



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

**„Legal Aspects of Artificial Intelligence: the Issue of Legal
Personhood and Liability in the Context of the European Union“**

verfasst von / submitted by

JUDr. Adam Gregor

angestrebter akademischer Grad / in partial fulfilment of the requirements for the
degree of

Master of Laws (LL.M.)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears
on the student record sheet:

UA 992 548

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht /
European and International Business Law

Betreut von / Supervisor:

Dr. Maria Elisabeth Sturm, LL.M.

I. INTRODUCTION	1
I.I BACKGROUND	1
I.II AIM AND STRUCTURE OF THE THESIS	2
II. CONCEPT OF ARTIFICIAL INTELLIGENCE.....	3
II.I DEFINITION OF AI	3
II.I.I Robot	4
II.II EXAMPLES IN INDUSTRY.....	5
II.II.I Credit risk scoring	5
II.II.II Autonomous driving	7
II.II.III Military robotics	9
III. ETHICAL, SOCIAL AND LEGAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE	12
III.I THE ISSUE OF ETHICS.....	12
III.II SOCIO-ECONOMIC IMPLICATIONS	14
III.III LEGAL CHALLENGES	16
III.III.I Cybersecurity	16
III.III.II Data Protection	17
III.III.III Intellectual Property	19
IV. LEGAL PERSONALITY	22
IV.I CONCEPT OF LEGAL EXISTENCE/PERSONALITY	22
IV.II CURRENT LEGALLY RECOGNIZED TYPES OF LEGAL PERSONS.....	23
IV.III CRITERIA FOR RECOGNIZING NEW TYPES OF LEGAL PERSONS.....	24
V. LEGAL PERSONALITY OF ARTIFICIAL INTELLIGENCE	26
V.I RECOGNITION OF AI IN CONTEMPORARY EU LEGISLATION.....	26
V.I.I AI as a computer software	26
V.I.II AI as a product	27
V.I.III AI as a service	31
V.II MACHINE LEARNING VS. HUMAN INTELLIGENCE	31
V.III AI AS A DISTINCT LEGAL ENTITY.....	33
V.III.I EP resolution of 16 February 2017	34
V.III.II Open Letter.....	35
VI. LIABILITY.....	39
VI.I CONCEPT OF LIABILITY.....	39
VI.II TYPES OF LIABILITY	40
VII. LIABILITY FOR HARM CAUSED BY ARTIFICIAL INTELLIGENCE	41
VII.I RELEVANT DEBATE SO FAR	41
VII.II EU EFFORTS AFTER REJECTION OF E-PERSONALITY.....	42
VII.II.I High-Level Expert Group.....	44
VII.II.II Product Liability Directive of 1985.....	47
VII.II.III Automated decision-making	48
VII.II.IV White Paper	49
VII.III NON-HARMONIZED AREAS - EXAMPLE OF THE CZECH REPUBLIC	51
VII.III.I Damage caused by an animal	51
VII.III.II Damage caused by a person unable to assess the consequences of his acts.....	52
VII.III.III Damage caused by a particularly hazardous operation.....	53
VII.III.IV Damage caused by a thing.....	54
VII.III.V Vicarious liability.....	56
VIII. CONCLUSION	58

LIST OF ABBREVIATIONS

Anti-Money Laundering as **AML**

Artificial Intelligence as **AI**

Austrian Council on Robotics and Artificial Intelligence as **ACRAI**

Business-to-Consumer as **B2C**

Court of Justice of the European Union as **CJEU**

Credit Risk Management as **CRM**

Defense Advanced Research Projects Agency as **DARPA**

European Commission as **EC**

European Defence Fund as **EDF**

European Economic and Social Committee as **EESC**

European Parliament as **EP**

European Patent Office as **EPO**

European Union as **EU**

European Union Agency for Cybersecurity as **ENISA**

General Data Protection Regulation as **GDPR**

High-Level Expert Group as **HLEG**

Information and communications technology as **ICT**

Intellectual property as **IP**

Internet of Things as **IoT**

Society of Automotive Engineers as **SAE**

Treaty on the Non-Proliferation of Nuclear Weapons as **NPT**

Trustworthy AI assessment list **ALTAI**

United Kingdom as **UK**

United Nations as **UN**

United Nations Educational, Scientific, and Cultural Organization as **UNESCO**

United States as **US**

World Commission on Ethics of Scientific Knowledge and Technology as **COMEST**

World Health Organization as **WHO**

„(...) from Mary Shelley's Frankenstein's Monster to the classical myth of Pygmalion, through the story of Prague's Golem to the robot of Karel Čapek, who coined the word, people have fantasized about the possibility of building intelligent machines (...)”

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

I. INTRODUCTION

I.I Background

Technological advancement always sparked excitement as well as concerns. However, progress in certain areas makes people especially anxious. It comes as no surprise that when it comes to being worried, invention of kettle can hardly be compared with introduction of atomic bomb. If the two mentioned devices represented edges of scale used for measuring uneasiness, AI would certainly be found very close to the latter.

It is entirely understandable. Science-fiction genre certainly played a significant role. Works of Isaac Asimov or famous Hollywood films influenced millions and helped to portray a world of machinery overpowering humanity.

Many famous economy experts believe that AI will make redundant more jobs than it will create; consequently, cause significant disturbance of economy. Furthermore, many scholars and known industry figures who we regard as intellectual leaders publicly expressed their beliefs that autonomous killing machines might eventually subjugate or even annihilate human kind.

The truth is that the speed at which advancement of technologies takes place has been stunning. And it certainly accelerates. Computers defeat chess masters, autonomous vehicles drive our roads, garden water system will not turn on in the morning if it rained at night, and our internet browser always seems to know what kind of article we would like to read and what product or service we are currently looking for.

In medicine, machines carried out their first complicated surgeries outperforming human surgeons. AI ensures that airplanes do not collide in the air or when taking off and landing at airports. In rescue missions computers process aerial footage so quickly, that success rate of finding survivors has multiplied.

And so displays of AI have so far been generally accepted as something rather beneficial to the society. Making our lives safer, simpler and therefore more enjoyable. Despite that, concerns have stayed as they relate to the future which is, by definition, uncertain.

I.II Aim and structure of the thesis

The law is often behind innovation, as it usually merely reacts to it, rather than defines regulatory framework within which technological progress would take place. It is difficult to avoid, therefore, to some extent, legitimate. Furthermore, considering the fact that new technologies are typically introduced as means to create value for humanity, restrictions might not even be desirable.

On the other hand, not having clear, applicable and enforceable rules governing issues such as development and operation of autonomous weapons or automatic generating of medical diagnoses could, eventually, prove to be a tragic mistake.

The master thesis attempts to answer a number of questions associated with the matter briefly outlined above, and, as the title hints, focuses on AI.

After short introductory part the reader is provided with explanation of basic terms that will be used in the main sections of the work, examples of industries already heavily impacted by AI as well as description of challenges that AI represents for various realms of society.

The following chapters examine the question of whether AI is worthy of existence in the eyes of the law, i.e. if it should be endowed with rights and subject to obligations as legally recognized entity similar to corporations and individuals.

Irrespective of how the previous is answered, the crucial topic of liability follows in the next chapter. The vision of AI behaving in manners deviating from designers' expectations remains to be the most frightening, and serves as the ultimate trigger for all the discussions and regulatory efforts, that the thesis aims to explore, assess and propose.

In order to have a structured, transparent and sensible approach, and despite existence of large amounts of rules of different nature, legal force and jurisdictions throughout the world, the thesis focuses on the relevant debate within the framework of EU.

Used methodology entails especially review of relevant literature and existing legislation and analysis of regulatory efforts with emphasis on the activity of EC and EP. Comparative approach is seldom used to emphasize different approaches to regulation.

II. CONCEPT OF ARTIFICIAL INTELLIGENCE

II.I *Definition of AI*

Almost no jurisdiction provides legal definition of AI. A rare example is attempt of New Jersey's legislator according to whom AI means „use of computers and related equipment to enable a machine to duplicate or mimic the behavior of human beings“.¹

In January 2017, EP requested EC to propose common EU definitions of certain AI-based technologies such as cyber physical systems, autonomous systems and smart autonomous robots by taking into consideration list of characteristics of a smart robot (self-learning from experience, adaptation of behavior and actions to the environment, absence of biological life, etc.).²

Later in 2017, EESC identified AI broadly as „a catch-all term for a large number of (sub)fields such as: cognitive computing (algorithms that reason and understand at a higher (more human) level, machine learning (algorithms that can teach themselves tasks), augmented intelligence (cooperation between human and machine) and AI robotics (AI imbedded in robots)“³, and dared to go even further claiming that „central aim of AI research and development is, however, to automate intelligent behavior such as reasoning, the gathering of information, planning, learning, communicating, manipulating, detecting and even creating, dreaming and perceiving“⁴.

In April 2018, EC straightforwardly referred to AI as „systems that display intelligent behavior by analyzing their environment and taking actions - with some degree of autonomy - to achieve specific goals“, while emphasizing that AI-based systems can be entirely software-based such as search engines or speech and face recognition systems or AI can be embedded in physical devices (e.g. robots or autonomous vehicles).⁵

¹ Act concerning autonomous vehicles, and supplementing chapter 3 of Title 39 of the Revised Statutes Bill (NJ) 2016, S343, s. 1.

² European Parliament, 'Report with recommendations to the Commission on Civil Law Rules on Robotics', 2015/2103 (INL), 27 January 2017, s. 1.

³ European Economic and Social Committee, 'Opinion on Artificial intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (2017/C 288/01), s. 2, sub-s 2.1.

⁴ Ibid.

⁵ European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018, p. 1.

ACRAI views AI as „systems that display “intelligent” behavior by analyzing their environment and taking actions - with some degree of autonomy - to achieve specific goals“⁶, while a popular understanding of AI is that it will enable a computer to think like a person. The famous “Turing test”⁷ holds that AI is achieved when a person is unable to determine whether a response to a question he or she asked was made by a person or a computer.⁸ Therefore, the results of the test are not dependent on the ability of the machine to answer correctly, but rather it is observed how much the answers resemble those of a human.

EC in its latest document on AI significantly simplified all the previous definitions into „a collection of technologies that combine data, algorithms and computing power”⁹ as such definition „needs to be sufficiently flexible to accommodate technical progress”¹⁰.

II.I.I Robot

Perhaps if this paper was a dissertation, we would be going very deep into areas such as IoT, Blockchain or Industry 4.0 and other “state-of-the-art” or “cutting-edge” technologies but, in accordance with the purpose of the master thesis, the only other AI-related term which should be explained, as it is frequently interchanged with AI, is “robot”.¹¹

Robots and AI are two different things. The most important distinction lies in the fact, that a robot is just a machine, a physical device which moves as it is programmed to do so if triggered (drones, autonomous vehicles, etc.),¹² while AI can be found virtually everywhere. It can be within a physical device such as a robot. It could be in a fixed machine, or it can be just a mere software without physical existence in the usual sense. AI is about programming a software, so that it imitates (human) intelligence, or, in case the predictions are true, actually possesses it.

⁶ Austrian council on robotics and artificial intelligence , 'Shaping the Future of Austria with Robotics and Artificial Intelligence' (www.acrai.at) <<https://www.acrai.at/en/home/>> accessed 20 June 2020.

⁷ Named after its author, the famous Alan Turing.

⁸ Amitai & Oren Etzioni, 'Should Artificial Intelligence Be Regulated?' (www.issues.org, 1 July 2017) <<https://issues.org/perspective-should-artificial-intelligence-be-regulated/>> accessed 20 June 2020.

⁹ European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust (Brussels, Cm 65, 2020), p. 2.

¹⁰ Ibid, p. 16.

¹¹ The term was firstly coined by Czech writer Karel Čapek in his play R.U.R. (Rossum's Universal Robots, 1920). The expression was derived from “robota”, which is Czech term for “forced labor”.

¹² Even though, according to some robot can actually refer even to virtual entities such as “(chat)bots”.

To conclude, robot is a machine which either needs or doesn't need AI to perform its assignments. Robot, as opposed to AI, has physical form and either serves or doesn't serve as AI carrier.

Therefore, AI is an area of computer science, while robotics is a field of engineering, that is focused on building and operating robots, which are mechanical tools, that can, due to their AI equipment and at different levels of advancement, act autonomously.

II.II Examples in industry

This short sub-chapter contains three examples of areas which are and going forward will be gradually more influenced by AI. I intentionally chose those fields of industry, where safety and potential invasion into rights of individuals is especially at stake so as to demonstrate the importance of existence of proper legal framework and to emphasize the necessity to address the issues, that form the subject matter of this master thesis.

II.II.I Credit risk scoring

In financial industry AI has tremendous future, but evidence of its use can be found already today. It finds its place in investment consultancy or when fulfilling obligations prescribing monitoring of customer behavior (e.g. mandatory reporting of suspicious transactions pursuant to AML legislation).

However, as the heading indicates, the use of big data and machine learning for the purpose of credit risk scoring assessments has had especially significant impact. Such procedure entails evaluation of one's creditworthiness based on which credit decisions are taken.¹³

Traditionally, such scoring methods focus primarily on data provided by the applicant in the credit application, such as pay slips as well as information the institution itself may request from central credit registers (typically public) or purchase from credit bureaus (typically private). The various data points collected are then used to develop a model through a traditional process that can involve varying degrees of

¹³ European Banking Authority, 'Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech' (www.eba.europa.eu, 3 July 2018) 23 <<https://eba.europa.eu/sites/default/documents/files/documents/10180/2270909/02c7859f-576e-421e-b243-a145c0eaa131/Report%20on%20prudential%20risks%20and%20opportunities%20arising%20for%20institutions%20from%20FinTech.pdf?retry=1>> accessed 21 June 2020, p. 23.

statistical analysis which is steered, to a large extent, by the developer of the model. Through these means, credit institutions try to establish the probability that the customer defaults on payments.¹⁴

Lately, increasing importance of e-commerce, IoT or big data use triggered emergence of alternative credit scoring models. These use customer data from variety of many other sources, such as social media, location data, mobile data or behavioral data. These sources can then be used to assess willingness to pay or the potential debtor's responsibility in order to be able to predict such customer's probability of default.¹⁵ These alternative modeling techniques will therefore have access to and assess many other types of information such as the customer's payments of non-loan products (rent, insurance, energy), or they will be taking into account data relating to the client's stability (how frequently the individual changes residence, employment or e-mail address), and consider behavioral data (how the consumer browses the internet, shops or uses various other devices).¹⁶

In general, it is quite clear that the more efficient processing of information, and not exclusively in the area of credit decisions, the more efficient financial system. FinTech applications of AI and machine learning can even help improve regulatory compliance and increase supervisory effectiveness. These applications show substantial promise but only if their specific risks are properly managed.¹⁷

Because where AI and machine learning is employed in CRM, certain risks can be found that are not present to the same extent when traditional means for assessing creditworthiness are used. For example, if financial health is assessed based on a calibrated algorithm, that is encouraged to learn and evolve in accordance with obtained information, then lack of transparency, human supervision and auditing can result in false results that would else be easily detected by human intelligence.

The use of machine learning algorithms in credit scoring tools may lead to financial exclusion from access to financial services, even if unintentionally. This could

¹⁴ Ibid.

¹⁵ Ibid.

¹⁶ Ibid., p. 25.

¹⁷ Financial Stability Board, 'Artificial intelligence and machine learning in financial services - Market developments and financial stability implications' (*Www.fsb.org*, 1 November 2017) 1, 2 <https://www.fsb.org/wp-content/uploads/P011117.pdf> accessed 21 June 2020.

arise, for instance, if the algorithms discriminate against those who are less willing to share their data online.¹⁸

The presence of risks is undeniable, but the vision of employing AI and machine learning and thereby producing more precise risk assessments while saving internal resources is so tempting, that it is unavoidable. Not having these possibilities will be considered a competitive disadvantage, which creditors will not be willing to risk.

II.II.II Autonomous driving

Ever since the 1930s, science fiction writers portrayed a future with cars that drive themselves, and building them has been a challenge for the AI community since the 1960s. By the 2000s, the dream of autonomous vehicles became a reality in the sea and sky, and even on Mars, but self-driving cars existed only as research prototypes in labs. Driving in a city was considered to be a problem too complex for automation due to factors like pedestrians, heavy traffic, and the many unexpected events that can happen outside of the car's control.¹⁹

During DARPA's "grand challenge" on autonomous driving in 2004, research teams failed to complete the challenge in a limited desert setting. But in eight short years, between 2004-2012, speedy and surprising progress occurred in both academia and industry.²⁰ Today, due to rapid advancements in development of technologies such as object detection and trajectory algorithms, autonomous vehicles drive on the roads in several countries.

