance that the action is tied to a result for the question of liability the result obviously needs to be achieved through the action also of the AI agent.

3.5.3 Omissions - Failure to Act

Omission is a crime where the *actus reus*, or the guilty act, is the complete opposite; a failure to act. In the early common law system criminal laws there was no general duty to care for others than yourself. It was, however, decided that some failures to act may be so morally faulty that there was reason to charge the non-actors with criminal offense. Generally the circumstances under which a omission might have occured, and where there has been no risk to the accused non-actors health or well being there should have been action taken to prevent injury or death being inflicted on a victim or a select person in a larger group of potential at risk persons.[103]

Generally, in civil law systems, unlike many common law systems, there is no immediate duty to take action, even when you are not put at risk personally.[104] Witnessing a crime and not acting upon it, however, can still cause criminal liability to arise, in some situations, such as when witnessing a person being beaten to death and not calling police or otherwise assisting to the largest extent possible.[105] Generally for omissions to be criminal in civil law systems like Sweden there has to be a duty to act explicitly imposed by legal statute. The crimes can be committed consciously and with intent, or through negligence, without intent.[106]

Criminal omission in countries that require an explicit statute imposing a duty to act can generally be divided into two categories; true and false omissions. True omissions consist of failure to act where failure to act is explicitly forbidden by law

[103] Jonathan W. Cardi. Reconstructing Foreseeability, Boston College Law Review 46, 921–988 (2005) <.https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2311&context=bclr>
Accessed April 5 2022.
[104] Petter Asp, Magnus Ulväng and Nils Jareborg, Kriminalrättens Grunder (Lustus) 2013, 127
[105] Madeleine Leijonhufvud and Susanne Wennberg, Straffansvar (Norstedts juridik 2009) 39.
[106] Asp, Ulväng, Jareborg (n 104).

and the crime can only be committed through failure to act.[107] False omissions are crimes where there is no explicit prohibition on failure to act, but rather a duty to act imposed, and where refraining from such duty constitutes criminal omission.[108]

Similarly to an ordinary *actus reus* the question of omission should be easily satisfied by an AI agent; if the duty to act is somehow imposed on an AI entity and it fails to do so, the *actus reus* in the form of an omission, appears to be fulfilled.

3.5.4 Hallevy's models for the Attribution of Criminal Liability to Artificial Intelligence Agents

There appears to be a case to be made for AI being able to fulfill the foundational requisatory elements for a criminal act, if even with some reservation. The question remains regarding whether liability could, or should, be attributed to an AI agent - or any other person - for the actions of the AI agent.

Hallevy is a proponent of the attribution of criminal liability to AI agents, and argues, after having established that an AI agent is capable of fulfilling the requisites of most crimes, that there should be a possibility to attribute criminal liability in the same way it is possible to do for a physical or legal person.[109] He argues that, while it took a long time, corporations, who, like an AI agent are viewed to be capable of fulfilling both *mens rea* and *actus reus*, the prerequisites for criminal liability, are held liable for criminal actions. He deems it outrageous for society not to hold these corporations, or other legal entities, responsible, as they are fully incorporated into human life.[110] He goes on to question why a different set of rules should apply to AI, as the same principles are applicable to them. He further argues that there are criminal liability regimes in place and questions what more would be needed.[111] It would be necessary to establish a mode through which AI agents are viewed by the law. One such mode could be the establishment of an electronic legal personality, as

[107] See e.g. Sveriges Riksdag (n 91) 10:8.
[108] See e.g. Trafikförordning (SFS 1998:1276), 2(8).
[109] Hallevy, G. (2018) (n 95) 42.
[110] *Ibid* 43.
[111] *Ibid* 43-44.

previously suggested by the European Parliament. This suggestion has, however, seen fierce opposition - while there are also supporters of it.[112]

Hallevy instead suggests three different models of criminal liability. The first is the Perpetration-by-Another liability Model. This is a model of liability that views the AI entity as an innocent agent - according to the device that it is just a machine. In this model, Hallevy argues, the AI would take the role of a child; lacking in the mental element of the crime, that is instructed to commit an action equating a crime, making the instructor liable as the perpetrator-by-another, as it is him to which the *mens rea* can be attributed.[113] Hallevy then poses the issue of finding the perpetrator-by-another. He establishes two candidates, the programmer of the AI - giving the base instructions, or the user of the AI system, giving further instructions.[114] This model deems the AI entity a tool, no more or less liable than a crowbar used by a burglar.

Hallevy points out that one weak point of this regime is the fact that it is not suitable for AI that acts out of its own volition, due to accumulated experience and knowledge, where the AI entity makes an informed decision outside of the original programming or user control.[115]

A second model for criminal liability, as presented by Hallevy, is that of the Natural-Probable-Consequence Liability Model, which deals with offenses committed by AI that would be foreseeable, without the knowledge or intent of the programmer of the entity.[116] This would be cases of negligence, a form of *mens rea*, and could be situations like the aforementioned[117] case of the worker killed by a factory machine; where the programmer of the machine likely did not intend for the machine to slaughter a worker to protect its mission, but still programmed the machine to protect its mission, failing to consider the possibility.

[112] *See section 6.1.*
[113] Hallevy, G. (2018) (n 95) 10-12.
[114] *Ibid* 12.
[115] *Ibid* 14.
[116] *Ibid* 15.
[117] *See section 6.2.*

Due to a lack of intent in such a negligence case, while liability would fall on the programmer under the liability model, it would not be for murder or manslaughter, as there was no intent to kill or maim.[118] It would also incorporate cases where the AI is instructed to commit one crime, but instead happens to commit another, that is not in the original intent of the instructor, such as if the instruction was to rob people - not to kill people, but the AI entity still does this. This would be a case of transferred intent[119] and the programmer would be held accountable for all crimes committed.[120]

In the first situation mentioned in the relation to this liability model the AI agent remains innocent, as per the first model. In the secondary situation the AI does not remain innocent, as it has made its own decision to commit a separate crime, and as such should, according to Hallevy, be held equally liable.[121] The third model that Hallevy Suggest be applied is the Direct Liability Model.