Statistics have shown that the major factor in 94 percent of all fatal crashes is human error.²¹ WHO adds that each year nearly 1.3 million people die as a result of a road traffic collision.²²

Autonomous vehicles represent a means of improving these statistics and in the future maybe even eliminating car accidents entirely. Moreover, removing human factor

¹⁸ Consumer Financial Protection Bureau, 'Requests for Information: Use of Alternative Data and Modeling Techniques in Credit Process' (www.regulations.gov, 19 May 2017) <https://www.regulations.gov/document?D=CFPB_FRDOC_0001-0521> accessed 21 June 2020.

¹⁹ Stanford university, 'Artificial Intelligence and Life in 2030' (One Hundred Year Study on Artificial Intelligence (AI100), 1 September 2016), p. 19 <<https://ai100.stanford.edu/>> accessed 21 June 2020.

²⁰ Ibid, p. 20.

²¹ US Department of Transportation, 'Automated Driving Systems: A Vision for Safety' (National Highway Traffic Safety Administration, 1 September 2017) <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069aads2.0_090617_v9a_tag.pdf> accessed 22 June 2020.

²² World Health Organization, 'Global Plan for the Decade of Action for Road Safety 2011-2020' (www.who.int, 11 May 2011), p. 4 <https://www.who.int/roadsafety/decade_of_action/plan/plan_english.pdf> accessed 22 June 2020.

could deal with traffic jams and generally improve mobility of people; consequently, their overall productivity.

Nonetheless, like in the financial sector, introduction of AI and machine learning into road transport brings its risks and obstacles. What if such vehicle causes an accident? We are still at the stage when most AI-equipped vehicles require permanent driver control. Who shall be held accountable for harm caused by its operation? Who should be responsible once vehicles are entirely autonomous? And how will AI cope with complicated situations such as making a decision between crashing into another vehicle or avoiding it while hitting a pedestrian?

It is absolutely essential that the law gives answers to these questions. So far, as we will discuss further in the thesis, such situation would typically be dealt with using provisions governing product liability or liability for damage caused by a thing, but it has become clear that special liability legislation coping with situations where AI plays a role might be needed.

Fortunately, discussions concerning making amendments to regulation of using AI in road traffic have been taking place in developed countries for years now. In EU, various Member States have already enacted rules on conditions for testing of such vehicles prior to their market introduction and even amended their road transport legislation which often considered autonomous driving illegal in adherence to original phrasing of Art. 8 of Vienna Convention on Road Traffic of 1968 according to which „every moving vehicle shall have a driver“, and „every driver shall at all times be able to control his vehicle“. In 2016, even the Convention was finally revised, so that it reflects reality and does not stand in the way of further technological advancements. The new wording permits AI technology („Vehicle systems which influence the way vehicles are driven“) to take over driver’s tasks, provided that such technology is in compliance with other UN regulations or can be „overridden or switched off by the driver“. ²³

²³ Economic Commission for Europe - Working Party on Road Traffic Safety, 'Report of the sixty-eighth session of the Working Party on Road Traffic Safety' (www.unece.org, 17 April 2014), p. 9 <<https://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf>> accessed 24 June 2020.

Individual efforts of Member States are coordinated by EU. Most notable is probably introduction of guidelines which attempt to harmonize exemption procedure for EU approval of automated vehicles from 2019.²⁴ The document describes procedure for allowing introduction of technologies not foreseen by current EU legal framework. Such exemption shall be granted on the basis of national ad-hoc safety assessment. The document expressly refers to vehicles on SAE levels 3 and 4,²⁵ which are being tested and, in some countries, already even operated.

However, the initiatives described above merely deal with making operation of such vehicles on roads legal, but do not address the issue of accountability for harm caused by them.

II.II.III Military robotics

There are pros and cons to everything. That is ancient wisdom. Positives of introducing AI into our daily lives are undeniable as well as dangers it carries. However, certain dangers are more concerning than other. Legislator will hardly be putting much effort into making sure, that chatbots really answer the questions, that the website's visitor is asking. On the other hand, succeeding at ensuring global consensus on enactment of rules in certain other areas is so important, that the alternative could result in global catastrophe.

Autonomous weapons development serves as a great argument of those pointing out the dangers of AI development and utilization. Hollywood films helped all of us to visualize what lack of rule framework in this field could result in. Image of AI making a decision on when the weapon should fire, at what intensity, and on what targets is so sobering that the international community has been paying much attention to it for some time now.

States weren't hesitant about signing NPT, which was the cause of many countries abandoning their nuclear programs. Similarly, other treaties forbade landmines or biological and chemical weapons. One would think, that global ban on autonomous weapons development should be analogically "simple" to introduce. However, the challenge here is that, as opposed to the previous examples, it is very hard to draw a line

²⁴ European Commission, 'Guidelines on the Exemption Procedure for the EU Approval of Automated Vehicles' (Brussels, 2019).

²⁵ SAE is automotive standardization body, which in 2014 introduced their automation classification, according to which vehicles shall be classified on six levels ranging from entirely manual to fully autonomous.

between what should be prohibited and what should be allowed. The reason being that certain amount of autonomy forms an integral part of any software which uses algorithms.

Already in 2013, EP published study called Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare, where it came to the conclusion, that:

„rapid development and proliferation of drone and robotic technology and the perceived lack of transparency and accountability in current policies, has the potential of polarizing the international community, undermining the rule of law and, ultimately, of destabilizing the international security environment as a whole”.²⁶

In the document EP, inter alia, proposed that EU works towards the adoption of a binding international agreement, or a nonbinding code of conduct, aiming at restricting the development, proliferation and/or use of certain unmanned weapon systems.²⁷

In famous open letter signed by leading intellectuals and researchers²⁸, which was presented at the 2015 International Conference on AI, UN is urged to propagate ban on offensive autonomous weapons systems:

The key question for humanity today is whether to start a global AI arms race or to prevent it from starting. If any major military power pushes ahead with AI weapon development, a global arms race is virtually inevitable. (...) Unlike nuclear weapons, they require no costly or hard-to-obtain raw materials, so they will become ubiquitous and cheap for all significant military powers to mass-produce. It will only be a matter of time until they appear on the black market and in the hands of terrorists, dictators wishing to better control their populace, warlords wishing to perpetrate ethnic cleansing, etc. (...) We therefore believe that a military AI arms race would not be beneficial for humanity. (...) Starting a military AI arms race is a bad idea, and should be prevented by a ban on offensive autonomous weapons beyond meaningful human control.²⁹

In September 2018, EP adopted resolution „urging to work towards the start of international negotiations on a legally binding instrument prohibiting the use of lethal

²⁶ European Parliament - Directorate General for External Policies, 'Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare' (www.europarl.europa.eu, 1 May 2013), p. 4 <[https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPODROI_ET\(2013\)410220_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPODROI_ET(2013)410220_EN.pdf)> accessed 24 June 2020.

²⁷ Ibid.

²⁸ Stephen Hawking, Elon Musk, Steve Wozniak, Frank Wilczek, Noam Chomsky, Nils J. Nilsson, Barbara J. Grosz, Stuart Russell, etc.

²⁹ Future of life institute, 'Autonomous Weapons: An Open Letter From AI & Robotics Researchers' (<https://www.futureoflife.org>, 28 July 2015) <https://futureoflife.org/open-letter-autonomous-weapons> accessed 24 June 2020.

autonomous weapons systems,”³⁰ which are referred to as „weapon systems without meaningful human control over the critical functions of selecting and attacking individual targets”.³¹

Unfortunately, until now attempts to ban or at least control development of autonomous weapons had the form of mainly soft law and not many concrete steps towards adoption of binding rules have been done; no doubt due to the nature of international law.

Perhaps the biggest and most tangible step towards such aim was accomplished within the framework of EU, when an interinstitutional agreement between EC, EP, and the Council of the EU was struck, pursuant to which it will not be possible to use the common defence budget (EDF) for years 2021-2027 to fund development of lethal autonomous weapons systems.³²

³⁰ European Parliament resolution 2018/2751(RSP) of 12 September 2018 on autonomous weapon systems.

³¹ Ibid.

³² Andreea Stoian Karadeli, 'The European Defence Fund - What are the political, economic and ethical aspects of the most important measures of the EU's new security and defence agenda?' (www.euro-sd.com, 13 December 2019) <<https://euro-sd.com/2019/12/articles/15510/the-european-defence-fund-what-are-the-political-economic-and-ethical-aspects-of-one-of-the-most-important-measures-of-the-eus-new-security-and-defence-agenda/>> accessed 24 July 2020.

III. ETHICAL, SOCIAL AND LEGAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

It was already mentioned how AI benefits society and what risks go hand in hand with it. The reader was presented with representative examples of fields, where AI plays a role and shall be increasingly applied going forward. Previous parts of the thesis indicated, that the implications are far-reaching and challenge most areas of social life.

If we want to discuss how legal systems should react to such fundamental changes to society, it is essential that first we pay attention to the question of what features of human life are to be impacted, how socio-economic factors will be influenced and what consequences these changes will have for human rights and liberties. Therefore, in this sub-chapter the paper briefly elaborates on the ethical side of things, socio-economic implications with emphasis on transformation of labor market, and certain specific legal challenges such as IP and data protection, before the paper proceeds with the core topics of legal existence and liability for damage or injury caused by AI.

III.I The issue of ethics

New ethical questions emerge in connection with development and employment of AI. The part of morality which attempts to give answer to such questions is commonly referred to as “roboethics“. Despite reference to „robots“ the term should be understood as dealing with principles regulating below listed problems with respect to AI in general including AI in the form of software without any external physicality.

Roboethics aims to resolve matters such as algorithmic bias³³ or privacy breach by adopting codes of ethics, which promote leaving essential decision-making to humans, refuse shifting liability onto AI and require full transparency of AI functioning.

Codes of ethics and ethical solutions will affect adoption, interpretation and application of legal rules governing development and use of AI. They will play an especially crucial role in the areas of prevention and liability.

³³ Algorithmic bias should be understood as a prejudice that leads to discrimination of certain individuals or groups. Such prejudice can be established due to particular AI’s design which reflects understanding of the world in the way the developer sees it (which can be entirely unintentional), or because of automation in accordance with certain data as patterns defining AI’s future behavior. Consequently, if in the past black people received longer sentences than white people for the same crimes and AI uses this data in order to determine the logic of its decision-making, it could repeat those errors.

This field of ethics, no doubt due to its undeniable importance, gained worldwide attention. In 2017, initiative of Future of Life Institute (the same institution that published the above mentioned open letter) presented its 23 “Asilomar AI Principles”³⁴ which apply to research and development as well as utilization of AI. The document emphasizes, that the goal of AI research should be to create beneficial intelligence, and that there should be a so called “science-policy link“, i.e. constructive and healthy exchange between AI researchers and policy-makers. Furthermore, it promotes safety measures, existence of rules for liability, privacy protection, human control or avoidance of arms race in lethal autonomous weapons.³⁵

In EU, efforts to adopt ethical approach to development and use of AI have been apparent for some time now. In 2017, EP called on the Council to „develop a strict and effective common EU framework, giving the utmost importance to respect for ethical principles, human rights and international humanitarian law“.³⁶ At the same time, EP formulated so called “Charter on Robotics“, which comprises Code of Ethical Conduct for Robotics Engineers, Code for Research Ethics Committees (REC), License for Designers and License for Users.³⁷

EC in April 2018 published its “Artificial Intelligence for Europe“, where it is acknowledged that:

AI may raise new ethical and legal questions, for example related to liability or biased decision-making. The EU must therefore ensure that AI is developed and applied in an appropriate framework which promotes innovation and respects the Union’s values and fundamental rights as well as ethical principles such as accountability and transparency.³⁸

EC vowed to further invest into creation of appropriate ethical and legal framework based on EU’s values and in line with the Charter of Fundamental Rights of the European Union while stating that „the EU is also well placed to lead this debate on the global stage“.³⁹

³⁴ Future of Life Institute, 'Asilomar AI Principles' (www.futureoflife.org, 8 January 2017) <<https://www.futureoflife.org/ai-principles/>> accessed 25 June 2020.

³⁵ Ibid.

³⁶ European Parliament, 'Report with recommendations to the Commission on Civil Law Rules on Robotics', 2015/2103 (INL), 27 January 2017.

³⁷ Annex to European Parliament’s 'Report with recommendations to the Commission on Civil Law Rules on Robotics', 2015/2103 (INL), 27 January 2017.

³⁸ European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018.

³⁹ Ibid.

III.II Socio-economic implications

Introduction of AI has many positive consequences for labor market. Benefits of automatization can be clearly observed where jobs entail routine and repetitive actions. Those will be taken over by AI so that human resources may be used where creative activities with higher added value are required. In addition, automatization increases effectivity and quality where machines are able to be employed instead of men. In developed countries with unfavorable demographic development machines can resolve the problem with missing manpower.

Furthermore, according to EC two million jobs were created due to automatization over the last ten years in EU and another 1,75 million are anticipated to be created in the ten years to come in ICT sector.⁴⁰

However, and as was already demonstrated in the previous sections, every coin has two sides and this is not an exception. Certain professions can be quite legitimately worried about these developments as employers will rather invest into automatization because, in the long run, high initial investment will eventually pay off. Since automatization is introduced in certain industries and certain regions first, society will inevitably face the prospect of deepening of economic inequality.

EC has been well aware of the challenges AI poses with respect to employment and repeatedly stressed out that „it is time to make significant efforts to ensure that no one is left behind in the digital transformation“.⁴¹

AI is changing the nature of work: jobs will be created, others will disappear, most will be transformed. Modernization of education, at all levels, should be a priority for governments. All Europeans should have every opportunity to acquire the skills they need. Talent should be nurtured, gender balance and diversity encouraged.⁴²

The idea is rather straightforward. Those workers whose professions will disappear or transform to such extent that these individuals will not be of use to their employers (or clients/customers in case of freelancers) anymore, must have the

⁴⁰ European Commission, 'AI and Automation' (www.ec.europa.eu, 23 July 2019) <https://ec.europa.eu/knowledge4policy/foresight/topic/changing-nature-work/AI-and-automation_en> accessed 26 June 2020.

⁴¹ European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018.

⁴² Ibid.

possibility to acquire new skills they need in order to be able to succeed in the transformed market.⁴³

In the latest communication (2020), EC intensified its warnings and announced new predictions for development of automation. Apparently, between 2020 and 2022 two million new robots are to be installed in industrial plants worldwide. Up to fifty percent of jobs could be automated in the years to come. Industry fields, such as manufacturing, customer services, healthcare or agriculture are in particular predisposed to automatization.⁴⁴

Therefore, in order to minimize the above mentioned and other negative effects of automatization legal systems have to undergo significant changes. This transformation will entail adjustments of education, social security schemes and various alterations to employment legislation.

With regards to concrete steps undertaken, EU supports the Member States in several areas but perhaps the most tangible result of the EC's activities is the fact that over the period 2014-2020 the European Social Fund which forms a part of the European Structural and Investment Funds invested EUR 2,3 billion specifically in digital skills development.⁴⁵

On 7 May 2018, EC even announced establishment of dedicated High-Level Expert Group on the Impact of the Digital Transformation on EU Labor Markets, comprising academics as well as representatives of industry. In April 2019, the newly formed body issued report⁴⁶ with recommendations including policy actions for EU, Member States and businesses.

Another notable measure proposed with the aim to face the challenge of such labor market transformation takes us to US. In January 2019, a bill was introduced in the House of Representatives named "Artificial Intelligence Job Opportunities and Background Summary Act of 2019" also known as "AI Jobs Act of 2019", requiring the US Department of Labor, in collaboration with academia, industry and government, to

⁴³ European Commission, 'AI and Automation' (www.ec.europa.eu, 23 July 2019) <https://ec.europa.eu/knowledge4policy/foresight/topic/changing-nature-work/AI-and-automation_en> accessed 26 June 2020.

⁴⁴ Ibid.

⁴⁵ Aoife Kennedy, 'European Social Fund' (www.europarl.europa.eu, 1 February 2020) <<https://www.europarl.europa.eu/factsheets/en/sheet/53/european-social-fund>> accessed 24 July 2020.