The Direct Liability Model considers the AI entities the direct subjects of criminal liability. It disregards the user or programmer, focusing instead on the entity itself, basing criminal liability completely on the presence of *mens rea* and *actus reus*, as these are oftentimes the only elements truly required to impose criminal liability.[122]

[118] Hallevy, G. (2018) (n 95) 19.

[119] *See section 3.1.*

[120] Hallevy, G. (2018) (n 95) 19.

[121] *Ibid* 20-21.

[122] *Ibid* 21-22.

3.6 Summarizing Discussion with Regards to the European Parliament Proposals on Solutions for Liability

Civil liability of AI is a complicated issue, but one that the European Parliament has begun to untangle. It establishes that there is no necessity for a total overhaul of any other current liability regimes, but that some may need adjustments. The proposals are welcome, it is good to see resolutions being made at a European Union level, as they, while they remain legally un-binding and free from obligations for the Member States, set the tone for united and standardized regimes of liability for the increased application of AI overall in our everyday life. This is something that the Parliament also underlines in their general considerations, e.g. establishing that the digital single market must be fully harmonized.

The European Parliament proposals fail to provide for specific principles on liability in relation to autonomous cars, not going beyond stating that this is a subject which needs to be investigated further. Instead the Parliament proposes a more generally held liability regime, suggesting ways to allocate liability with regards to a multitude of different types of AI. The proposals do however suggest that autonomous vehicles fall into a high-risk category, when categorizing different types of AI. As such, in principle, the suggestions on what should apply in terms of civil liability and high-risk systems would also apply to autonomous vehicles, though there may later come proposals for more specific legislation on the topic.

It is interesting that there is no legislative proposal specifically relating to autonomous traffic made at an EU level as of yet, as the Parliament speaks of autonomous transport being one of the sectors in most dire need of regulation. The liability regime as proposed would still include autonomous vehicles, however, and a proposal for an autonomous vehicle-specific legislation may still be presented in the future to promote legal harmonization and dispel fragmentation between member states.

The regime for civil liability, as suggested in the legislative proposal, is clear, and based on the grade of control exercised. The clarity of these regulations was one of the fundamental aspects discussed by the European Parliament in their general considerations in relation to the proposals. The Parliament suggests attributing liability for the actions of an AI agent to any persons exercising a modicum of control over an AI agent. The liability is suggested to be strict liability in relation to all AI systems that are deemed to be high-risk, thus falling into an exhaustive list categorizing systems as high risk, encompassing e.g. autonomous vehicles. This list is suggested to be annexed to any adopted civil liability regime for artificial intelligence.

The strict liability is suggested to be inescapable, although with room for redress, even under circumstances of third party interference. It is also suggested that there be a mandatory system for insurance instated for all matters related to high-risk AI systems, to ensure that any liabilities for damages are covered. On the matter of non high-risk systems it is instead suggested that the civil liability be based on fault of the operator. All Parliament-suggested civil liability regimes in the proposals are connected to an insurance system, pointing to the fact that the European Parliament views the coverage of compensation for damages arising from civil liabilities in relation to AI-activities, such as autonomous driving, one of the top priorities in the liability regime.

On the topic of establishing a criminal liability there are no solutions proposed by the European Parliament directly. Hallevy presents a persuasive argument for the possibility of attributing criminal liability to an AI agent, with AI agents being perfectly capable of fulfilling the key elements of a criminal act. This would require some sort of legal personality to be established for AI agents, as an object can hardly be held liable for a crime. One of the solutions for civil liability proposed by the European Parliament would be the attribution of such a legal personality.

The European Parliament, however, recognizes solutions related to the attribution of an electronic legal personality as superfluous in the latter proposal. It becomes apparent that the proposed strict- and at-fault liability regime, backed by mandatory insurance and product liability, is capable of covering damages arising from AI-activities, such as autonomous driving, which is the main purpose of the European Parliament in establishing the liability regimes. There is no benefit of the attribution of criminal liability to AI in fulfilling this purpose. It is also recognized by experts that the attribution of an electronic legal personhood could potentially muddle legal certainty and allow escape from civil liability in various cases, which would be directly opposed to both the legislative proposal in itself, as well as the general considerations taken by the European Parliament in presenting the resolutions and proposals for the liability regimes.

4. Proposal on Regulating Autonomous Traffic in Sweden

Whereas the European Parliament proposals fail to provide for specific principles on liability in relation to autonomous cars, not going beyond stating that this is a subject which needs to be investigated further and including it under the general umbrella of high-risk systems, the Swedish government has taken initiative in the issue and launched an investigation into specific solutions for liability and the regulation of autonomous traffic. From the investigation stems a concrete legislative proposal where these issues of liability are dealt with.

The purpose of this thesis is to comparatively study alternative principles and models proposed by the European Parliament for the attribution of liability in relation to AI, and the more concrete and specific legislative proposal for the regulation of autonomous traffic made by the Swedish government. This section is intended to give an overview of the more concrete solution for the issue of liability and autonomous cars, drawing comparisons to the European Parliament proposals throughout the presentation, noting key differences, as well as similarities between the respective approaches to liability.

4.1 The Proposal for a New Regulation of Autonomous Vehicles in Sweden

4.1.1 Introduction

The Swedish investigation and following legislative proposal for a regulatory framework on autonomous vehicles in Sweden, Förslag till lag (2019:000) om automatiserad fordonstrafik, is brought forward by the recent fast paced increases in interest in these vehicles, and the need to adapt regulations that were born in a time where all driving took place manually and under full control of a human driver. In short the proposal is intended to simplify a gradual introduction of vehicles with increasingly advanced autonomous driving systems.[123]

[123] Sveriges Riksdag (n 35) 29-30.