⁴⁶ European Commission, 'Report of the High-Level Expert Group on the Impact of the Digital Transformation on EU Labor Markets', April 2019.

prepare a report on artificial intelligence and its effects on the workforce,⁴⁷ that would later serve as a basis for adoption of various necessary legislative enactments.

III.III Legal challenges

In this part, the thesis begins to focus exclusively on how emergence of AI challenges the law, even though already in the previous sections it was many times pointed out, that the legislator has to act in numerous areas of regulation.

Most studies concerning the need for adaptation of current rule frameworks and adoption of new guidelines including legal rules concentrate on imperfections of current legal systems and present principles which shall govern introduction, interpretation and application of the new norms (transparency, accountability, ethical approach, cooperation between policy-makers, academics and industry, etc.).

III.III.I Cybersecurity

There are many areas of the law that have to be adapted due to the technological progress associated with AI. Here, the paper gives several examples, where legislation in its current form is challenged. One of them is cybersecurity.

AI poses threat to information security as well as a highly effective tool, for instance, due to its ability to analyze data from millions of cyber-attacks, which enables it to identify further threats.

On EU level, “NIS Directive”⁴⁸ „provides legal measures to boost the overall level of cybersecurity”⁴⁹, while “Cybersecurity Act”⁵⁰ „revamps and strengthens ENISA and establishes an EU-wide cybersecurity certification framework for digital products, services and processes”.⁵¹

⁴⁷ H.R. 827 - 116th Congress: AI JOBS Act of 2019. www.GovTrack.us. 2019. June 26, 2020 <<https://www.govtrack.us/congress/bills/116/hr827>>.

⁴⁸ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

⁴⁹ European Commission, 'The Directive on security of network and information systems (NIS Directive)' (www.ec.europa.eu, 15 April 2020) <<https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>> accessed 27 June 2020.

⁵⁰ Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [17 April 2019] OJ L 151/15.

⁵¹ European Commission, 'The EU Cybersecurity Act' (www.ec.europa.eu, 28 February 2020) <[https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act#:~:text=The%20EU%20Cybersecurity%20Act%20grants,more%20resources%20and%20new%20tasks.&text=This%20task%20builds%20on%20ENISA,information%20systems%20\(%20NIS%20Directive\).>](https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act#:~:text=The%20EU%20Cybersecurity%20Act%20grants,more%20resources%20and%20new%20tasks.&text=This%20task%20builds%20on%20ENISA,information%20systems%20(%20NIS%20Directive).>)> accessed 27 June 2020.

Despite the fact that none of the above listed legislative acts mentions AI or machine learning, they are technology-neutral in the way that their provisions are applicable to the development and usage of these technologies in order to ensure:

that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services.⁵²

However, the relationship between cybersecurity and AI or machine learning, respectively, is a topic that would deserve a dissertation rather than several paragraphs in this master thesis. And we are indeed not going to dive into that discussion. It is much more interesting to examine the relationship between AI and (personal) data protection in EU's legislative framework due to adoption of GDPR⁵³ which entered into force on 25 May 2018.

III.III.II Data Protection

GDPR sparked wave of debates about privacy protection in relation to AI and machine learning as these technologies require extensive amounts of data including data relating to individuals, i.e. personal data. This regulation also doesn't specifically refer to AI or machine learning, but it doesn't need to. It is not an industry-specific legislation. Instead, it applies to processing of personal data in general (subject to limitations in accordance with its relevant provisions).

Therefore, GDPR applies even to processing of personal data when using AI and machine learning technologies and it has to comply with its applicable provisions. Those include, for example, Art. 5(b) according to which „personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes“. This provision referred to as “purpose limitation” can often only hardly be adhered to since AI processes various data that were originally obtained for entirely different purposes.

Pursuant to Art. 5(c) „personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed“. This principle of “data minimization” is in particular of concern to developers, because it

⁵² Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1, Art. 16(1).

⁵³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

relates to the question of the scope of data that are really needed to be processed. And what about systems that evolve in time? Systems that will be programmed to decide on their own, whether they need further data or not?

Another provision significantly impacting processing of personal data using AI or machine learning is Art. 22 (para. 1) which prescribes that „data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her“. The previous does not apply, for instance, if the decision is necessary for contract conclusion or contract performance, or the decision is based on the data subject's explicit consent (para. 2).

“Automated decision-making” basically means making a decision without involving humans, while “profiling” should be understood as automated processing of data about an individual to evaluate certain specific aspects about that person. For example, in CRM, software may automatically decline application for credit loan, because, based on certain data input about the applicant, a profile was created, according to which there is a high probability of default. In this particular case, legal basis is provided based on the fact that the individual, by submitting the credit loan application, makes it clear, that he or she intends to enter into contract with the credit institution. But even so, in accordance with Art. 13 and 14, respectively, the data controller has to inform the data subject about:

the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

But what exactly is „meaningful information about the logic involved”? Does it involve setting of the algorithm employed, so that decision can be made automatically? Or even the input data, based on which the decision was made? And if Art. 22 applies only if automated processing „produces legal effects concerning him or her or similarly significantly affects him or her”, what is the content of these terms in specific situations?

All these questions will probably be clarified either by courts, data protection authorities or authoritative interpretations by academics and practitioners. Until then however, this uncertainty can have restrictive effect on AI development and application,

because breaches of these (and many other) articles of GDPR can be sanctioned with monetary fines „up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher”.⁵⁴

III.III.III Intellectual Property

So far little attention has been granted to the questions arising with respect to emergence of AI in the field of IP legislation. However, certain gaps can be found especially in copyright and patent law which will need to be addressed rather sooner than later.

The discussion could be split into two parts. One of them centers around the topic of copyrightability and patentability of AI per se, while the other one attempts to answer questions related to the issue of AI-generated works and inventions.

With respect to the question of whether an AI system should per se be protected by copyright, that depends on if it can be considered a software or not. If so, then according to WIPO, it is generally accepted that „computer programs should be protected by copyright, whereas apparatus using computer software or software-related inventions should be protected by patent”⁵⁵.

The matter of patentability of AI was subject to international conference held by EPO in May 2018 which resulted in extension of EPO’s documentation providing guidance on patentability criteria, so that it gives answers relating to patentability of AI and machine learning. EPO is of the opinion, that since AI and machine learning are based on computational models and algorithms, which are of an abstract mathematical nature, then, apart from exceptions, the guidance provided for mathematical methods should apply.⁵⁶

However, protecting works and inventions generated by AI is a much bigger challenge. Copyright law is based on the humanist approach and copyright offices throughout the world are reluctant to register works produced by machines or

⁵⁴ Ibid, Art. 83(5).

⁵⁵ World intellectual property organization, 'Copyright Protection of Computer Software' (www.wipo.int, unknown date of publication) <<https://www.wipo.int/copyright/en/activities/software.html>> accessed 30 June 2020.

⁵⁶ European Patent Office, 'Guidelines for Examination' (www.epo.org, 1 May 2018) <https://www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_3_1.htm> accessed 28 June 2020.

mechanical processes operating automatically without any creative feature contributed by human author.

There are copyright scholars advocating for AI-generated works to be placed in public domain, and there are others who propose to ensure at least a certain level of protection.⁵⁷

The truth is that intelligent systems already produce their own texts, paintings, music and films. And even though it is generally accepted, that AI can be used as a tool for creating a work subject to copyright protection, AI cannot be considered “author”.⁵⁸ Instead, nature and scope of human contribution must be assessed.

Appropriate example can be found in UK, where according to sec. 9 para. 3 of the Copyright, Designs and Patents Act 1988 „In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken”.

And what about inventions? Can AI be considered an inventor? We mentioned how patentability requirements are to be applied to development of AI as such, but how to apply them to inventions devised by AI? Can they even be considered inventions? And if so, who owns them?

Jurisdictions do not allow for AI systems to be considered as inventor under their patent law regimes. Determining an inventor, similarly as in case of searching for authors of works for the purpose of copyright protection, always entails identification of the person responsible for creative conception of the invention.⁵⁹

EPO seems to reject the idea of AI as an inventor claiming that:

it has been established that the broadening of the definition of inventor so as to include AI systems may be unwarranted and is likely to result in unnecessary deviation from the basic rationale underpinning the patent regime.⁶⁰

⁵⁷ Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H., Lopez Cobo M., Mertens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic L., Artificial Intelligence - A European Perspective (ISBN 978-92-79-97219-5, Publications Office of the European Union, Luxembourg, 2018) 66.

⁵⁸ Andres Guadamuz, 'Artificial intelligence and copyright' (www.wipo.int, 1 October 2017) <https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html#:~:text=Artificial%20intelligence%20is%20already%20being,used%20and%20reused%20by%20anyone.> accessed 24 July 2020.

⁵⁹ Noam Shemtov, 'A study on inventorship in inventions involving AI activity' (www.epo.org, 1 February 2019) 5 <[http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/\\$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf](http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf)> accessed 28 June 2020.

⁶⁰ Ibid, p. 6.

However, when questioned about potential extension of inventor status not being limited to natural persons EPO admits that:

Hypothesising that a change to our legal framework is to take place, within which changes to the patent regime will be introduced where AI systems will be considered as inventors, the study concludes that any indication of such inventorship may be done by reference to a legal personhood status and an accompanying system of registration that would be established for that purpose.⁶¹

The associated matter of ownership can therefore be divided into two possible scenarios. One of them is the current approach, according to which the right to European patent belongs to the person(s), whose contributions in the chain of creation played the role in the invention-making process.⁶² The second alternative pertains to the scenario when „ownership may rest with a newly created legal status for AI systems”.⁶³ The related issue of AI’s “legal personhood” forms the core part of this master thesis.

⁶¹ Ibid.

⁶² Ibid.

⁶³ Ibid.

IV. LEGAL PERSONALITY

The master thesis aims to examine the idea of granting certain highly developed types of AI the status of legal person, particularly so that it can have rights and obligations and be held accountable for breaching them. For that reason a short discourse into the part of theory of law which deals with the notion of legal personality follows.

IV.I Concept of legal existence/personality

One of the fundamental principles of legal systems is that it must recognize the subjects it seeks to govern. In another words, if the law wants to regulate conduct in society, it must first acknowledge existence of its members. This is done by the law recognizing distinct “legal persons”⁶⁴.

Legal existence (personality, subjectivity) refers to the capability to carry subjective rights and obligations.⁶⁵ Therefore, to legally exist is to be recognized by the law as a subject which is conferred rights, entitlements and imposed duties and liabilities.⁶⁶

It is the ability to take part in legal relationships as opposed to legal capacity which is one’s capability to amend its rights and obligations, for example, via entering into contracts, suing, marrying, etc.⁶⁷ Naturally, legal personality is a precondition for having legal capacity. Furthermore, legal personality is unlimited (but could be partial), while presence of legal capacity can be bound to many criteria such as age or mental fitness in the case of natural persons.

The term “person” itself is derived from Latin “persona”, which means a mask that theater actors wear in a drama. Later on it started to be used as referring to a living being capable of having rights and obligations. Today its content is much wider covering, for example, even private and public corporations and funds.⁶⁸

⁶⁴ In this sense meaning all the subjects of the law including natural persons.

⁶⁵ Aleš Gerloch, *Theory of Law* (6 edn, Vydavatelství a nakladatelství Aleš Čeněk 2013) 110.

⁶⁶ S. Padmavathi, D.G. Hari Prasath, *Supreme Court Judgement On Ayodhya Issue: Ram Janmabhoomi – Babri Masjid Land Title Dispute* (Notion Press 2020).

⁶⁷ It should be noted that certain scholars consider the term “legal capacity” as comprising both: the capability to have rights and obligations (here as “legal personality”) and the ability to act upon such rights and thereby amend legal relations which contain those rights and corresponding duties.

⁶⁸ Naresh kumar, 'Legal Personality, Legal Person in Jurisprudence' (www.lawnotes4u.in, 26 April 2019) <<https://www.lawnotes4u.in/2019/04/legal-personality-legal-person-in-jurisprudence.html>> accessed 29 June 2020.

IV.II Current legally recognized types of legal persons

Since “subjectivity” is a prerequisite for having rights and obligations, it is not limited to humans. It has been established ever since ancient Rome that groups of people (or certain amount of property in case of funds) can be recognized as separate legal entity distinct from its members.

These “subjects” comprise mainly individuals (natural persons) and legal (juridical, artificial) persons. Legal persons (entities) are private corporations as well as government agencies.

Individuals have legal personality from birth to their death. However, certain rights are granted even to “unborns”⁶⁹, i.e. children conceived in mother’s womb. They can inherit or a gift can be made in favor of them. Understandably, even after death the law protects the deceased; at least his or her body and reputation.

Legal personality of individuals exists given their nature per se, however, legal persons in the sense of entities, in accordance with the fiction theory, exist in the eyes of the law only because the law says so. Either the law directly establishes them, or provides conditions for their formation. They have legal personality by fiction, artificially.⁷⁰ Typically, they have it as of incorporation and lose it upon dissolution.

The approach as described above is characteristic for most civil law and common law jurisdictions based on Roman and Anglo-Saxon tradition but there are other legal systems such as customary or religious.

In India, idols in Hindu temples and even the rivers Ganga and Yamuna were given status of a legal person by the High Court:

(...) the Rivers Ganga and Yamuna, all their tributaries, streams, every natural water flowing with flow continuously or intermittently of these rivers, are declared as juristic/legal persons/living entities having the status of a legal person with all corresponding rights, duties and liabilities of a living person in order to preserve and conserve river Ganga and Yamuna.⁷¹

⁶⁹ So called “nasciturus fiction” means, that if foetus is later on born alive, it shall have all the rights of children which are already born whenever it is to its advantage.

⁷⁰ While realist opponents of the fiction theory consider subjectivity of legal entities something entirely natural as if it was a living organism with a body and will. And there are other theories explaining existence of corporations in the eyes of the law such as purpose or symbolist theory, however fiction theory currently prevails in most jurisdictions.

⁷¹ *Salim v. State of Uttarakhand* [2014] PIL 126, [2017] 126.

The court further explained its stance on the concept of a juristic person:

(...) like any other natural person is in law also conferred with rights and obligations and is dealt with in accordance with law. In other words, the entity acts like a natural person but only through a designated person, as their Lordships have held in the judgments cited hereinabove, that for a bigger thrust of socio-political-scientific development, evolution of a fictional personality to be a juristic person becomes inevitable. This may be any entity, living inanimate, objects or things. It may be a religious institution or any such useful unit which may impel the Courts to recognise it.⁷²

The decision was later overruled by the Supreme Court but another New Zealand river Whanganui was declared a living entity and appointed two guardians to protect its interests⁷³, while recognizing mosques⁷⁴ or a forest⁷⁵ as juristic persons is not unheard of.

IV.III Criteria for recognizing new types of legal persons

Criteria for recognition of new legal persons evolved significantly and it always depended on historic circumstances. The power of legal systems to recognize and hence deny legal personality has even been used to justify breaches of human rights including justifying slavery.⁷⁶

The example above shows, that not all humans were always considered persons in the legal sense. Today, the situation is opposite. No legal system or its jurisdiction distinguishes between humans who hold rights and obligations and humans who don't. Today's question is rather who (or rather what) else apart from humans should be considered a subject in the eyes of the law.

In the previous section, it was established that content of the term "legal person" has, especially in some jurisdictions, broadened significantly. In New Zealand, the status of a person was granted to the Te Urewera forest for „its intrinsic worth, its distinctive natural and cultural values, the integrity of those values, and for its national importance”⁷⁷.

⁷² Ibid.

⁷³ SwachhIndia, 'Ganga And Yamuna Are Not Living Entities, Rules Supreme Court' (www.swachhIndia.ndtv.com, 22 September 2017) <<https://swachhIndia.ndtv.com/ganga-and-yamuna-are-not-living-entities-rules-supreme-court-9716/>> accessed 29 June 2020.

⁷⁴ See Shankar Das v. Said Ahmad [1884] PR 153, [1914] 59 or Maula Bux v. Hafizuddin [1926] AIR 372, [1926] 372.6.

⁷⁵ Te Urewera Act 2014 (51) 11.

⁷⁶ S. Padmavathi, D.G. Hari Prasath, Supreme Court Judgement On Ayodhya Issue: Ram Janmabhoomi – Babri Masjid Land Title Dispute (Notion Press 2020).

⁷⁷ Te Urewera Act 2014 (51) 4.

On the one hand, the purpose of enactment of the Te Urewera Act was environmental protection, on the other hand, it served as proof of recognition of Maori cosmology by the government and was, at least in part, political.

A theory exists, according to which all rights have corresponding obligations, thus duties arising from legislation protecting the forest must correspond with rights of the forest. If we accept this theory, and at the same time the above mentioned definition that legal personality refers to the capability to carry subjective rights and obligations, then forest is a legal person.

That is, by the way, one of the arguments of those calling for granting legal personhood to non-human animals as they also have rights corresponding with our obligations pursuant to animal welfare laws.

Such approach would probably result in granting the status of legal person to almost everything, that is why the “will theory” limited its applicability. According to it, right-holding is only one criterion. The other one is control. Not just any control, but such control that can only be performed by rational beings with mental faculties that correspond to those of adult human beings.⁷⁸

Unfortunately, not even this theory provides a clear guidance on when the status of legal person should be granted. It’s logic even contradicts the principle according to which human being becomes legal person upon birth. Legal systems treat newly born children differently than fetuses even though they both carry rights and in spite of the fact, that newborns hardly perform higher degree of control than nasciturus.⁷⁹

No other conclusion can be found other than that, theoretically speaking, legal personality can be granted to absolutely anything. The only truly decisive criterion is purpose. If there is a purpose for conferment of legal personality, if there are rights and/or duties that such a being should be bestowed or imposed upon, then legal systems can expand the content of the term “legal personality” beyond natural persons, and grant it to rivers, buildings, trees, ships and they have done that for centuries.

Therefore, if a legal system intended to grant AI the status of distinct legal person having rights and obligations, the question would not be whether it can, but rather whether there is a reason to do it.

⁷⁸ Visa Aj Kurki, Tomasz Pietrzykowski, *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (Springer 2017) 81.

⁷⁹ Ibid.

V. LEGAL PERSONALITY OF ARTIFICIAL INTELLIGENCE

V.I *Recognition of AI in contemporary EU legislation*

In the previous parts, it was already established that there is no single generally accepted definition of AI. It is important to note here that a uniform legal definition does not exist either. And because content of the term is not clear, legal systems usually do not work with it explicitly. However, there are situations when legislation can be applied to a specific case involving AI because law often intentionally works with vague and indefinite expressions, so that such rules can be applied even to similar situations whose occurrence was originally not anticipated. Therefore, even though AI is only rarely mentioned expressly, it can fall under various legal regimes whose applicability will, for example, be crucial for ensuring, that there is a person to be held liable in case of AI playing a role in infliction of harm.

V.I.I AI as a computer software

Irrespective of whether AI-based systems are exclusively software-based such as search engines or chatbots, or they form an integral part of a physical device, they are a creation of its developer and they deserve copyright protection.

In accordance with the EU Computer Programs Directive⁸⁰ „Member States shall protect computer programs⁸¹, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works”⁸².

However, according to Recital 11:

(...) to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive. In accordance with the legislation and case-law of the Member States and the international copyright conventions, the expression of those ideas and principles is to be protected by copyright.

Recital 11 could be understood as exclusion of algorithms themselves from copyright protection in the EU. In order for them to be protected they need to be part of

⁸⁰ Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) [2009] OJ L 111.

⁸¹ According to Recital 7 „‘computer program’ includes programs in any form, including those which are incorporated into hardware”.

⁸² Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) [2009] OJ L 111, Art. 1(1).

a computer program as its “expression”, so that they can be “covered” by the protection of the program as a whole.⁸³

Unfortunately, content of the term “expression” is nowhere to be found within the Computer Programs Directive, but CJEU gave a certain guidance in 2009 when interpreting the same provisions of the previous Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs:

Directive 91/250 does not define the notion of ‘expression in any form of a computer program’ (...) notion must be defined having regard to the wording and context of Article 1(2) of Directive 91/250, where the reference to it is to be found and in the light of both the overall objectives of that directive and international law (see, by analogy, Case C-5/08 Infopaq International [2009] ECR I-6569, paragraph 32). (...) reference must be made to Article 10(1) of the TRIPS Agreement, which provides that computer programs, whether expressed in source code or in object code, will be protected as literary works pursuant to the Berne Convention (...) It follows that the source code and the object code of a computer program are forms of expression thereof which, consequently, are entitled to be protected by copyright as computer programs, by virtue of Article 1(2) of Directive 91/250 (...) Accordingly, the object of the protection conferred by that directive is the expression in any form of a computer program which permits reproduction in different computer languages (...) any form of expression of a computer program must be protected from the moment when its reproduction would engender the reproduction of the computer program itself, thus enabling the computer to perform its task.⁸⁴

Consequently, if an “expression” of a software is protected in case it enables the computer to realize its tasks (its functions), it can be claimed that current forms of AI fall under the term and therefore enjoy protection under EU Computer Programs Directive and its implementations within Member States.

V.I.II AI as a product

Implication of the fact that AI can be viewed as a computer software is that it can be copyright protected under the regime established by EU Computer Programs Directive.

However, for the purpose of this master thesis it is more important to address the issue of AI with respect to product safety and liability rules, as they give guidance on how current legal systems in EU Member States deal with situations when AI is involved in causing harm.

⁸³ „Protection in accordance with this Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive”. Ibid, Art 1(2).

⁸⁴ Case C-393/09 *Bezpečnostní Softwarová Asociace - Svaz Softwarové Ochrany v Ministerstvo Kultury* [2011] OJ C 63.

Common safety and liability rules are pillars of the internal market. Their objective is to ensure that all products and services, including those which integrate emerging digital technologies, operate safely, reliably and that damage having occurred is remedied efficiently.⁸⁵

Most below listed directives do not mention AI expressly, because they were enacted before technologies such as AI or IoT emerged. However, as the legal framework is technologically neutral, it does not mean that it would not apply to products incorporating these technologies.⁸⁶ The framework can be divided into areas of safety and liability.

EU product safety framework comprises especially General Product Safety Directive⁸⁷, which prescribes that all consumer products need to be safe. The directive complements sector-specific legislation such as Machinery Directive⁸⁸, Medical Devices Regulation⁸⁹, Radio Equipment Directive⁹⁰, Toy Safety Directive⁹¹ or relevant vehicle approval legislation⁹².

These above listed directives and regulations are generally applicable and do not provide for specific mandatory safety requirements for products containing AI technology. Typically, this could be of concern due to connectivity. The product may be “safe” in the classic physical sense but there is no protection against, for example, cyber-threats affecting safety of users.

⁸⁵ European Commission, Report from the Commission to the European Parliament, the Council and the European and Economic Social Committee - Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (Brussels, Cm 64, 2020), p. 1.

⁸⁶ Ibid, p. 4.

⁸⁷ Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2001] OJ 2 L 11.

⁸⁸ Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC [2006] OJ 2 L 157.

⁸⁹ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ 2 L 117.

⁹⁰ Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ 2 L 153.

⁹¹ Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] OJ 2 L 170.

⁹² Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ 2 L 151.

For that reason, in some of the later adopted directives and regulations⁹³ provisions governing security matters can be found setting up voluntary information security certification scheme for ICT products that would complement EU mandatory safety framework.

There is a common misconception, that safety legislation applies only when placing products on the market. However, EU product safety rules already set obligation of manufacturers to perform risk assessment taking into account the use of the products throughout their lifetime, i.e. they have to consider intended use of the product, the foreseeable use and the reasonably foreseeable misuse. Producers also have to provide appropriate instructions and safety information.⁹⁴

In the case of products enhanced with AI problems may occur with respect to their “autonomy”. In the future, such product “behavior” might not be entirely foreseeable due to its self-learning ability. In these cases a risk re-assessment must be performed by the manufacturer. Therefore, apart from the risk assessment performed prior to introducing a product to the market:

a new risk assessment procedure could be put in place where the product is subject to important changes during its lifetime, e.g. different product function, not foreseen by the manufacturer in the initial risk assessment. This should focus on the safety impact caused by the autonomous behaviour throughout the product lifetime.⁹⁵

In any case, the self-learning ability of AI can result in making decisions not originally anticipated by the manufacturer and consequently by the end user. That concerns the broader issue of human control or supervision, the question of how and whether humans should delegate decision-making to AI systems and products. The truth is that current EU product safety framework does not address the matter of human oversight specifically in relation to AI-based products.

Another challenge that EU legislator will have to cope with is, as EC admits in its White Paper of February 2020⁹⁶, that the primary focus of EU product safety framework is on placing products on the market. If software forms an integral part of the final

⁹³ The Cybersecurity Act, Radio Equipment Directive, Medical Devices Regulation.

⁹⁴ European Commission, Report from the Commission to the European Parliament, the Council and the European and Economic Social Committee - Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (Brussels, Cm 64, 2020), p. 6.

⁹⁵ Ibid, p. 7. These re-assessments are already required in transport industry; for example, in railway transport legislation, in case a vehicle is modified after its certification, special procedure is prescribed to follow, and it is defined in what cases the supervisory authority needs to be involved.

⁹⁶ European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust (Brussels, Cm 65, 2020), p. 14.

product it must adhere to the relevant product safety legislation. It is questionable, however, whether stand-alone software is covered by the safety framework, apart from certain sector-specific exceptions⁹⁷. It rather seems that currently applicable EU product safety framework does not cover services, and therefore not even services based on AI either (e.g. financial services).

EU product safety framework and product liability legislation are complementary regulatory mechanisms, whose common aim is functioning single market with goods that attempts to decrease risk of damage or injuries and, at the same time, if such harm occurs, ensure that compensation will be provided for damage caused by such defective products.

Liability framework in EU comprises Product Liability Directive⁹⁸ harmonising producer's strict liability for defective products⁹⁹, and other national fault-based and strict liability rules that are not harmonised.¹⁰⁰

The problem here is associated with the fault-based regimes, because some features of AI or IoT and similar technologies could make it very difficult or even virtually impossible to trace infliction of damage back to human behaviour and/or prove the necessary causal link. This could result in victims not being adequately compensated.

The matter raises the question of how to apply the concept of fault to damage harm by AI-based products. Also, as fault-based regimes are the domain of Member States, should they adopt necessary legislative changes? That could result in different legal regimes in different Member States; therefore, fragmentation of internal market and, subsequently, increasing costs of AI-enhanced product development and reduction of cross-border trade.

Another issue is associated with the assessment of defectiveness based on product safety legislation. If only a defective product can cause harm and the nexus between damage infliction and defect of the product has to be proven, then in case of AI-

⁹⁷ Software intended by the producer to be used for medical purposes is considered a medical device under the Medical Device Regulation (Regulation (EU) 2017/745).

⁹⁸ 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 [1985] OJ 2 L 210.

⁹⁹ Even here the question of distinguishing between products and services is present. This is especially difficult in the case of embedded and non-embedded software.

¹⁰⁰ Damage caused by an animal, abnormally dangerous operations, vicarious liability in employment, etc.

enhanced products it may be very complicated to determine if the damage was caused by the product itself or by other elements connected to it in the digital environment.¹⁰¹

V.I.III AI as a service

It was already mentioned, that it is unclear whether stand-alone AI software should be considered a product in the sense of EU product safety and liability regime. However, some will certainly be viewed as Information Society services as defined by EU Directive 2015/1535¹⁰², according to which a “service” is „any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”¹⁰³. Those are, for example, web search engines, social networks, e-shops, video-sharing service, etc. Other AI-based applications would probably fall under the regime prescribed by the Audiovisual Media Services Directive¹⁰⁴.

V.II *Machine learning vs. human intelligence*

In the previous sub-chapter, the paper briefly elaborated on how current EU legislation views AI or AI-based products and/or services, respectively. However, an opinion exists, that AI, at least its most developed form, could perhaps in the future be granted a special status of a distinct legal entity, which would, for instance, help solve the problem of identifying the party liable for harm caused by it. There are many arguments for and against introducing such solution, which will be discussed in the following sub-chapter. But it is no secret, that the main argument for it is the claim that the most advanced AI will resemble human beings so much, that it wouldn't make sense to treat them as things or products and services, but rather as autonomous entities similar to humans. That is the reason why information on status quo should be provided here, i.e. how current state-of-the-art AI and machine learning technologies differ from men at this very moment.

¹⁰¹ European Commission, Liability for emerging digital technologies accompanying the document 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018, Art. 4.1.

¹⁰² Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ 2 L 241.

¹⁰³ Ibid, Art. 1 para. 1(b).

¹⁰⁴ Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services [2010] OJ 2 L 95.

Throughout the paper, the terms AI and machine learning are used interchangeably, but it could be argued that AI, in fact, doesn't exist yet. Because the discussed technologies are better described as "machine learning", i.e. obtaining experience based on predefined algorithms. Machine learning, however, does not allow to reach true autonomy in the same sense as human intelligence. Instead, "real" AI *stricto sensu* would be a system capable of autonomous learning, "breaking free" from the control of producer or operator and having dreams, its own goals and emotions.

There is an important distinction between automatic (or automated) and autonomous. To demonstrate, we could use an example of a robot working in a factory. Automatic robot can perform routine activities and repeat a prescribed procedure all over again. Semi-autonomous robot is a higher form of such technology. Such robot has a higher extent of autonomy and can perform its tasks with certain amount of unpredictability, which is its producer's intention. This "semi-autonomy" consists in ability to analyse surrounding environment and "learn" from feedback received from particular situations. It is important to realize that the word "learning" used in this sense does not imply that:

these systems are artificially replicating the higher-order neural systems found in human learning. Rather, these algorithms improve their performance by examining more data and detecting additional patterns in that data that assist in making better automated decisions.¹⁰⁵

This "learning" can be referred to as "machine-learning", i.e. the ability to process received data and, for example, not make the same mistake in an analogous situation in the future. As already discussed at the beginning of the thesis, e.g., autonomous vehicles make use of this technology. They already have knowledge of traffic rules, but they also perceive objects in the surrounding space (direction and speed of other vehicles, other objects and pedestrians), predict their further movement, process the received data and "decide" how to proceed.

However, even the most advanced machine learning-based technology is not AI in the narrow sense. Such AI with capabilities that meet or surpass those of human cognition often referred to as "Strong AI"¹⁰⁶ is only aspirational. Strong AI has always

¹⁰⁵ Harry Surden, 'Artificial Intelligence and Law: An Overview' [2019] 35(4) Georgia State University Law Review 8.

¹⁰⁶ Terence Mills, 'AI Vs AGI: What's The Difference?' (www.forbes.com, 17 September 2018) <<https://www.forbes.com/sites/forbestechcouncil/2018/09/17/ai-vs-agi-whats-the-difference/#215462f738ee>> accessed 2 July 2020.

been a goal of researchers, but there is hardly any evidence suggesting that humanity is close to achieving such development in the near future.

Current AI systems cannot (and are not even designed to) be compared with human capabilities, such as abstract reasoning, general problem-solving skills and the wide spectrum of other abilities that are associated with human intelligence.¹⁰⁷ The truth is that human intelligence:

has no match in the biological and artificial worlds for sheer versatility, with the abilities to reason, achieve goals, understand and generate language, perceive and respond to sensory inputs, prove mathematical theorems, play challenging games, synthesize and summarize information, create art and music, and even write histories.¹⁰⁸

V.III AI as a distinct legal entity

Interpretation of the concept of AI was provided. It was established that the term “machine-learning” would probably better and more truthfully describe the related technologies at their current level of development. The thesis explained the term “legal entity” as well as presented the criteria for introducing a new type into a legal system. Let us follow up on that topic.

We came to the conclusion that, theoretically speaking, there are no obstacles to granting the status of legal person to virtually anything. If a jurisdiction decides to confer rights and impose duties on someone or something, it has decided to view that entity as if it was actually a person. It is a sort of pretence. It was also mentioned that we have witnessed recognition of corporations, funds, animals, and even forests and rivers as persons in the eyes of the law.

The scope of rights and obligations that define content of such legal personhood depends on the very nature of such an entity. Obviously, for example, limited liability companies have entirely different array of rights and duties than individuals, however, both should have the right to own property and to sue as well as the capacity to be sued.¹⁰⁹

¹⁰⁷ Jack Krupansky, 'Untangling the Definitions of Artificial Intelligence, Machine Intelligence, and Machine Learning' (www.perma.cc, 13 June 2017) <<https://perma.cc/RVZ4-88NP>> accessed 2 July 2020.

¹⁰⁸ Stanford university, 'Artificial Intelligence and Life in 2030' (One Hundred Year Study on Artificial Intelligence (AI100), 1 September 2016) 19 <<https://ai100.stanford.edu/>> accessed 21 June 2020, p.13.