The proposal is especially so intended to, in the short term, enable the use of highly automated driving, in vehicles classified as SAE levels 4 and 5[124], as well as enabling testing of highly automated goods transports. In the long term it is ascertained that there is a lot of work to be done, mainly on a governmental level in bringing these ideas to fruition.[125] Furthermore it is motivated by environmental-, sustainability-, and traffic safety based political goals.[126]

The investigation also brings up international efforts that are in the pipeline, as well as the historical importance of e.g the 1968 Vienna Convention on road Traffic, ratified by Sweden, on which all Swedish road traffic laws are based, and the challenged this ratification brings, in for example the Vienna Convention requiring a driver, in control, in every car on the road.[127]

The investigation, in addition to proposing a new law regarding the use of autonomous vehicles on public roads in Sweden, also proposes changes to a plethora of other laws related to traffic. It is, however, also established that many Swedish traffic laws and laws relating to the area are technology neutral and will apply the same no matter the level of automation of a vehicle bound by these, *inter alia* laws on civil liability and traffic insurance, where the current system is considered relevant still.[128] Changes to laws that are already in force are generally intended to be general, and to apply to all vehicles, and all classes of automation, while there are a handful of laws that need to take special consideration to autonomous vehicles, such as privacy laws etc. An intention to, from the Swedish side, work for adjustments in law related to autonomous vehicles on an international level, and to adjust the country's own law in accordance with such changes is also made clear.[129]

[124] *See section 2.4.2.*
[125] *Ibid 35-36.*
[126] *Ibid 37.*
[127] United Nations, Vienna Convention on Road Traffic [1968], Article 8.
[128] Sveriges Riksdag (n 35) 33-34.
[129] *ibid* 33-36.

4.1.2 Liabilities and Responsibilities of the Owner

The legislative proposal, if accepted, would further introduce ownership based liability. Under fully autonomous operation of autonomous vehicles the owner is to be held strictly liable in regards to the vehicle operating in accordance with relevant road safety rules and other traffic regulation, as he is the person deemed most likely to be able to see to the status of the vehicle AI. In other words the ownership based liability only extends to vehicular actions, rather than driver related issues. Operations contrary to traffic rules are proposed to be connected to sanction fees[130] directed towards the owner, in a similar way as penal fees would be given to a driver in a manually driven vehicle.[131]

The investigation also clarifies that, as many of these faults may be related to security faults in the system operating the vehicle. As such, while the owner may be held liable for damages caused, or crimes committed, during a fully autonomous trip, there will be a possibility for the owner to reclaim eventual fees through the Swedish product reliability laws.[132]

In the legislative proposal the owner is defined to be the person who, at the time of, or after an incident, was registered as owner of the vehicle with the Swedish vehicle registry[133], or a corresponding registry abroad.[134] If the vehicle is under transport by a retailer or importer with a special sales license he shall instead be considered the owner.[135]

[130] Sveriges Riksdag, Förslag till lag (2019:000) om automatiserad fordonstrafik 5(1-20).
[131] Sveriges Riksdag (n 35) 31.
[132] *Ibid 45-46.*
[133] Sveriges Riksdag (n 130) 1(4)(1).
[134] *Ibid* 1(4)(2).
[135] *Ibid* 1(4)(3).

If the vehicle is yet to be registered with a legal or physical person it would instead be the legal person, who through branding, or otherwise, is shown to be the owner of the vehicle[136], or the physical or legal person who was otherwise in control of the vehicle.[137] Furthermore the rules that apply to the owner are intended to apply to a non-owning person in control of the vehicle if it is purchased through credit with a take-back policy for non payment[138], or if there is a right of use that extends beyond one year of time.[139] If the owner of the vehicle is underage their legal guardians are considered the owners in the application of the law.[140]

The owner is proposed to be liable for the actions of the vehicle in fully autonomous driving. He is also liable in ensuring that there is a driver available during the autonomous driving, and, in failing to do so, will be fined.[141] A driver must be qualified to drive the vehicle at the time of the driving.[142]

The liability of the owner is based on a similar principle of control over the risk associated with the use of the autonomous vehicle as the control-based liability proposed by the European Parliament to be connected to the use of AI. The main reason behind the allocation of responsibility to the owner being that he is the one likely in the best position to control the state of the autonomous vehicle, similarly to the controlling operator in the European Parliament proposal being the person most likely to be in control of the risks associated with the use of any specific AI. In turn, the owner under the Swedish proposal, could be said to fall within the back-end operator spectrum of the European Proposal.

[136] *Ibid* 1(4)(4).
[137] *Ibid* 1(4)(5).
[138] *Ibid* 1(5)(1).
[139] *Ibid* 1(5)(2).
[140] *Ibid* 1(5)(3).
[141] *Ibid* 2(1).
[142] *Ibid* 2(2).

In the Swedish proposal criminal liability for any traffic crimes committed by an autonomous vehicle is also attributed to the owner, whereas the European Parliament proposals do not deal with criminal liability. The crimes remain only penalized in the form of sanction fees, with no possible jail time, which makes the liability seemingly look more like a civil one than a criminal one, although the fees are paid despite the lack of actual damage.

It must also be noted that, in similarity with the European Parliament proposals, the Swedish proposal provides a clear mode of redress in cases where the crimes committed are committed due to a faulty product, where

4.1.3 The notion of the Driver

As mentioned previously there is an international requirement for a driver to be ever present in vehicles operating in road traffic in the 1968 Vienna Convention on Road Traffic, which has been ratified by Sweden.[143] As such the requirement for a driver to be present will not be removed in the proposed regulation. The term '*Driver'*, however, will be redefined.

The legislative proposal will be considering a person in control of a vehicle either from inside of it or outside of it, through a remote, or otherwise, a driver. A driver can be in control of multiple vehicles simultaneously, and one vehicle can equally be controlled by multiple drivers simultaneously.[144]

The driver being able to control multiple vehicles and the possibility for a vehicle to be controlled by multiple drivers is reminiscent of the principles of control that are suggested in the European Parliament proposals, but whereas they provide a clear mode for the division of liability between controlling operators, there is no such division explicitly proposed in the Swedish proposal.[145] This could well be an improvement to be made in the interest of legal clarity and legitimate expectations for drivers.