¹⁰⁹ M. Petit, 'Towards a Critique of Algorithmic Reason A state-of-the-art review of artificial intelligence' [2018] XXI (44) Quaderns del Cac - Fake news, algorithms and filter bubbles.

Legal personality of humans is considered something natural. The law has developed over centuries and it followed the development of human mind. It was created while considering human capabilities, qualities, weaknesses, desires, etc.¹¹⁰ That is the reason why many argue against the idea of AI as a person due to the lack of elements which are present in case of men.

Their opponents are, however, equipped with other similarly valid arguments. They point to the fact that legal personhood has already been granted to many other entities, who are also not endowed with human-like elements.

Legal personhood of AI is really a political rather than a scientific topic. It is discussed at the highest levels of social organization and the first countries to start the debate were the most developed countries with the highest level of digitalization.¹¹¹ On the following pages, we will go through discussions that have been taking place within the framework of EU.

V.III.I EP resolution of 16 February 2017

The idea of AI as a person still sounds too sci-fi-like to many, however, it was expressed by Lawrence Solum already in 1992. Solum came to the conclusion that the question of whether AI should be granted legal personality cannot be answered unless humanity begins coming across AI on a daily basis.¹¹² Does that mean that time has come to make it happen?

In its famous resolution of 16 February 2017¹¹³ EP directly connected the concept of AI as a person to the issue of liability when noting that „at least at the present stage the responsibility must lie with a human and not a robot”¹¹⁴. However, at the same time it questions whether such current solution will be sufficient when AI reaches the level of complete autonomy and calls on EC:

whereas, ultimately, the autonomy of robots raises the question of their nature in the light of the existing legal categories or whether a new category should be created, with its own specific features and implications (...) when carrying out an impact assessment of its future legislative instrument, to explore, analyse and consider the implications of all

¹¹⁰ Roman Dremluiga, Pavel Kuznetsov & Alexey Mamychyev, 'Criteria for Recognition of AI as a Legal Person' [2019] 12(3) Journal of Politics and Law, 106.

¹¹¹ Ibid, p. 107.

¹¹² Lawrence B. Solum, 'Legal Personhood for Artificial Intelligences' [1992] 70(4) North Carolina Law Review 1231-1287.

¹¹³ European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

¹¹⁴ Ibid, para. 56.

possible legal solutions, such as: (...) creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently.¹¹⁵

This was a rather innocent and subtle idea buried deep in the document which, if read in context, would necessarily come out as a mere possibility and only one of the potential solutions, that EP presented and even the person behind this proposal, vice chair of the EP's Legal Affairs Committee, Mady Delvaux, publicly declared that her „primary goal when suggesting legal personhood for robots was to raise a public debate about the issue”¹¹⁶ and that „maybe at the end of the day, we'll come to the conclusion that it is not a good idea”¹¹⁷.

In fact, the resolution contains more questions than answers. In particular, it was not entirely clear whether such electronic person should be a subject resembling natural persons with all the accompanying rights including human rights or a concept similar to legal person in the sense of corporation would be introduced.

Additionally, the document only deals with granting the status of legal person in the sphere of private (civil) law, which indicates that AI could, under such circumstances, be an autonomous party to a commercial transaction with everything that encompasses it. However, the issue of whether such person could be guilty of offence or commit a crime is not addressed.¹¹⁸

The document, nonetheless, sparked waves of resentment, the debate goes on until today and will only intensify in the years to come. In that respect, the goal of Mady Delvaux was accomplished.

V.III.II Open Letter

EESC was one of the first to give their opinion on the matter when stating that:

EESC is opposed to any form of legal status for robots or AI (systems), as this entails an unacceptable risk of moral hazard. Liability law is based on a preventive, behaviour-correcting function, which may disappear as soon as the maker no longer bears the liability risk since this is transferred to the robot (or the AI system). There is also a risk of

¹¹⁵ Ibid, AC., para. 59 (f).

¹¹⁶ Janosch Delcker, 'Europe divided over robot 'personhood'' (www.politico.eu, 4 November 2018) <<https://www.politico.eu/article/europe-divided-over-robot-ai-artificial-intelligence-personhood/>> accessed 3 July 2020.

¹¹⁷ Ibid.

¹¹⁸ Nor is it expected to be found in Civil Law Rules on Robotics, however, both spheres should probably be discussed simultaneously.

inappropriate use and abuse of this kind of legal status. The comparison with the limited liability of companies is misplaced, because in that case a natural person is always ultimately responsible. In this regard, it should be examined to what extent the current national and EU laws, rules and jurisprudence in the area of (product and risk) liability and own risk provide an adequate answer to this question and, failing that, what kind of legal solutions can be put forward.¹¹⁹

Similarly, in September 2017, UNESCO's COMEST commented on EP's resolution:

it is highly counterintuitive to call them 'persons' as long as they do not possess some additional qualities typically associated with human persons, such as freedom of will, intentionality, self-consciousness, moral agency or a sense of personal identity.¹²⁰

But by far the most publicly known negative reaction to the EP's resolution is so-called Open Letter to the European Commission Artificial Intelligence and Robotics, which was sent to EC in April 2018¹²¹, which was, to date, signed by 285 AI and robotics experts, industry leaders, law, medical and ethics experts.

The main argument against introducing the "e-person" status is that the shift of liability for harm caused by AI from the producer onto the AI entity would result in situations when producers would market products whose safety they are not entirely sure about. Generally speaking, introduction of AI legal personality and, therefore, liability could enable natural persons and corporations to abuse AI as a liability "shield" against their own legal accountability as well as corporations were used for that in the past.

The authors refuse the argument that was already mentioned in the thesis, that it will be increasingly more difficult to determine who or what exactly the damage was caused by in cases where harm is inflicted in a situation where AI is involved. Instead, they claim that the idea of creating a legal status of an electronic person is „justified by the incorrect affirmation that damage liability would be impossible to prove”.¹²² Furthermore, it is insisted in the Open Letter that such perspective is based on:

¹¹⁹ European Economic and Social Committee, 'Opinion on Artificial intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (2017/C 288/01), Art. 3.33.

¹²⁰ United Nations Educational, Scientific, and Cultural Organization - World Commission on Ethics of Scientific Knowledge and Technology, 'Report of COMEST on Robotics Ethics' (2017/SHS/YES/COMEST-10/17/2 REV), Para. 201.

¹²¹ Accessible at <http://www.robotics-openletter.eu/>.

¹²² Ibid.

an overvaluation of the actual capabilities of even the most advanced robots, a superficial understanding of unpredictability and self-learning capacities and, a robot perception distorted by Science-Fiction and a few recent sensational press announcements.¹²³

The Open Letter provides a short analysis into why it is inappropriate to create such legal personality irrespective of what legal status model. With regard to the natural person model, the concept is refused due to the fact, that AI would then have human right, such as dignity, integrity, citizenship, etc., which would contradict requirements of the Charter of Fundamental Rights of the European Union and the Convention for the Protection of Human Rights and Fundamental Freedoms.¹²⁴

With respect to the legal entity (legal person) model, the idea is deemed unacceptable especially because of the fact, that it „implies the existence of human persons behind the legal person to represent and direct it”¹²⁵, which would not be the case here.

Interestingly, apart from the natural person and legal entity models the Open Letter explicitly rules out the possibility of deriving the legal status for AI from the Anglo-Saxon Trust model (Fiducie) due to its complexity and the fact that it wouldn't solve the issue of liability. But most importantly, „it would still imply the existence of a human being as a last resort - the trustee or fiduciary - responsible for managing the robot granted with a Trust or a Fiducie”.¹²⁶

It appears, that the arguments expressed in the Open Letter are valid and, in any case, first it should be assessed whether current liability framework is sufficient to cope with the challenges AI represents.

There was one more important argument which the Open Letter failed to mention. EU can establish its bodies and agencies, but does not have the power to determine who is a person in the eyes of the law of the Member States.¹²⁷ This power stays with the Member States and is only limited by obligations arising for the states from international human rights treaties.

¹²³ Ibid.

¹²⁴ Ibid.

¹²⁵ Ibid.

¹²⁶ Ibid.

¹²⁷ Thomas Burri , 'The EU is right to refuse legal personality for Artificial Intelligence' (www.euractiv.com, 31 May 2018) <<https://www.euractiv.com/section/digital/opinion/the-eu-is-right-to-refuse-legal-personality-for-artificial-intelligence/>> accessed 24 July 2020.

Only several weeks after EC had received the Open Letter, it published its Artificial Intelligence for Europe¹²⁸. The document, which was many times referred to in the previous parts of the thesis, outlined EC's future strategy to address AI. Importantly, EC implicitly refused the concept of electronic person by not mentioning it at all.

EC was probably right to not take up EP's idea of establishing legal personality for AI and due to the enormous dissent against such solution and EC's approach to it presented in Artificial Intelligence for Europe, it can be concluded that, for the time being, it is abandoned.

¹²⁸ European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018.

VI. LIABILITY

VI.I *Concept of liability*

Liability or legal responsibility (accountability) has (at least) two meanings. One of them refers to a situation when a person, whose existence is affirmed by the law, has a legal obligation. Liability then means the relation of this person to such a duty. The second interpretation speaks of liability only after such obligation is breached, i.e. as a negative consequence of such a breach.¹²⁹

Liability is based on a legal delict, which is an action not in compliance with either what the law prescribes directly, or what has been imposed in accordance with the law. Therefore, liability arises even when a contract is breached because, in these cases, the law is breached indirectly, as *pacta sunt servanda* (contracts must be adhered to) applies as a general legal principle. For the same reason liability arises even in cases when a binding decision of a judicial or administrative body is not complied with, because the law gave these agencies the power to issue binding decisions in the area of their responsibility.

Legal delict can consist in an active action (a person acted in a forbidden way) or an omission (someone did not act as they should have).¹³⁰ It can be a crime if such legal obligation is prescribed by criminal law. It can be a civil delict, for example, if a contract is breached or damage caused. It can be an administrative delict, an offence, or a disciplinary delict in case of breaching internal normative instructions within an organization.¹³¹

Liability is an essential feature of the society and its importance is closely associated with sanctions. It goes without saying that a crime shouldn't go unpunished. Damage to property should be compensated; contractual obligations should be fulfilled; administrative offence should be fined so that the offender is properly motivated not to commit it again, etc.

¹²⁹ Škop Martin, Macháč Petr, *Základy právní nauky* (1 edn, Wolters Kluwer ČR 2011), p. 163.

¹³⁰ *Ibid*, p. 164.

¹³¹ There are differences among legal systems and even jurisdictions in terms of delict designations. For example, the term “tort” is rarely used in civil law jurisdictions, while in certain countries the term “delict” or “delictum” is used exclusively for civil wrongs.

VI.II Types of liability

There are certain differences in terms of how legal systems and their jurisdictions view particular types of legal responsibility, but liability can certainly be classified according to the branch of the law (civil, criminal, etc.) in which the breach occurred. In addition, two large groups differ depending on whether imposition of liability requires fault (negligence or intent) or not (strict liability). In order not to deviate too far from the topic at hand we shall only briefly mention the basic characteristics of those types of liability whose application could be relevant for making sure that AI causing harm does not result in *denegatio justitiae* for the injured party.

In civil law, strict liability, also often known as absolute liability, is typically used in cases of defective products, dog bites, or abnormally dangerous activities. Apart from certain exceptional cases, it is not required to prove that the producer of a product (or dog owner, or performer of a dangerous activity) acted with bad intent or negligence. It is sufficient if the injured party shows that the product (dog or dangerous activity) caused relevant harm in order for the liability to arise and be imposed.

However, strict liability regime is used even in criminal or administrative law. For example, it is not required for drivers to “intend” to, or even “be aware” that they were driving above the speed limit in order for a police officer to be entitled to give a fine for speeding.

Vicarious liability refers to the type of legal accountability, where one party is held responsible for actions of somebody else. Typical example is the employer-employee relationship where employer is responsible for employee’s actions if those took place during working hours when the employee was performing his or her assigned tasks (“in the course of employment”). Another example is a parent held vicariously liable for actions committed by under-age children if harm is caused by such child’s behavior.

Joint and several liability then concerns a situation when two (or more) parties are collectively liable for causing damage to a third person. Each such party is as accountable as the other and they are liable for inflicting harm both collectively and individually. In practice, this means that the injured person can demand the entire claim from any of the collectively responsible parties and it is up to them to, subsequently, sort out their respective participation on causing the damage.

VII. LIABILITY FOR HARM CAUSED BY ARTIFICIAL INTELLIGENCE

VII.I Relevant debate so far

The issue of liability of AI is one of the most discussed legal challenges, that legislators currently face. Legal scholars and practitioners have been occupied with answering questions relating to accountability for harm caused by autonomous systems for years now.

They have been investigating preventive measures to be adopted by producers as well as users (operators). They have been attempting to liken AI's liability to the one of animals, children, and even employees or disabled persons. They considered applicability of strict liability concepts and they analyzed existing product liability regulatory framework.

Due to the increasing autonomy of intelligent systems as well as increasing use of ICT technologies, the opinion emerged that in cases when such systems begin acting not on behalf of somebody else but rather on their own and independently, substantial adaptation of legal framework will be required.

As was elaborated in the previous chapter, one particular approach proposed creation of a special legal personality status at least for those most developed autonomous systems, that would resemble human beings in terms of having similar capabilities, intelligence, and even emotions.

At least for the time being, the idea was de facto rejected. However, more realistic suggestions were put forth, for example, those concerning mandatory safety certifications or obligatory insurance schemes.

On the other hand, many are of the opinion that current legal systems are entirely sufficient and no significant legislative transformation is required because of the fact that many of these rules are technologically neutral, generally applicable, and content of legal terms that these laws and regulations work with can be extended simultaneously with technological advancement. They are convinced, that current regulatory framework provides sufficient legal basis for society's requirement to remedy harm caused by AI, to ensure that AI's development and operation are adequately safe as well as to guarantee that such rules do not hinder technological progress and innovations, because,

after all, their primary purpose is to make human lives safer, easier, and therefore more enjoyable.

VII.II EU efforts after rejection of e-personality

After EC had received the Open Letter, it in fact dismissed the concept of e-person and instead began to concentrate on „whether the safety and national and EU liability frameworks are fit for purpose in light of these new challenges or whether any gaps should be addressed”.¹³²

EC announced that assessments of Product Liability Directive¹³³ and Machinery Directive¹³⁴ have already been completed and stated that Machinery Directive evaluation had indicated that some of its provisions do not entirely anticipate certain elements of AI and other emerging technologies and that it will assess if amending it is required.¹³⁵

Concerning the Product Liability Directive EC points out its „all-encompassing definition of producer”¹³⁶, against whom a claim can be brought. Furthermore, it refers to CJEU who indicated that the directive applies even to products used in the course of providing a service, even though the service provider does not fall within the scope of the directive which also does not prevent Member States from applying further national rules pursuant to which service providers who use defective products while providing a service would be liable for damage caused.¹³⁷

¹³² European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018.

¹³³ 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 [1985] OJ 2 L 210.

¹³⁴ Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC [2006] OJ 2 L 157.

¹³⁵ European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018.

¹³⁶ A producer can mean the producer of a raw material, the manufacturer of a finished product or of a component part, the importer of the product, any person putting their name, trade mark or other distinguishing feature on the product or any person supplying a product whose producer or importer cannot be identified. Art. 3.

¹³⁷ European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', Commission Staff Working Document, Liability for emerging digital technologies, COM(2018)237, 25 April 2018, p. 6.

In 2018, however, EC did not give a clear “yes” or “no” on whether the directive provides sufficient framework for B2C relationships that it covers. Instead, it vowed to evaluate whether:

a regulatory intervention on these technologies appears appropriate and necessary (in terms of new rules or an amendment to existing rules), it should be discussed whether that intervention should be developed in a horizontal or sectorial way and whether new legislation should be enacted at EU level.¹³⁸

In the following year, EC published a new document named Liability for Artificial Intelligence and other emerging digital technologies written by the Expert Group on Liability and New Technologies - New Technologies Formation which was established by EC for that very purpose.

Authors in the paper follow up on the issue of Product Liability Directive’s applicability on AI and other emerging technologies, but at the same time acknowledge that producer’s strict liability for defective products represents only a small part of private law liability regimes under which injured parties would claim damages for harm caused by AI,¹³⁹ while other regimes are usually domain of the Member States.