[143] United Nations (n 127), Article 8.
[144] Sveriges Riksdag (n 35) 31; Sveriges Riksdag (n 130) 2(2).
[145] European Parliament (n 42) 13.

4.1.4 Liabilities and Responsibilities of the Driver

In the Proposed regulation the responsibilities of the driver are adjusted as well, removing the criminal liability from a driver for any tasks performed by a system for autonomous operation while the system is in use. As such there is no responsibility for a driver to monitor activities performed by an autonomous vehicle. The driver will, however, still be required to operate the vehicle should this be requested by the AI system in circumstances where the system is not equipped to solve a specific task on its own. Failure to fulfill this responsibility results in a fine.[146]

Responsibility for other legal obligations related to road traffic will yet remain with the driver, such as seatbelting children under the age of 15. Furthermore the driver must ensure that he possesses the correct qualifications to operate the vehicle[147], as well as fulfilling a requirement of sobriety.[148] Drivers are generally responsible not to use electronics in a way that interferes with safe driving. With the prospect of fully automated, autonomous vehicles the prohibition of the use of cellphones while driving[149] is proposed to be eased to exclude drivers of autonomous vehicles.[150]

In the case of an accident there are a certain set of responsibilities imposed on the driver of a regular vehicle, such as moving away from the scene of the accident as best he can, to avoid interfering with traffic, as well as putting out warning signs for fellow trafficants to alert them to the accident.[151] This requires a driver to be physically present, which may not be the reality when it comes to autonomous vehicles, as the driver may be far away from the scene of the accident in a control room. Instead it is proposed that the driver takes the necessary steps to ensure that the vehicle stays put until instructed otherwise, and that all actions possible are taken to keep the vehicle from hindering other traffic, as well as contacting the proper authorities to give a statement and leave information.[152]

[146] Sveriges Riksdag (n 130) 2(5).
[147] *Ibid* 2(7)
[148] *Ibid* 2(8)
[149] Trafikförordning (SFS 1998:1276), 11(10).
[150] Sveriges Riksdag (n 35) *43.*
[151] Sveriges Riksdag, Lag (SFS 1951:649) om straff för vissa trafikbrott para 5.
[152] Sveriges Riksdag (n 35) 48; Sveriges Riksdag (n 130) 2(10).

The liability remains with the responsible driver also when there is a low-interference user in the vehicle, i.e. a user who does not interfere with the autonomous driving beyond activating it, deactivating it, or setting a destination.[153] Looking at the driver liability of the Swedish legislative proposal one can draw parallels to the legislative proposal made by the European Parliament and the solution of control-based strict civil liability. One key difference between the two, however, is that the Swedish driver liability does not extend to a low-interference user, whereas it seems that the liability in such a situation under the European control-based liability regime would, at least partially, transfer to that user, as he would then be considered an operator with some control over the vehicle or AI.[154]

It would also be reasonable that tasks such as seatbelting a child would fall on a non-interfering user, rather than a driver that may be situated remotely. The driver concept in the Swedish proposal is awkward, as some of the tasks imposed on a driver can only be fulfilled by someone physically present, such as the seatbelting of a child. The legislative proposal, in the name of clarity, could potentially benefit from a clearer split between a user and an operator and thus refraining from using the somewhat ambiguous term of driver. As such it would be possible to clearly distinguish what responsibilities fall with an operator and a user respectively.

[153] *Ibid* 2(4).

[154] European Parliament (n 42) 13.

4.1.5 Autonomous driving-related Crimes

Three new crimes are introduced in the proposed regulation, these are additive to technology-neutral traffic crimes in other regulatory instruments. These crimes consist of gross negligence during autonomous driving[155], covering situations where an autonomous vehicle is used in such a manner that lives are put at risk. Furthermore illegal operation of a autonomous vehicle[156] is introduced, meaning operations without proper qualifications. This crime can include an unlicensed driver, a person who employs such a person to be the driver of autonomous vehicles or otherwise a person who lets an unqualified person be what is considered a driver during autonomous driving.[157] The crime of illegally operating a vehicle is essentially a transposition of an already existing law with a wording more suitable to the drivers of autonomous vehicles.[158]

While autonomous vehicles are generally meant to be driving safely and soundly, following rules there may be modifications made by users, or inappropriate operation or hijacking of a system for autonomous driving that can put others at risk. These modifications may be of a nature that lets the vehicle operate at higher speeds than what is allowed on a certain stretch of road. The gross negligence in traffic while driving autonomously is proposed to deal with such users, proposing a maximum two year prison sentence and loss of license for negligent, or conscious operation of an autonomous vehicle that puts the lives or health of others at risk.[159]

Furthermore there is the crime of autonomous driving under the influence[160]. This being a crime is motivated by the need for basic operative functions of the driver in case of an emergency. Should an autonomous car stop inappropriately or partake in an accident it is central that the driver is capable of taking control either manually or by ordering the car to perform tasks as to not interfere with traffic. This crime is connected with a maximum of two years in prison and a retracted license.[161]

[155] Sveriges Riksdag (n 130) 2(6).
[156] *Ibid* 2(7).
[157] Sveriges Riksdag (n 35) *32.*
[158] *Ibid 47.*
[159] *Ibid 46-47.*
[160] Sveriges Riksdag (n 130) 2(8).
[161] *Ibid* 47-48.

4.1.6 Responsibilities and Liabilities of the Producer

The investigation deems autonomous vehicles, no matter the level of automation, along with the system which operates it, to be considered products. As such they fall within the scope of the Swedish Produktansvarslagen, or product liability regulation. Under this regime damages are to be paid for both physical and fiscal damages caused to a person due to a security flaw in a product.[162]

A security flaw is defined as whenever a product is not as safe as can be expected. This is assessed with regards to how the product could be expected to be used, how it's been marketed and with regards to the instructions that are attached to the product, age of the product and other circumstances.[163]

Under this regime, however, not only the producer can be held liable for the damages. Both producers, importers and marketers can become liable for damages caused by their product.[164] If no such person can be identified, in domestic cases, the person who supplies the product will be held liable, unless he can provide information to identify one of the aforementioned persons. For an imported product the liability falls on the person supplying the product unless he can show the importer, or another person who has supplied him with the product.[165] The claiming right to damages is regressive[166], and as such ideally it would ultimately fall on the producer of the product.

The legislative proposal suggests a dynamic liability relation between the producer and these flaws, increasing in strength the further up on the SAE scale of automotion the vehicle operates on. The reasoning is that the more autonomous the car is, the lesser the driver's ability to interfere will be, and as such the driver should not be held liable to the same extent in the operation of a fully autonomous vehicle as in a vehicle which has only partial autonomous elements.[167]

[162] Produktansvarslag (SFS 1992:18) para. 1.
[163] *Ibid* para. 3.
[164] *Ibid* para. 6.
[165] *Ibid* para. 7.
[166] *Ibid* para. 11.
[167] Sveriges Riksdag (n 35) 46.

In the Swedish proposal there is a clear indication that any form of autonomous vehicle be viewed as a product, and that they would fall within the scope of national product liability regimes. This allows for a clear route as to how to address claims for losses in relation to product faults. The Swedish proposal furthermore provides a scale under which the liable parties are more or less liable with regards to the level of automotion the autonomous vehicles functions under. This scale may, however, be more relevant to autonomous vehicles rather than AI in general, motivating the lack of such a scale in the European Parliament proposals.

4.1.7 Vehicular Requirements

The proposed regulation is also intended to deal with the requirements for the autonomous vehicles themselves. Vehicles that are constructed to be able to operate without human intervention must e.g. be equipped with a safe-stoppage system that engages when a situation which the system can not otherwise handle arises.[168]

The Proposal further suggests a requirement for data storage to be imposed on vehicles capable of switching between autonomous- driving and driving, to ensure that it can be verified whether a vehicle was operating autonomously or if there was a driver in control. The proposed data to be stored is vehicle identification data, when autonomous has been engaged or disengaged, and whether the vehicle has required manual assistance at any point. The suggested storage period is to be six months, and the producers or importers of the vehicles will need permits to store information, as well as inform authorities about who is responsible for the storing of the data.[169] This storing of data needs to take place to help in the efforts to establish liability in cases of actions contrary to road traffic rules, as well as both criminal and civil liability in cases of accidents. It is proposed that as little data as possible is to be stored, to avoid interfering with individual privacy and integrity.[170]

[168] *Ibid 31-32.*
[169] *Ibid* 32.
[170] *Ibid 82-83.*

4.1.8 Other Considerations

It is suggested that traffic with autonomous vehicles should, in principle, function on the same roads as any other vehicle. It is, however, borne in mind that there may arise a need for local traffic ordinances regarding certain vehicles, and as such local governing bodies are equipped with possibilities to formulate such ordinances in the proposal.[171] The investigation also considers where and how autonomous vehicles should be allowed to operate. In the short term it is argued that the introduction of autonomous vehicles must be very limited, until the current infrastructure is up to speed with what is needed, as well as with respect to the support by international regulations. The investigation suggests that further investigation should be conducted into what infrastructural needs exist to make autonomous driving a real possibility, as well as to make current automated functions easier to use. Further it is suggested that investigation into how laws relating to the construction, upkeep and signage of roads could be altered to simplify the introduction of autonomous vehicles.[172]

[171] *Ibid 53.*
[172] *Ibid 54.*

4.2 Comparative Discussion with Regards to the Swedish Proposal and the European Parliament solution

The Swedish proposal offers a three-tiered liability split, between the driver, the vehicle owner, and the producer. The legislative proposal of the European Parliament features a similar split, but mainly focuses on an operator as the subject of the civil liability. The operator, similar to the split that is proposed in the Swedish legislation, includes the frontend operator - comparable to the driver of an autonomous vehicle in the Swedish legislation, and backend operators, including owners of the vehicle, as well as the producer and developers of it.

Both proposals suggest that product liability regimes be applicable, albeit in differing terms. The key terms in the Swedish proposal leaves it slightly ambiguous, and an improvement could be to replace the driver, owner, and producer split with front- and backend operators, for the purpose of uniform laws and legal clarity. Both proposals further suggest an insurance system be in place to ensure coverage of damages. Both regulations retain similar systems for redress in case of damage, ending at the producer of the autonomous vehicle or AI-system.

The operator liability in the European Parliament proposals, however, does not fully coincide with the allocation of liability in the Swedish proposal. Whereas the Parliament establishes that the operator is anyone that exercises control over the risk associated with the operation of the AI-agent, and benefits from its action, the Swedish proposal suggests that a person who inputs destination, or turns AI on or off without otherwise interfering with the operations of an autonomous vehicle is viewed not to be a driver, while still exercising a degree of control over the operations of the autonomous vehicle, seemingly directly contradicting the proposal of the Parliament.

There is also a clear attribution of criminal liability arising from crimes committed by autonomous vehicles. The liability is suggested to be attributed to the owner of the vehicle, qua a backend operator. The liability only extends to penal fees, similar to the penalties on the lower end of the scale for regular traffic crimes when committed by a traditional driver.

There are also driver-specific crimes that do not relate to the vehicle itself, beyond the crimes only being committable by the driver of an autonomous vehicle. The European Parliament proposals do not propose any way of dealing with criminal liability, and prioritizes instead strict liability regimes with solid models for compensation and modes of redress, ensuring that anyone suffering damages be compensated fairly.

While the criminal liability with regards to traffic crimes is dealt with in the Swedish proposal, there is no mention of other crimes, however, any damages arising from other types of crime would be covered by the strict civil liability, despite no sentencing of purely penal sanction fees in relation to such crimes being suggested. The European Parliament proposals do not take criminal liability into consideration, and while the electronic legal personhood may have allowed for criminal liability to be imposed, the idea was abandoned, focusing instead on the main purpose of ensuring coverage of any damages arising from the activity.

The Swedish legislative proposal further suggests a clear way of scaling the grade of liability for producers, scaling the liability in relation to the grade of automation under which a vehicle operates, whereas the European Parliament proposes a solution which is based on the grade of control the different operators exercise with regards to the risks associated with the use of the AI.