The body, nonetheless, came to several general conclusions applicable for all liability regimes. For instance, it emphasized that even if operation of a technology, which poses an increased risk of causing harm, is permitted, such operator should be subject to strict liability. Moreover, in cases where a person ensuring necessary technology has a higher degree of control than the actual user of the AI-based product, that should be considered when determining who is subjected to liability.¹⁴⁰

However, when an AI-based technology which does not pose such an increased risk of harm to others is used, the operator should still have the obligation to properly select, operate and maintain the technology and - failing that - should be held liable for breach of such duties if at fault.¹⁴¹ Therefore, strict liability should be applied only in cases of technologies posing increased risk of causing harm to others or damage to property, and fault-based liability shall be applicable if the technology does not pose a higher risk even if AI-equipped.

¹³⁸ Ibid, p. 21.

¹³⁹ Expert Group on Liability and New Technologies - New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies (Publications Office of the European Union 2019), p. 3.

¹⁴⁰ Ibid.

¹⁴¹ Ibid.

Furthermore, manufacturers of products enhanced with such digital technologies should be liable for damage caused by their defective products, „even if the defect was caused by changes made to the product under the producer’s control after it had been placed on the market”.¹⁴²

Among other principles, two more are important to mention. Firstly, the document explicitly mentions the idea of mandatory insurance calling it “compulsory liability insurance”, which would on the one hand simplify access to remedy for victims, while at the same time protect the potential tortfeasor from the risk of being held liable for causing harm.¹⁴³

Secondly, EC in the paper for the first time explicitly admitted, that „it is not necessary to give devices or autonomous systems a legal personality, as the harm these may cause can and should be attributable to existing persons or bodies.”¹⁴⁴

VII.II.I High-Level Expert Group

EP already in 2017 came up with the proposal of establishing a European agency for AI and robotics which would, inter alia, perform supervision over development and utilization of AI within the framework of EU.¹⁴⁵ The idea was to form an agency which would perform various functions. Those would comprise, for example, administering a register of those AI-equipped technologies, which are the most technologically advanced, and therefore obligatory insurance scheme would have to be imposed on them.¹⁴⁶ Such identification would allow to avoid potential damage or injury. If one of these systems broke free from human control, all other systems of the same type could be identified and pulled away from the market so that they can be reprogrammed or destroyed.

Another task of such agency would be to establish and manage a compensation fund. The agency would be authorized to collect fees for such fund out of which compensation for injured parties would be realized. That would concern cases, when an AI developer with insurance obligation breached such duty and the developer’s AI-

¹⁴² Ibid, p. 3-4.

¹⁴³ Ibid, p. 4.

¹⁴⁴ Ibid.

¹⁴⁵ European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), para. 15-17.

¹⁴⁶ Peter Chapman, 'Regulating robots: a new reality? Civil Law Rules on Robotics' (www.cliffordchance.com, 16 July 2019) <<https://talkingtech.cliffordchance.com/en/emerging-technologies/internet-of-things/regulating-robots--a-new-reality-.html>> accessed 20 July 2020.

equipped system caused harm. The agency would, subsequently, claim the amount from the breaching party.¹⁴⁷

Ideally, the agency's personnel would include not only experts in the field of robotics and engineering, but also lawyers and philosophers, so that the body would be capable of proposing a set of ethical principles, that would then be required to be coded into AI systems.

It is clear from the EP's document that such principles should be based on the rules introduced by Isaac Asimov in its Runaround science-fiction story of 1942.¹⁴⁸ EP thereby emphasized the importance of human control over AI.

The agency was formed in June 2018 as the High-Level Expert Group¹⁴⁹ consisting of 52 experts. HLEG was formed with the aim to support EU's AI strategy including preparation of recommendations on „future policy development and on ethical, legal and social issues related to AI, including socio-economic challenges”.¹⁵⁰

In April 2019, HLEG presented its Ethics Guidelines for Trustworthy Artificial Intelligence.¹⁵¹ The document confirms EU's „human-centric” approach to AI, which pertains to the commitment to AI's use in the service to humanity and common good, with the aim to improve social welfare.

The Guidelines identify four ethical principles (respect for human autonomy, prevention of harm, fairness and explicability) and seven requirements which AI-enhanced technologies should meet in order for them to be considered trustworthy (human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity and non-discrimination, environmental and social well-being, and accountability).¹⁵²

¹⁴⁷ Robert Nešpůrek, 'Evropský parlament otevírá cestu regulaci umělé inteligence' (www.epravo.cz, 15 September 2017) <<https://www.epravo.cz/top/clanky/evropsky-parlament-otevira-cestu-unijni-regulaci-umele-intelligence-106387.html>> accessed 20 July 2020.

¹⁴⁸ „One, a robot may not injure a human being, or, through inaction, allow a human being to come to harm. Two, a robot must obey the orders given it by human beings except where such orders would conflict with the First Law. Three, a robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.”

¹⁴⁹ Not to be confused with EC's Expert Group on liability and new technologies.

¹⁵⁰ European Commission, 'High-Level Expert Group on Artificial Intelligence' (www.ec.europa.eu, 9 July 2020) <<https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>> accessed 20 July 2020.

¹⁵¹ High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) <<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>> accessed 20 July 2020.

¹⁵² Ibid.

Separate Chapter III is devoted to so-called „Trustworthy AI assessment list” (ALTAI), whose objective is to operationalize the above mentioned seven requirements. This section should be considered the most valuable as it contains actual operational tool for developers, who need to assess whether their AI system can be considered trustworthy and therefore marketable.

For example, in order to ascertain whether an AI system meets the requirement of human oversight, ALTAI lists questions to be answered within an organization:

Did you consider the appropriate level of human control for the particular AI system and use case?

Can you describe the level of human control or involvement?

Who is the “human in control” and what are the moments or tools for human intervention?

Did you put in place mechanisms and measures to ensure human control or oversight?

Did you take any measures to enable audit and to remedy issues related to governing AI autonomy?

Is there a self-learning or autonomous AI system or use case?

If so, did you put in place more specific mechanisms of control and oversight?

Which detection and response mechanisms did you establish to assess whether something could go wrong?

ALTAI was twice revised following piloting processes that involved feedback from organizations through online surveys, best practices sharing and series of in-depth interviews with selected industry players. The final version was published by HLEG on 17 July 2020.¹⁵³

The second most important document that HLEG introduced are Policy and investment recommendations for trustworthy Artificial Intelligence of June 2019¹⁵⁴. The main difference is that the recommendations are aimed at EU institutions and Member States rather than developers in the industry.

The paper follows up on the Guidelines and contains 33 policy and investment recommendations divided into four groups (humans and society at large, private sector, public sector, and Europe’s research and academia), that target the most pressing legal, ethical and technical issues with the aim of ensuring „Trustworthy AI”.¹⁵⁵

¹⁵³ High-Level Expert Group on AI, 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment' (www.ec.europa.eu, 17 July 2020) <<https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>> accessed 20 July 2020.

¹⁵⁴ High-Level Expert Group on AI, 'Policy and investment recommendations for trustworthy Artificial Intelligence' (www.ec.europa.eu, 26 June 2019) <<https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>> accessed 20 July 2020.

¹⁵⁵ Ibid.

VII.II.II Product Liability Directive of 1985

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 (the “Product Liability Directive”) was already mentioned several times within the thesis, but no final verdict on whether it is fit for today’s technologies was given.

In January 2020, EP’s Committee on Internal Market and Consumer Protection organized a public discussion named “Product Liability Directive: protecting consumers in the Digital Single Market”, where outcomes of “Liability for Artificial Intelligence and other emerging digital technologies” published in November 2019 by Expert Group on Liability and New Technologies were discussed. Participants shared their views on if the Directive needs to be adapted or whether its current state is sufficient due to its technology-neutrality.

At the meeting, various groups were represented including Professor Wendehorst participating on behalf of the University of Vienna, who pointed out many areas that are unclear and need to be adapted such as the question of the content of the term “product” itself, as it is nowhere explained whether it covers software that is not embedded in a tangible movable item. Apart from that, product certainly does not include services, therefore not even services which utilize AI technology. And even if software was included, the problem arises in case when it is provided “over-the-air” from a third country, which means that there is no importer against whom consumers can seek remedy.¹⁵⁶

Another interesting point she made was that in a complex networked environment it is often virtually impossible for the harmed consumer to prove existence of defect and that it caused the damage or injury. Therefore, alleviations from the burden of proof might be needed.¹⁵⁷

The participants agreed on several other areas where changes to the Directive and further discussion will be required. The definition of “producer” should be amended so that it comprises even those parties who perform update, upgrade or any form of

¹⁵⁶ Christiane Wendehorst, 'Product Liability Directive: protecting consumers in the Digital Single Market' (www.europarl.europa.eu, 22 January 2020) <<https://www.europarl.europa.eu/committees/en/product-liability-directive-protecting-c/product-details/20200107CHE06841>> accessed 21 July 2020.

¹⁵⁷ Ibid.

modification of the product. Additionally, it shall be assessed whether content of the term “damage” is needed to be expanded so that it includes damage to data and digital assets, or whether strict liability should apply with all jointly liable producers involved in the production.¹⁵⁸

VII.II.III Automated decision-making

On 12 February 2020, EP published “Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services”¹⁵⁹. While the document is aimed at ensuring that development and application of these technologies do not endanger EU’s high level of consumer protection, it also serves as an overview of EU’s previous activities with respect to AI. It explicitly mentions all the in this paper discussed resolutions, reports, communications, ethics guidelines, etc. published by EP, EC, HLEG and Expert Group on Liability and New Technologies.

Subsequently, the resolution lists all the many times discussed issues that accompany AI’s utilization: its rapid pace of development, its obvious contributions to the society and social welfare but, at the same time, doesn’t forget to point out that AI, for instance in the area of automated decision-making, poses certain threats for consumer trust and welfare.¹⁶⁰

Therefore, EP calls on EC to examine if current EU legal framework, including consumer law acquis and product safety legislation is needed to be checked to the extent whether it is able to respond to emergence of AI in relation but not limited to automated decision-making, while providing a high level of consumer protection in adherence to the Charter of Fundamental Rights of the EU.¹⁶¹

Specifically with regards to automated decision-making, EP urges EC to monitor the implementation of new rules under several new directives and regulations such as the Better Enforcement Directive¹⁶², which requires traders to inform consumers when

¹⁵⁸ Sylvie Gallage-Alwis, 'Updating The EU Product Liability Directive For The Digital Era' (www.signaturelitigation.com, 25 February 2020) <<https://www.signaturelitigation.com/updates/the-eu-product-liability-directive-for-the-digital-era-sylvie-gallage-alwis/>> accessed 21 July 2020.

¹⁵⁹ European Parliament, Resolution on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP), 12 February 2020.

¹⁶⁰ Ibid.

¹⁶¹ Ibid.

¹⁶² Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ 2 328/7.

prices of goods or services have been personalized on the basis of automated decision-making and profiling of customer behavior,¹⁶³ or the Geo-blocking Regulation¹⁶⁴, so that it is ensured that automated decision-making is not used to discriminate against consumers based on their nationality, residence or temporary location.¹⁶⁵

Furthermore, EP calls on EC to bring forward proposals to adapt EU's safety rules including the already mentioned Machinery Directive, Toy Safety Directive or General Product Safety Directive and especially the Product Liability Directive, which, for over 30 years, may have „provided a valuable safety net to protect consumers from harm caused by defective products”, but nevertheless needs to be reviewed with focus on the concepts of “product”, “defect”, “damage” and burden of proof.¹⁶⁶

VII.II.IV White Paper

On 19 February 2020, EC introduced its White Paper on AI - A European approach to excellence and trust¹⁶⁷ as a document following up on the many times mentioned European strategy for AI of April 2018, Liability for Artificial Intelligence and other emerging digital technologies written by the Expert Group on Liability and New Technologies in 2019, and the two works of HLEG.

The paper follows the tradition of providing a discourse into what has already been discussed and proposed with respect to development and use of AI in EU. It mentions the “twin objective” of promoting utilization of AI as well as addressing risks associated with it. The declared purpose of the paper is to „set out policy options on how to achieve these objectives”.¹⁶⁸

EC continues the discussion concerning liability regime by repeating all the risks arising from use of AI in case appropriate rule framework is not in place. The implications of AI, IoT and other digital technologies for safety and liability legislation are analyzed in the Commission Report accompanying the White Paper. It especially

¹⁶³ Ibid, recital 45.

¹⁶⁴ Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC [2018] OJ 2 60/1.

¹⁶⁵ European Parliament, Resolution on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP), 12 February 2020.

¹⁶⁶ Ibid.

¹⁶⁷ European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust (Brussels, Cm 65, 2020).

¹⁶⁸ Ibid, p. 1.

emphasizes the problem associated with difficulties pertaining to the fact, that those who suffered harm may not have access to evidence that is necessary to build a case in court (the burden of proof issue).¹⁶⁹ Apart from that, hardly any novelty can be found in the White Paper's provisions apart from EC's view on the concept of high-risk AI.

EC in general proposes a risk-based approach. That means that future regulation will usually function in the way that the developers will themselves assess whether their AI poses high-risk to the society or not.¹⁷⁰ Obviously different (differently burdening) regulatory requirements will then apply.

EC is of the opinion that relevant AI should be treated as high-risk „in light of what is at stake”, particularly in terms of safety and other consumer rights. The technology shall be considered high risk if two cumulative criteria are met. Firstly, depending on in which sector the relevant AI-enhanced technology is in use. The “high-risk sectors” should be exhaustively listed in the new regulatory framework. Examples are given mentioning healthcare, transport or energy. In addition, AI utilized in one of the mentioned sectors should only be considered high-risk provided that it is used „in such a manner that significant risks are likely to arise (injury, death, significant material damage)”.¹⁷¹

Chapter 5 of the White Paper is devoted to the issue of the regulatory framework more generally. Most of its content has already been discussed throughout the thesis apart from one pressing issue, which will be further elaborated in the subsequent sub-chapter. EC acknowledges that Member States are pointing at missing common EU framework. Even despite apparent efforts of EU, concrete tangible steps including amendment of relevant legislation (especially the necessary changes to the Product Liability Directive) are missing. Consequently, Member States began to take initiative of their own. German Data Ethics Commission has called for a five-level risk-based system of regulation that would range from no regulation at all to the complete ban for the most unpredictable and dangerous AI systems. Malta introduced a voluntary certification system for AI while Denmark launched its Data Ethics Seal prototype program.¹⁷²

¹⁶⁹ Ibid, p. 15.

¹⁷⁰ Ibid, p. 17.

¹⁷¹ Ibid.

¹⁷² Ibid, p. 10.

While such efforts on the Member States level are understandable, the approach has to be uniform in order to avoid internal market fragmentation, as different Member State frameworks form barriers for businesses who want to operate their AI technology within the single market.

VII.III Non-Harmonized Areas - Example of the Czech Republic

It was already indicated that the area of product liability represents only a small portion of liability regimes potentially applicable to harm caused while using AI-enhanced technologies (harm caused by a product in the sense of Product Liability Directive is not the only situation when AI may cause harm). Most of these are not harmonized and remain in the hands of Member States' legislators. There are several types of regimes that might be applicable to AI, even though not originally intended to. As an example, on the following pages Czech civil law liability regimes hypothetically applicable to situations when use of AI technology results in damage or injury are described.

VII.III.I Damage caused by an animal

When deciding which out of the existing liability regimes could be applicable to AI, one of the first that comes on mind is liability for injury or material damage caused by an animal. According to the Act no. 89/2012 Coll., Civil Code:

Section 2933

Where damage is caused by an animal, its owner is to provide compensation for the damage, whether or not the animal was under his supervision or under the supervision of a person to whom the owner entrusted the animal, or whether or not the animal strayed or escaped. A person to whom an animal has been entrusted or who keeps or otherwise uses the animal shall provide compensation for the damage caused by the animal jointly and severally with the owner.

Animals as well as AI-enhanced robots have certain physical strength, therefore they are certainly capable of causing harm. Furthermore, their actions can be to certain extent unpredictable and they can get into a situation when they are not supervised by a human. Despite these similarities, analogical application of the provision above does not seem to be ideal.

Algorithm-based actions of AI are comparable to human behavior rather than animal instincts and drives.¹⁷³ Importantly, these actions are programmed by a person different from the owner (end-user). However, if the provision above was applied to a situation when AI actions resulted in causing damage or injury, liability would be imposed on the owner of the device using AI technology and that owner would not be able to claim remedy from the manufacturer. Producers (or AI programmers) would then be able to avoid liability entirely.