In considering the effects of self-learning, and the actions that might be taken at the volition of the autonomous, or AI, systems on the basis of information that has been picked up during the use of the product. This raises the question of when the liability can be moved from the producer to elsewhere, when the product, or fault in the product starts being viewed as a result of “modification” by self-learning through use, or misuse, and when it is considered a fault due to the programming of the self-learning functions. In this case the Swedish approach would be more rigid, but in turn allow for a higher grade of certainty, as the degree of automation is unchanged - while the approach of the European Parliament is more flexible and could potentially change with regards to these factors.

5. Conclusion

In this section the answers to the research question initially posted in the beginning of the essay will be answered with regards to the research material. The author will also present his opinions to fulfill the full purpose, as stated in the introductory segment of the thesis. Conclusions will be drawn from the research material, and the assessment of a reasonable way forward will mainly be based on the comparative discussion of the previous section.

5.1 Conclusions with Regards to the Research Questions

In the beginning of this essay I stipulated three questions to be answered to give clarity to what types of solutions could be adopted for the attribution of both civil and criminal liability in relation to artificial intelligence and autonomous vehicles;

> *‘What EU-level proposed principles and possibilities exist for the attribution of civil and criminal liability in relation to autonomous vehicles?’;*
>
> ‘*What concrete solutions for the attribution of civil and criminal liability are suggested in the Swedish draft legislation on autonomous vehicles?’* and;
>
> *‘’Is it realistically possible to attribute an artificial intelligence agent with civil or criminal liability qua some sort of legal personality?’.*

With regards to the first question there are four solutions proposed for the attribution and allocation of civil liability in relation to AI and autonomous vehicles by the European Parliament.

The first option that was discussed is a control based operator liability, backed by product liability. This solution would deem that all operators of an autonomous vehicle would be attributed civil liability for the damages caused by it. The term operator would include anyone with some form of control over the risks associated with the use of the AI, and would not just include the ‘driver’ of a car, but would extend to producers, software developers, service-persons etc. insofar as they are not already covered by the rules on product liability.

The liability would come in the form of strict liability, as autonomous vehicles fall into the category of high-risk AI under the proposals of the Parliament. Non high-risk AI would instead be connected to an at fault liability for the operator, under this regime. This solution is also connected to multi-level mandatory insurance systems, to ensure that damage arising from AI-activities be covered.

The liability for civil claims is limited to ten or thirty years depending on circumstances, and can be limited due to contributory negligence. The operator is also proposed to be liable to obtain correct insurances to ensure coverage of any civil liability that arises.

The European Parliament also discusses a second solution in applying a limited liability solution, split between the producer, owner and user - where all these actors contribute to a common insurance fund for all civil liability claims arising from AI activities and autonomous driving, pointing to the coverage of damages being the most important factor in the civil liability regime.

The third solution discussed by the European Parliament is a no-fault liability regime connected to a mandatory insurance system for any and all AI-agents falling under an annex to the proposed regulation, under the category of high risk systems. This system would operate similarly to that in place for traditional vehicles. These damages are suggested not be limited on the basis of autonomous operation, to ensure adequate protection of victims.

A fourth way suggested was the direct attribution of civil liability to the AI-agent or autonomous vehicle through the deeming of capable AI as a new form of electronic legal personality. This personhood, or legal persona, is suggested to be connected with an obligation to compensate for any damage caused, although it is left open who this obligation should apply to, but could likely be connected to the no-fault system that has also been suggested. This solution was later abandoned, with the Parliament stating that it would not be necessary in the light of the other proposed solutions for civil liability regimes in relation to AI.

The European Parliament seemingly settles on control based operator liability, backed by product liability, as the ideal solution, as this is the solution around which the concrete legislative proposal is formed. While abandoning the idea of an electronic legal personality, this solution balances aspects of the other two solutions proposed, incorporating the mandatory insurance system, a categorical split between strict and limited liability based on the type of AI-agent involved with modes of redress for liable parties when the product is faulty.

For the issue of attribution of criminal liability for artificial intelligence, there are no solutions proposed by the European Parliament. It could, however, be theorized that AI-agents, including autonomous vehicles, would be capable of fulfilling the fundamental elements of a crime, the *mens rea* and the *actus reus* - but not be held liable as they are viewed as objects. In the light of this the proposed solution for the creation of an electronic legal personality for the direct attribution of civil liability could also mean that criminal liability could possibly also be attributed to AI directly.

As for the second question, the regime for attributing liability in the Swedish legislative proposal is a three tiered one, relying heavily on product liability as a last resort. The proposal suggests for producers, owners and drivers of autonomous vehicles to be liable for different aspects of autonomous driving. The notion of a driver is changed to include remote controllers as well as physically present persons exercising a cautious control over the vehicle in case of emergency. Unlike the operator liability that is suggested in the European Parliament legislative proposal the Swedish model for liability is not entirely focused on the control of the risks associated with the use of the artificial intelligence, as it explicitly excludes someone who has control, but where the control does not go beyond activating, deactivating or choosing the destination for an autonomous vehicle.

The Swedish proposal gives a clear view that any form of autonomous vehicle be viewed as a product, and that they would fall within the scope of national product liability regimes. This allows for a clear route as to how to address claims for losses in relation to product faults. The Swedish proposal furthermore provides a scale under which the liable parties are more or less liable with regards to the level of automotion under which the autonomous vehicles function.

The criminal liability for any traffic offenses caused by an autonomous vehicle befall the owner of the vehicle, should this liability arise due to a faulty system the owner can claim damages with the producer, importer or distributor, in order of proximity. The driver is only responsible for non-AI related offenses.

With regards to the third question the suggestion to give AI electronic legal personalities initially faced criticism. A group of 150 experts argued that such a personality complicates things beyond what is necessary, with regards to the potential lack of a person standing behind the AI-agent or autonomous car, which is not the case with other types of legal persons. This could potentially become a step in the wrong direction in terms of legal certainty and clarity, and legitimate expectations for afflicted persons, and thus a direct contradiction to the principles laid out in the Parliaments general considerations.

It could also be argued that there really is no necessity to either attribute liability directly to an AI-agent. Especially so, as Papakonstantinou and de Hert recognize, since the establishment of an AI legal personality could potentially even be used to escape liability in e.g. situations involving autonomous vehicles, which would be quite the opposite of the intended effect of a liability regime.

Additionally the possibility for punishment directly aimed at an autonomous vehicle or other AI-agent does not seem to fulfill any penological purposes, or otherwise add any value to the possibility of claiming any damages arising from a criminal act conducted by an AI-agent. The important matter, judging by what both the European Parliament and the Swedish Government propose, is the awarding of damages and compensation to an afflicted party through the establishment and enforcement of a civil, rather than criminal, liability. As such there are no benefits to the establishment of electronic legal personalities for AI in neither matters of criminal, or civil, liability.

In the light of these considerations I would argue that, while creating a legal personality for AI would definitely be possible through legislative means, it would not fill any beneficial function beyond what would be filled by the other suggested liability regimes. The establishment of an electronic legal personality for AI-agents also leaves gaps and uncertainty as to where to direct claims for compensation, and theoretically enable escaping liability altogether. While this seems to be the only way in which criminal liability could be attributed to AI, no benefits can be identified in doing so. As such I would argue that the creation of a legal personality for AI, while possible, is not a realistic or viable way forward.

5.1 Author Opinions on A Reasonable Way Forward

In my opinion the most reasonable way forward in terms of regulating liability in relation to autonomous vehicles would be through a framework for liability regimes set out at a European Union level to ensure coherence and dispel fragmentation in the concrete applications in the shape of Member State legislations.

I argue that the best manner of attributing liability would be an operator based, strict, liability that is divided between operators with respect to the extent of the control exercised over the risk associated with the use of an autonomous vehicle.

I also propose a more clear division between back- and frontend '*Operators'*. Similarly to the European Parliaments Proposal I would also suggest that each variation of the '*Operator*' is associated with a guiding, but non-exhaustive list of examples of what persons would fall into respective categories of operators of an autonomous vehicle. I would refrain from mixing the '*Driver'*-term into the regulation, reserving it for the drivers of traditional vehicles rather than the persons in control of different aspects of an autonomous vehicle, in an effort to avoid ambiguity and further legal clarity.

My opinion is further that the balancing scale for front- and backend '*Operator*'-liability should take into consideration both the level of automation under which the vehicle operates, as is suggested in the Swedish Proposal, leaning more so to liability of the backend '*Operators'* as the level of automation in the vehicle rises. It should also be made clear that autonomous vehicles are products, and to what extent product liability rules apply to them, in place of backend '*Operator'*-liability.

I suggest that the SAE-scale be adopted for the purpose of establishing the extent of the backend '*Operator*' liability as proposed in the Swedish proposal. I do however think that there should be consideration paid to the extent of which decisions made by a highly autonomous vehicle rely on self- or deep-learning through use or misuse, potentially shifting focus away from the backend '*Operators'*, but that the burden of proof of misuse leading to faulty learning in the AI-system should be placed with the backend '*Operator*'.

My suggestion is further that, in likeness with the Swedish proposal, a low-interference user with no other relation to the autonomous vehicle than a short time use, e.g. in the shape of a autonomous taxi service, would be considered a '*passenger*', rather than a user, as to avoid associating any form of liability with a person in this situation. Not doing this, I would argue, muddles the lines between liable and non-liable parties. It would also discourage users from making use of some of the possible benefits of autonomous vehicles, hampering the development of the technology at large. The European Parliament has already expressed a wish to be on the vanguard in regulating this issue, and as such it would not make sense to hamper use.

With regards to criminal liability I consider the model adopted in the Swedish legislation as a reasonable way to move forward, attributing the liability to mainly backend '*Operators'*, and connecting the criminal liability to a sanction fee. The liability for damages arising from the criminal activities of autonomous vehicles should be civil in nature.

Finally I would propose, in concurrence with both the European Parliament and Swedish proposals, that coverage of liability should be ascertained through the implementation of a mandatory insurance regime, as I view the guarantee of damage coverage to be a key factor in encouraging the general public to trust and adopt the new technology. My suggestion would be that the responsibility for obtaining and upholding the correct insurances should fall on the registered owner of the autonomous vehicle.

6. Sources Index

6.1 Primary Sources

6.1.1 Case Law

Högsta Domstolen (Swedish Supreme Court), B 379-16

Högsta Domstolen (Swedish Supreme Court), NJA 2004 s. 176

6.1.2 International Legislation

European Parliament, 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

European Parliament, Directive (EU) 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licenses [2006] OJ L 403

United Nations, Vienna Convention on Road Traffic [1968]

6.1.3 National legislation

Sveriges Riksdag, Brottsbalk (1962:700)

Sveriges Riksdag, Lag (SFS 1951:649) om straff för vissa trafikbrott
(Swedish Parliament, Law on Punishment for Certain Traffic Crimes)

Sveriges Riksdag, Produktansvarslag (SFS 1992:18)
(Swedish Parliament, Swedish Law on Product Liability)

Sveriges Riksdag, Trafikförordning (SFS 1998:1276)
(Swedish Parliament, Traffic Regulation)

6.1.4 Policy Documents, Press Releases, Legislative Proposals etc.

European Parliament, Autonomous driving in European transport European Parliament resolution of 15 January 2019 on autonomous driving in European transport (2018/2089(INI) (15 January 2019)

European Parliament, 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) (20 October 2020)

European Parliament, Proposal For a Regulation of the European Parliament and of The Council on Liability for the Operation of Artificial Intelligence Systems (October 20 2020)

European Parliament, Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), (27 January 2017)

Sveriges Riksdag, SOU 2018:16

Sveriges Riksdag, Förslag till lag (2019:000) om automatiserad fordonstrafik

6.2 Secondary Sources

6.2.1 Literature

Asp, P, Ulväng, M, and Jareborg, N. *Kriminalrättens Grunder* (Lustus 2013)