Taking into account the above, it is safe to say that liability regime used for remedying damage caused by animals is not suitable for dealing with situations when material or immaterial harm is caused by AI. Moreover, it is virtually impossible to imagine applying it to situations when relevant AI operates only in cyber-space without any representation in physical world.

VII.III.II Damage caused by a person unable to assess the consequences of his acts

If we established that AI can only hardly be compared to an animal because, as opposed to animals, AI is to various extent capable of imitating human behavior, it could be examined whether provisions on damage caused by a person unable to assess the consequences of his acts can be applied instead:

Section 2920

A minor who has not yet acquired full legal capacity or a person who suffers from a mental disorder shall provide compensation for the damage caused if he was capable of controlling his behavior and assessing its consequences;

(...)

Section 2921

The person who has neglected to exercise proper supervision over a tortfeasor shall compensate the damage jointly and severally with the tortfeasor. If the tortfeasor does not have the duty to provide compensation for damage, the victim is compensated by the person who neglected to exercise supervision over the tortfeasor.

Classic example is obligation of minors to remedy caused damage (provided statutory conditions are met) together (jointly and severally) with the person who has neglected to exercise proper supervision (typically a parent).

¹⁷³ Čerka Paulius, Grigienė Jurgita & Sirbikytė Gintarė, 'Liability for damages caused by artificial intelligence' [2015] 31 Computer Law & Security Review, p. 386.

Users (operators) of AI would, similarly to parenting, supervise whether AI behaves appropriately. Advantage of this approach is that, at least to certain extent, it reflects the fact that AI undergoes certain stages of development. Even a child will grow up once and, as of that moment, it would not be just to further burden parents with threat of accountability. Even AI could, eventually, “grow up” to the state when such “parenting” would no longer be required.

However, due to the fact that AI does not have legal personality, it could not be held liable even if it was „capable of controlling (its) behavior and assessing its consequences”. That means that the liability would be solely imposed on the user (operator). In case of children, this is entirely understandable, as parents are themselves the children’s “manufacturers” of sorts, but applied to AI, the same problem arises as in case of applying liability for harm caused by animal regime - there is no way for the user to claim redress from the producer, i.e. the entity who is usually actually responsible.

VII.III.III Damage caused by a particularly hazardous operation

Pursuant to Section 2925 of the Czech Civil Code:

(1) A person who operates an enterprise or another facility which is particularly hazardous shall compensate the damage caused by the source of the increased danger; an operation is particularly hazardous if the possibility of serious damage cannot be reasonably excluded in advance even by exercising due care. Otherwise, the person is released from the duty if he proves that the damage was externally caused by force majeure or that it was caused by the very acts of the victim or unavoidable acts of a third person; if other grounds for the release from the duty have been stipulated, they are disregarded.

Although AI in its current stages of development should be characterized as algorithmic machine-learning rather than autonomous entity, due to its capability to analyze collected data and act accordingly which means to certain extent unpredictably, its nature can certainly be considered dangerous.

In many jurisdictions, applicability of similar legislation requires that the relevant activity (operation) “is not of common usage”, therefore the more ordinary use of such AI technology, the less likely it is to be determined to be an abnormally dangerous activity.¹⁷⁴ The Czech provision, however, does not provide such condition for its applicability and it could therefore be considered in cases when harm is caused by or

¹⁷⁴ Hubbard F. Patrick, 'Sophisticated Robots: Balancing Liability, Regulation, and Innovation' [2014] 9, University of South Carolina - Faculty Publications, p. 1865.

while using AI.

The question is who is “a person who operates” AI. Generally, operator is the person, who is legally and physically capable of using a thing, therefore in this case an AI-enhanced physical device or mere software. It is understandable that such person should be held liable in case the device causes harm.

But in a situation when such operator is, for example, a consumer who purchased an AI-equipped kitchen robot, this person operates the device while following all the instructions for safe use, and the device still causes harm due to its “autonomous” nature, imposition of liability onto the consumer himself is unacceptable.

Therefore, not even this liability regime is universally applicable to fairly deal with situations when AI plays a role within a harmful event. Specifically to the case at hand, no regime other than the traditional scheme of manufacturer’s liability for faulty goods (product liability) should be applied.

VII.III.IV Damage caused by a thing

Another possibility is application of provisions on damage caused by a thing due to Civil Code’s broad definition of things according to which „a thing in a legal sense (hereinafter a “thing”) is everything that is different from a person and serves the needs of people (...)”.¹⁷⁵

Pursuant to Section 2936:

The person who is obliged to provide a performance to someone and, in doing so, uses a defective thing shall provide compensation for the damage caused by the defect of the thing. This also applies in the case of the provision of health care, social, veterinary and other biological services.

In addition, in accordance with Section 2937:

(1) If a thing causes damage by itself, the person who should have had supervision over the thing shall pay compensation for the damage; if such a person cannot be otherwise determined, the owner of the thing is conclusively presumed to be such a person. A person who proves not to have neglected due supervision is released from the duty to provide compensation.

The first provision refers mainly to situations when a contracting party uses a defective thing to fulfil its contractual obligation, while Section 2937 is an important example of strict liability of supervisor or owner. Under this regime, producer’s liability is excluded. Unfortunately, manufacturers often disclaim liability which is then shifted

¹⁷⁵ Civil Code, Section 489.

to the buyer. In fact, Tesla, Inc. successfully used this argumentation in 2016 after the very first fatal crash of its famous Model S and has repeatedly warned its customers that the autopilot technology is not yet sophisticated enough for the driver to entirely ignore what is going on on the road.¹⁷⁶

The above mentioned provision is applied in cases when „a thing causes damage by itself”. If something happens “by itself”, it originates in the nature of the very thing without any external stimulus.¹⁷⁷ As a result, a harmful event occurs, even if the thing is not flawed.

This regime is indeed typically applicable in case of semi-autonomous vehicles. Liability lies with the owner, but if a defect was subsequently discovered the owner should be entitled to claim remedy from the producer in accordance with product liability rules.

The requirement of supervision is understandable and legitimate when it comes to semi-autonomous technologies. The easiest defense of producers of current semi-autonomous vehicles is to insist, that the driver is at all times obligated to monitor the traffic and interfere in case it is clear that the AI cannot be relied upon.¹⁷⁸ Such condition is however unacceptable in case of fully autonomous technologies including vehicles. Firstly, such technologies are developed in the way that all the elements of driving will be handled autonomously without any human interference. Any form of supervision is denied. Consequently, such vehicles won't even have pedals or steering wheel, which will effectively deny the driver to interfere, even if he/she wanted. Understandably, any form of liability on the side of the driver is unthinkable in these cases.

Due to unpredictability of highly autonomous systems, it would not be possible to prove that owner or supervisor neglected its duty of supervision. Therefore, they could not be held liable which would result into the situation similar to when applying the above described liability regimes, when the injured party would not have anyone to claim damages from, which is sometimes referred to as “liability gap”.

¹⁷⁶ Sky News, 'Tesla Driver In First Self-Drive Fatal Crash' (www.news.sky.com, 1 July 2016) <<https://news.sky.com/story/tesla-driver-in-first-self-drive-fatal-crash-10330121>> accessed 23 July 2020.

¹⁷⁷ Milan Hulmák and Petr Bezouška, *Občanský zákoník VI Závazkové právo Zvláštní část (§ 2055-3014) Komentář* (1 edn, Nakladatelství C H Beck 2014) 1640-1641.

¹⁷⁸ Linda Kolaříková, 'Odpovědnost (za) robota aneb právo umělé inteligence' ([Http://www.bulletin-advokacie.cz](http://www.bulletin-advokacie.cz), 18 April 2018) <<http://www.bulletin-advokacie.cz/odpovednost-za-robota-aneb-pravo-umele-inteligence>> accessed 23 July 2020.

And again, the only solution seems to be to apply the product liability regime. However, as many times emphasized, it could be very complicated for the harmed person to prove that the product had a defect and that defect resulted in (causal nexus) the harm sustained.

VII.III.V Vicarious liability

In ancient Rome, pater familias was solely liable for delicts committed by his dependents including slaves.¹⁷⁹ The logic behind the scheme is that, according to Roman legal system, slave was an object, a thing, rather than a subject of the law. Accordingly, he could not be held liable as he did not exist (in the eyes of the law). Full subjectivity (personality) belonged only to the head of the family. Consequently, if a slave inflicted injury or caused damage, accountability belonged to the owner as well as if any other thing in pater familia's disposal caused harm.¹⁸⁰

Similarity between an early Roman slave and current AI-enhanced technologies is apparent. They are both treated as a thing by the law, while both being to certain extent autonomous and capable of causing damage or injury. The underlying concept known as respondeat superior principle, however, did not disappear from legal systems. In the Czech law, for example, its manifestation can be found in the following provisions of the Civil Code:

Section 1935

If a debtor performs through another person, the debtor is liable in the same way as if he performed himself.

Section 2914

A person who, in his activities, uses an agent, employee or another helper shall provide compensation for the damage caused by such a person as if he caused it himself. (...)

This form of accountability, mainly in common law systems known as vicarious liability, is used, for instance, in employer-employee relationships, where employer is liable for damage caused by employees to a third party provided that the harmful act took place in the course of employment.

And as AI, i.e. some sort of a mechanical “slave” is on track to supersede employees in the same way like employees replaced slaves in the past, the “employer”

¹⁷⁹ Jaromír Kincl and others, *Římské právo* (1 edn, CH Beck 1995), p. 221.

¹⁸⁰ Leon E. Wein, 'The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence' [1992] 6 (Fall) *Harvard Journal of Law & Technology*, p. 110.

(not necessarily *stricto sensu*) of a computerized system may once again be held liable for injury caused by his property in the same way that he used to be in Rome if the damage had been caused by a human slave.¹⁸¹

¹⁸¹ Ibid, p. 111.

VIII. CONCLUSION

The thesis attempted to elaborate on the matter of legal aspects associated with development and utilization of AI. After general introductory part presenting basic concepts and wider socio-economic implications of emerging technologies, the crucial topics of AI's potential recognition as separate legal entity and closely associated issue of liability for harm caused by it followed. Even despite many initiatives and already existing rules of different nature in various jurisdictions of the world, the paper focused on the relevant discussion within EU.

Although various attempts to launch broader discussion and enact legislative amendments were made long before that, only after the famous proposal by the team of Mady Delvaux in 2017 to, going forward, consider granting the most sophisticated kind of AI status of distinct legal person kick-started what today is EU's hot topic number one when it comes to technology and innovation.

The revolutionary idea of "promoting" AI to the level of individuals and legal persons brought more questions than answers and due to its strong opposition can only hardly be materialized in the years to come. The truth is that Mrs. Delvaux was grossly misunderstood and misinterpreted. It was merely a suggestion, a topic for discussion and it only concerned the most developed kinds of AI, which have not even been yet designed, let alone in 2017.

Its rejection by experts as well as general public, no matter to what extent influenced by Asimov's Frankenstein complex and certain Hollywood films, is indeed supported by list of strong and valid arguments. For me, the most important reason for not granting AI the status of e-person is the one not mentioned in the text above but perhaps the most pragmatic and practical. The idea, if realized, would have far-reaching consequences for many areas of the law, but it pertains only to the most advanced AI, which means that for the rest the question of according to which existing liability regime its actions are to be considered still needs to be answered. Having one type of AI legally responsible while the rest not would only add one more regime, which would complicate things even further.

And the society would impose on itself all these complications only because of a prediction according to which certain type of AI might in the future resemble human

beings. But would we really want to realize that? The idea's supporters have several relatively relevant arguments of their own, but it's all a little like crystal-gazing.

My suggestion would be to focus on the present issues rather than speculate about future AI advancement. History showed us that nature and speed of technological progress are highly unpredictable. Although we may be able to reasonably predict advancements of the nearest future, we are not capable of reliably predicting technology's direction for much more than the next several years.

In any case, EU decided to, at least for the time being, reject the idea of AI's legal existence entirely and instead focus on adapting the existing liability framework so that it is ready for the challenges that AI poses. Understandably, EC plays the most important role and most of its initiatives were mentioned within the master thesis. It is not, however, the simplest of tasks and so far not many tangible results can be found. The most important one, i.e. adaptation of the Product Liability Directive and subsequent implementation in the Member States is far from accomplished and there will still be a great deal more discussion before the actual legislative revision takes place.

Nonetheless, due to the fact that product liability represents only a small portion of regimes applicable to situations when AI directly or indirectly caused damage or injury, it is also up to the Member States to assess whether their national non-harmonized liability frameworks are ready for the challenge of emerging technologies including AI.

As an example, I attempted to identify Czech civil law provisions potentially applicable to situations when liability arises in connection with operation of AI. While it would be exaggerated to claim that current legal system in the Czech Republic would not be able to ensure just remedies at all, as these regimes were not enacted with the intention to be applied to such situations, they are only partially fit to cope with the issues at hand.

With further advancement and "autonomisation" existing regimes will become even more insufficient, and therefore unjust either for the injured party or for the person to be held liable in accordance with the current rules.

Moreover, insufficient legal framework could discourage potential buyers from purchasing these technologies, which would result in unwanted economic consequences and deceleration of innovations.

In order to avoid fragmentation of internal market, EU's efforts to adapt the harmonized product liability framework so that it extends its applicability to situations currently regulated by national regimes seems to be the best solution. The new order should be primarily based on strict liability concept, and legal accountability of owner, operator or supervisor should, apart from specific situations where it is legitimate, disappear entirely, so that the legal responsibility is carried by those most profiting from AI's use, i.e. the manufacturers. Due to diverse nature and level of autonomy of AI technologies, the framework will have to be complemented by additional mandatory safeguards for technologies posing higher risk to life or property, such as obligatory safety certification or insurance schemes.

ABSTRACT

The law is often behind innovation, as it usually merely reacts to it, rather than defines regulatory framework within which technological progress would take place. It is difficult to avoid, therefore, to some extent, legitimate. Furthermore, considering the fact that new technologies are typically introduced as means to create value for humanity, restrictions might not even be desirable.

On the other hand, not having clear, applicable and enforceable rules governing issues such as development and operation of autonomous weapons or automatic generating of medical diagnoses could, eventually, prove to be a tragic mistake.

The master thesis attempts to answer a number of questions associated with the matter briefly outlined above, and, as the title hints, focuses on artificial intelligence (AI).

After short introductory part the reader is provided with explanation of basic terms that will be used in the main sections of the work, examples of industries already heavily impacted by AI as well as description of challenges that AI represents for various realms of society.

The following chapters examine the question of whether AI is worthy of existence in the eyes of the law, i.e. if it should be endowed with rights and subject to obligations as legally recognized entity similar to corporations and individuals.

Irrespective of how the previous is answered, the crucial topic of liability follows in the next chapter. The vision of AI behaving in manners deviating from designers' expectations remains to be the most frightening, and serves as the ultimate trigger for all the discussions and regulatory efforts, that the thesis aims to explore, assess and propose.

In order to have a structured, transparent and sensible approach, and despite existence of large amounts of rules of different nature, legal force and jurisdictions throughout the world, the thesis focuses on the relevant debate within the framework of the European Union.

Used methodology entails especially review of relevant literature and existing legislation and analysis of regulatory efforts with emphasis on the activity of the European Commission and the European Parliament. Comparative approach is seldom used to emphasize different approaches to regulation.

ZUSAMMENFASSUNG

Das Gesetz steht oft hinter der Innovation, da es in der Regel lediglich auf sie reagiert, anstatt einen regulatorischen Rahmen zu definieren, innerhalb dessen sich der technologische Fortschritt vollziehen würde. Es ist schwer zu vermeiden, und daher in gewissem Maße legitim. Angesichts der Tatsache, dass neue Technologien in der Regel als Mittel zur Wertschaffung für die Menschheit eingeführt werden, dürfen Beschränkungen nicht einmal wünschenswert sein.

Andererseits könnte sich das Fehlen klarer, anwendbarer und durchsetzbarer Regeln für Fragen wie die Entwicklung und der Betrieb autonomer Waffen oder eine automatische Erstellung medizinischer Diagnosen letztlich als tragischer Fehler erweisen.

Die Masterarbeit versucht, eine Reihe von Fragen im Zusammenhang mit dem oben kurz skizzierten Thema zu beantworten, und konzentriert sich, wie der Titel andeutet, auf die künstliche Intelligenz (KI).