Hall, D.E. *Criminal Law and Procedure*, (Cengage Learning 2015)

Holmes, O. W. *The Common Law* (*1st Edition*) (Macmillan, 1882)

Leijonhufvud, M and Wennberg, S. *Straffansvar* (Norstedts juridik 2009)

Russell, S, Norvig, P. *Artificial Intelligence - A Modern Approach (4th Edition)* (Pearson 2020)

6.2.2 Other Secondary Sources

Björklund, F. ‘Lurade Tesla att köra fel: ”Ett alarmerande svar”’, NyTeknik (25 June 2019)
<https://www.nyteknik.se/fordon/lurade-tesla-att-kora-fel-ett-alarmerande-svar-6962918>
Accessed 2 March 2022

Cardi, J. W. Reconstructing Foreseeability, Boston College Law Review 46, 921–988 (2005)
<.https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2311&context=bclr>
Accessed April 5 2022

Copeland, J et. al. ‘Alan Turing and the beginning of AI’, Britannica (20 July 1998)
<https://www.britannica.com/technology/artificial-intelligence/Alan-Turing-and-the-beginning-of-AI>
Accessed 5 March 2022

Hallevy, G. The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control, Akron Intellectual Property Journal (Akron Law Journals, 2016)

Hallevy, G. Dangerous Robots - Artificial Intelligence vs. Human Intelligence,(21 February 2018)
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3121905>
Accessed 5 May 2022

Hildebrandt, M. Ambient Intelligence, Criminal Liability and Democracy, 2 Criminal Law & Philosophy. 163, 164-170 (2008).

IBM Cloud Education, ‘Strong AI’, IBM (31 August 2020)
<https://www.ibm.com/cloud/learn/strong-ai>
Accessed 8 March 2022.

IBM Cloud Education, ‘What is machine learning?’, IBM (15 July 2020)
<https://www.ibm.com/cloud/learn/machine-learning#toc-machine-le-K7VszOk6>
Accessed 10 March 2022.

IHS Markit, Artificial intelligence driving autonomous vehicle development (30 January 2020)
<https://ihsmarkit.com/research-analysis/artificial-intelligence-driving-autonomous-vehicle-development.html>
Accessed 15 March 2022

Instructional Design, ‘General Problem Solver (A. Newell & H. Simon)’
<https://www.instructionaldesign.org/theories/general-problem-solver/>
Accessed 5 March 2022

IOP Publishing, Experts debate the possible paths to human-like AI, Physics World
<https://physicsworld.com/a/experts-debate-the-possible-paths-to-human-like-ai/>

Accessed 10th of March

Johnson, M. Powering Self-Driving Cars with Data Annotation (December 15 2021)
<https://tdan.com/powering-self-driving-cars-with-data-annotation/28890>
Accessed 15 March 2022.

Lee, T.B. ‘Safety driver in 2018 Uber crash is charged with negligent homicide’, ars Technica (16 September 2020)
<https://arstechnica.com/cars/2020/09/arizona-prosecutes-uber-safety-driver-but-not-uber-for-fatal-2018-crash/>
Accessed 2 March 2022

Legal Information Institute, Actus Reus, Cornell Law School
<https://www.law.cornell.edu/wex/actus_reus>
Accessed April 2 2022.

Legal Information Institute, Civil Liability, Cornell Law School
<https://www.law.cornell.edu/wex/civil_liability>
Accessed May 5 2022

Levitt, A. "Origin of the doctrine of mens rea." Illinois Law Review, 17, (1922)
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/illlr17&div=14&id=&page=>
Accessed 23 March 2022.

Loizos, C. ‘Uber has settled with the family of the homeless victim killed last week’, TechCrunch (March 30 2018)
<https://techcrunch.com/2018/03/29/uber-has-settled-with-the-family-of-the-homeless-victim-killed-last-week>
Accessed 2 March 2022

Lutkevich, B. Self-driving car (autonomous car or driverless car), TachTarget (October 2019)
<https://www.techtarget.com/searchenterpriseai/definition/driverless-car>
Accessed 15March 2022.

Malle, B.F, Nelson S.E. "Judging mens rea: The tension between folk concepts and legal concepts of intentionality." Behavioral sciences & the law 21 May 2003
<https://www.researchgate.net/publication/9085796_Judging_Mens_Rea_The_Tension_Between_Folk_Concepts_and_Legal_Concepts_of_Intentionality>
Accessed 23 March 2022

McCarthy, J. 'What is Artificial Intelligence?', Stanford University (24 November 2004).
<https://borghese.di.unimi.it/Teaching/AdvancedIntelligentSystems/Old/IntelligentSystems_2008_2009/Old/IntelligentSystems_2005_2006/Documents/Symbolic/04_McCarthy_whatisai.pdf>
Accessed 8 March 2022

Michael Tamir, 'What Is Machine Learning (ML)?', Berkley School of Information (26 June 2020)
<https://ischoolonline.berkeley.edu/blog/what-is-machine-learning/>
Accessed 10 March 2022

NHTSA, Automated Vehicles for Safety
<https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>
Accessed 2 March 2022

Vagelis Papakonstantinou, Paul de Hert. Refusing to award legal personality to AI: Why the European Parliament got it wrong, European Law Blog (25 November 2020)
<https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/>
Accessed 5 May 2022

Povolny, S. ‘Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles’, McAfee Labs (19 February 2020)
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/>
Accessed 2 March 2022

PwC ‘No longer science fiction, AI and robotics are transforming healthcare’,
<https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html>
accessed 3 March 2022

The Society of Automotive Engineers, SAE J3016

Searle, J. ‘The Chinese Room Argument’, Stanford Encyclopedia of Philosophy (2020)
<https://plato.stanford.edu/entries/chinese-room/>
Accessed 8 March 2022

Various Authors, Open Letter to the European Commission - Artificial Intelligence and Robotics, Politco.eu (April 2018)
<https://www.politico.eu/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf>
Accessed 2 May 2022