Nach einem kurzen Einführungsteil werden die Grundbegriffe erläutert, die in den Hauptabschnitten der Arbeit verwendet werden, Beispiele für Branchen, die bereits stark von KI betroffen sind, sowie eine Beschreibung der Herausforderungen, die KI für verschiedene Bereiche der Gesellschaft darstellt, werden angegeben.

In den folgenden Kapiteln wird der Frage nachgegangen, ob die KI im Rechtssinne existenzwürdig ist, d. h. ob sie als rechtlich anerkannte Einheit ähnlich wie Kapitalgesellschaften und natürliche Personen mit Rechten und Pflichten ausgestattet werden sollte.

Unabhängig davon, wie die vorstehende Frage beantwortet wird, folgt im nächsten Kapitel das entscheidende Thema der Haftung. Die Vision einer KI, die sich auf eine Art und Weise verhält, die von den Erwartungen der Schaffer abweicht, ist nach wie vor am erschreckendsten und dient als ultimativer Auslöser für alle Diskussionen und Regulierungsversuche, die diese Arbeit zu erforschen, zu bewerten und vorzuschlagen versucht.

Um einen strukturierten, transparenten und vernünftigen Ansatz zu haben, und trotz der Existenz einer großen Anzahl von Regeln unterschiedlicher Art, Rechtskraft und Rechtsprechung in der ganzen Welt, konzentriert sich diese Arbeit auf die einschlägige Debatte im Rahmen der Europäischen Union.

Die angewandte Methodik beinhaltet insbesondere die Durchsicht der einschlägigen Literatur und der bestehenden Gesetzgebung sowie die Analyse der Regulierungsversuche mit Schwerpunkt auf Tätigkeit der Europäischen Kommission und des Europäischen Parlaments. Der komparative Ansatz wird nur selten verwendet, um unterschiedliche Regulierungsansätze hervorzuheben.

BIBLIOGRAPHY

Legislation

Directive (EU) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1

Regulation (EU) of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [17 April 2019] OJ L 151/15

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2018] OJ L 119/1

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety [2001] OJ 2 L 11

Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC [2006] OJ 2 L 157

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ 2 L 117

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ 2 L 153

Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] OJ 2 L 170

Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ 2 L 151

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 [1985] OJ 2 L 210

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ 2 L 241

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services [2010] OJ 2 L 95

Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ 2 328/7

Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC [2018] OJ 2 60/1

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) [2009] OJ L 111

Act concerning autonomous vehicles, and supplementing chapter 3 of Title 39 of the Revised Statutes Bill 2016 (NJ), S343

Vienna Convention on Road Traffic of 1968 (adopted 8 November 1968, entered into force 21 May 1977)

Copyright, Designs and Patents Act 1988

Civil Code 2012

Te Urewera Act 2014 (51)

Cases

Salim v. State of Uttarakhand [2014] PIL 126, [2017] 126

Shankar Das v. Said Ahmad [1884] PR 153, [1914] 59

Maula Bux v. Hafizuddin [1926] AIR 372, [1926] 372.6

Case C-5/08 Infopaq International v. DanskeDagblades Forening [2009] OJ C 220

Case C-393/09 Bezpečnostní Softwarová Asociace - Svaz Softwarové Ochrany v Ministerstvo Kultury [2011] OJ C 63

Books

Aleš Gerloch, Theory of Law (6 edn, Vydavatelství a nakladatelství Aleš Čeněk 2013)

Škop Martin, Macháč Petr, Základy právní nauky (1 edn, Wolters Kluwer ČR 2011)

Isaac Asimov, Runaround (Street & Smith 1942)

Milan Hulmák and Petr Bezouška, Občanský zákoník VI Závazkové právo Zvláštní část (§ 2055-3014) Komentář (1 edn, Nakladatelství C H Beck 2014) 1640-1641

Jaromír Kincl and others, *Římské právo* (1 edn, CH Beck 1995)

Journals

Čerka Paulius, Grigienė Jurgita & Sirbikytė Gintarė, 'Liability for damages caused by artificial intelligence' [2015] 31 *Computer Law & Security Review*

Harry Surden, 'Artificial Intelligence and Law: An Overview' [2019] 35(4) *Georgia State University Law Review*

Roman Dremluga, Pavel Kuznetsov & Alexey Mamych, 'Criteria for Recognition of AI as a Legal Person' [2019] 12(3) *Journal of Politics and Law*

Lawrence B. Solum, 'Legal Personhood for Artificial Intelligences' [1992] 70(4) *North Carolina Law Review*

Hubbard F. Patrick, 'Sophisticated Robots: Balancing Liability, Regulation, and Innovation' [2014] 9, *University of South Carolina - Faculty Publications*

Leon E. Wein, 'The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence' [1992] 6 (Fall) *Harvard Journal of Law & Technology*

M. Petit, 'Towards a Critique of Algorithmic Reason A state-of-the-art review of artificial intelligence' [2018] XXI (44) *Quaderns del Cac - Fake news, algorithms and filter bubbles*

Other sources

Austrian Council on Robotics and Artificial Intelligence, 'Shaping the Future of Austria with Robotics and Artificial Intelligence' (www.acrai.at) <<https://www.acrai.at/en/home/>> Amitai & Oren Etzioni, 'Should Artificial Intelligence Be Regulated?' (www.issues.org, 1 July 2017) <<https://issues.org/perspective-should-artificial-intelligence-be-regulated/>>

Consumer Financial Protection Bureau, 'Requests for Information: Use of Alternative Data and Modeling Techniques in Credit Process' (www.regulations.gov, 19 May

2017) <https://www.regulations.gov/document?D=CFPB_FRDOC_00010521>accessed 21 June 2020

European Banking Authority, 'Report on the Prudential Risks and Opportunities Arising for Institutions from Fintech' (Eba.europa.eu, 3 July 2018) <<https://eba.europa.eu/sites/default/documents/files/documents/10180/2270909/02c7859f-576e-421e-b243-a145c0eaa131/Report%20on%20prudential%20risks%20and%20opportunities%20arising%20for%20institutions%20from%20FinTech.pdf?retry=1>> accessed 21 June 2020

Financial Stability Board, 'Artificial intelligence and machine learning in financial services - Market developments and financial stability implications' (www.fsb.org, 1 November 2017) <https://www.fsb.org/wp-content/uploads/P011117.pdf> accessed 21 June 2020

Stanford University, 'Artificial Intelligence and Life in 2030' (One Hundred Year Study on Artificial Intelligence (AI100), 1 September 2016) <<https://ai100.stanford.edu/>> accessed 21 June 2020

US Department of Transportation, 'Automated Driving Systems 20: A Vision for Safety' (National Highway Traffic Safety Administration, 1 September 2017) <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069aads2.0_090617_v9a_tag.pdf> accessed 22 June 2020

World Health Organization, 'Global Plan for the Decade of Action for Road Safety 2011-2020 ' (www.who.int, 11 May 2011) <https://www.who.int/roadsafety/decade_of_action/plan/plan_english.pdf> accessed 22 June 2020

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

European Commission, Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe, COM(2018)237, 25 April 2018

European Economic and Social Committee, Opinion on 'Artificial intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (2017/C 288/01)

Economic Commission for Europe - Working Party on Road Traffic Safety, 'Report of the sixty - eighth session of the Working Party on Road Traffic Safety' (www.unece.org, 17 April 2014) <<https://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf>> accessed 24 June 2020

European Commission, 'Guidelines on the Exemption Procedure for the EU Approval of Automated Vehicles' (Brussels, 2019)

European Parliament - Directorate General for external policies, 'Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare' (www.europarl.europa.eu, 1 May 2013) 4 <[https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPODROI_ET\(2013\)410220_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPODROI_ET(2013)410220_EN.pdf)> accessed 24 June 2020

European Commission, Report from the Commission to the European Parliament, the Council and the European and Economic Social Committee - Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics (Brussels, Cm 64, 2020)

European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust (Brussels, Cm 65, 2020)

Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H., Lopez Cobo M., Mertens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic L., Artificial Intelligence - A European Perspective (ISBN 978-92-79-97219-5, Publications Office of the European Union, Luxembourg, 2018)

Future of life institute, 'Autonomous Weapons: An Open Letter From AI & Robotics Researchers' (<https://futureoflifeorg/>, 28 July 2015) <https://futureoflife.org/open-letter-autonomous-weapons> accessed 24 June 2020

European Parliament resolution 2018/2751(RSP) of 12 September 2018 on autonomous weapon systems

Future of life institute, 'Asilomar AI Principles' (www.futureoflife.org, 8 January 2017) <[https:// futureoflife.org/ai-principles/](https://futureoflife.org/ai-principles/)> accessed 25 June 2020

European Commission, 'Report of the High-Level Expert Group on the Impact of the Digital Transformation on EU Labor Markets ', April 2019

European Commission, 'AI and Automation' (www.ec.europa.eu, 23 July 2019) <https://ec.europa.eu/knowledge4policy/foresight/topic/changing-nature-work/AI-and-automation_en> accessed 26 June 2020

H.R. 827 - 116th Congress: AI JOBS Act of 2019.” www.GovTrack.us. 2019. June 26, 2020 <<https://www.govtrack.us/congress/bills/116/hr827>>

European Commission, 'The Directive on security of network and information systems (NIS Directive)' (www.ec.europa.eu, 15 April 2020) <<https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>> accessed 27 June 2020

European Commission, 'The EU Cybersecurity Act' (www.ec.europa.eu, 28 February 2020) <[https://ec.europa.eu/digital-single-market/en/eu-cybersecurityact#:~:text=The%20EU%20Cybersecurity%20Act%20grants,more%20resources%20and%20new%20tasks.&text=This%20task%20builds%20on%20ENISA,information%20systems%20\(%20NIS%20Directive\).>](https://ec.europa.eu/digital-single-market/en/eu-cybersecurityact#:~:text=The%20EU%20Cybersecurity%20Act%20grants,more%20resources%20and%20new%20tasks.&text=This%20task%20builds%20on%20ENISA,information%20systems%20(%20NIS%20Directive).>)> accessed 27 June 2020

European Patent Office, 'Guidelines for Examination' (www.epo.org, 1 May 2018) <[https://www .epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_3_1 .htm](https://www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_3_1.htm)> accessed 28 June 2020

Noam Shemtov, 'A study on inventorship in inventions involving AI activity' (www.epo.org, 1 February 2019) <[http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/\\$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf](http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf)> accessed 28 June 2020

Swachhindia, 'Ganga And Yamuna Are Not Living Entities, Rules Supreme Court' (www.swachhindia.ndtv.com, 22 September 2017) <<https://swachhindia.ndtv.com/ganga-and-yamuna-are-not-living-entities-rules-supreme-court-9716/>> accessed 29 June 2020

S. Padmavathi, D.G. Hari Prasath, Supreme Court Judgement On Ayodhya Issue: Ram Janmabhoomi - Babri Masjid Land Title Dispute (Notion Press 2020)

Naresh Kumar, 'Legal Personality, Legal Person in Jurisprudence' (www.lawnotes4u.in, 26 April 2019) <<https://www.lawnotes4u.in/2019/04/legal-personality-legal-person-in-jurisprudence.html>> accessed 29 June 2020

Visa Aj Kurki, Tomasz Pietrzykowski, Legal Personhood: Animals, Artificial Intelligence and the Unborn (Springer 2017)

World Intellectual Property Organization, 'Copyright Protection of Computer Software' (www.wipo.int, unknown date of publication) <<https://www.wipo.int/copyright/en/activities/software.html>> accessed 30 June 2020

Terence Mills, 'AI Vs AGI: What's The Difference?' (www.forbes.com, 17 September 2018) <<https://www.forbes.com/sites/forbestechcouncil/2018/09/17/ai-vs-agi-whats-the-difference/#215462f738ee>> acc-essed 2 July 2020

Jack Krupansky, 'Untangling the Definitions of Artificial Intelligence, Machine Intelligence, and Machine Learning' (www.perma.cc, 13 June 2017) <<https://perma.cc/RVZ4-88NP>> accessed 2 July 2020

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))

Janosch Delcker, 'Europe divided over robot 'personhood'' (www.politico.eu, 4 November 2018) <<https://www.politico.eu/article/europe-divided-over-robot-ai-artificial-intelligence-personhood/>> accessed 3 July 2020

United Nations Educational, Scientific, and Cultural Organization - World Commission on Ethics of Scientific Knowledge and Technology, 'Report of COMEST on Robotics Ethics' (2017/SHS/YES/COMEST-10/17/2 REV)

European Commission, 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', Commission Staff Working Document, Liability for emerging digital technologies, COM(2018)237, 25 April 2018

Expert Group on Liability and New Technologies - New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies (Publications Office of the European Union 2019)

Peter Chapman, 'Regulating robots: a new reality? Civil Law Rules on Robotics' (www.cliffordchance.com, 16 July 2019) <<https://talkingtech.cliffordchance.com/en/emerging-technologies/internet-of-things/regulating-robots--a-new-reality.html>> accessed 20 July 2020

Robert Nešpůrek, 'Evropský parlament otevírá cestu regulaci umělé inteligence' (www.epravo.cz, 15 September 2017) <<https://www.epravo.cz/top/clanky/evropsky-parlament-otevira-cestu-unijni-regulaci-umele-intelligence-106387.html>> accessed 20 July 2020

European Commission, 'High-Level Expert Group on Artificial Intelligence' (www.ec.europa.eu, 9 July 2020) <<https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>> accessed 20 July 2020

High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (8 April 2019) <<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>> accessed 20 July 2020

High-Level Expert Group on AI, 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment' (www.eceuropa.eu, 17 July 2020) <<https://>

ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> accessed 20 July 2020

High-Level Expert Group on AI, 'Policy and investment recommendations for trustworthy Artificial Intelligence' (www.ec.europa.eu, 26 June 2019) <<https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>> accessed 20 July 2020

Christiane Wendehorst, 'Product Liability Directive: protecting consumers in the Digital Single Market' (www.europarl.europa.eu, 22 January 2020) <<https://www.europarl.europa.eu/committees/en/product-liability-directive-protecting-c/product-details/2020107CHE06841>> accessed 21 July 2020

Sylvie Gallage-Alwis, 'Updating The EU Product Liability Directive For The Digital Era' (www.signaturelitigation.com, 25 February 2020) <https://www.signaturelitigation.com/updates/the-eu-product-liability-directive-for-the-digital-era-sylvie-gallage-alwis/> accessed 21 July 2020

European Parliament, Resolution on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP), 12 February 2020

Sky News, 'Tesla Driver In First Self-Drive Fatal Crash' (www.news.sky.com, 1 July 2016) <<https://news.sky.com/story/tesla-driver-in-first-self-drive-fatal-crash10330121>> accessed 23 July 2020

Linda Kolaříková, 'Odpovědnost (za) robota aneb právo umělé inteligence' ([Http://www.bulletin-advo-kacie.cz/](http://www.bulletin-advo-kacie.cz/), 18 April 2018) <<http://www.bulletin-advokacie.cz/odpovednost-za-robota-aneb-pravo-umele-intelligence>> accessed 23 July 2020

Andreea Stoian Karadeli, 'The European Defence Fund - What are the political, economic and ethical aspects of one of the most important measures of the EU's new security and defence agenda?' (www.euro-sd.com, 13 December 2019) <<https://euro-sd.com/2019/12/articles/15510/the-european-defence-fund-what-are-the-political-econo>

mic-and-ethical-aspects-of-one-of-the-most-important-measures-of-the-eus-new-security-and-defence-agenda/> accessed 24 July 2020

Aoife Kennedy, 'European Social Fund' (www.europarl.europa.eu, 1 February 2020) <<https://www.europarl.europa.eu/factsheets/en/sheet/53/european-social-fund>> accessed 24 July 2020

Andres Guadamuz, 'Artificial intelligence and copyright' (www.wipo.int, 1 October 2017) <https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html#:~:text=Artificial%20intelligence%20is%20already%20being,used%20and%20reused%20by%20anyone.> accessed 24 July 2020

European Commission, Liability for emerging digital technologies accompanying the document 'Communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions - Artificial Intelligence for Europe', COM(2018)237, 25 April 2018

Thomas Burri, 'The EU is right to refuse legal personality for Artificial Intelligence' (www.euractiv.com, 31 May 2018) <<https://www.euractiv.com/section/digital/opinion/the-eu-is-right-to-refuse-legal-personality-for-artificial-intelligence/>> accessed 24 July 2020