INTERNATIONAL
HELLENIC
UNIVERSITY

LEGAL LIABILITY OF ARTIFICIAL INTELLIGENCE-DRIVEN SYSTEMS ("AI")

Charikleia Bertsia

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

Master of Laws in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation (LLM)

February 2019

Thessaloniki – Greece

Student Name: Charikleia Bertsia

SID: 1104170003

Supervisor: Prof. Teresa Rodriguez De Las Heras Ballell

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

February 2019
Thessaloniki - Greece

Abstract

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation at the International Hellenic University.

The main aim of this thesis is to determine whether AI systems may be held liable for tort and contractual damages caused by their actions or even omissions. In the absence of direct legal regulation of AI, the thesis begins by recounting the history and definition of AI and examines current technological AI applications. This history raises critical questions as to how AI's specific features impact tortious liability. In parallel, this thesis explores the applicability of existing liability regimes to AI and evaluates potential points of inadequacy. Moreover, this thesis will analyze the Product Liability regime in the European Union ("EU") to determine whether it suitably addresses issues raised by increasing AI usage.

Thereafter, the thesis examines other theories for allocating liability through the application of various other paradigms of legal responsibility, such as strict liability. Subsequently, this thesis will also identify certain scenarios where AI could enter into contractual obligations, or engage in tortious behaviors. At this point, the thesis will proffer possible solutions for adjudicating liability while, *inter alia*, elaborating on the issue of Robot Personhood, with a specific inquiry as to its impact on Europe. The fact that AI is not yet the subject of law or regulation raises both ethical and liability questions for the damages AI causes. Finally, the thesis examines whether proper regulation can be meaningfully impactful, but also under which circumstances regulation might carry risks, especially when considering its potential for hindering technological innovation.

Keywords: Legal Liability; Artificial Intelligence; Legal Personhood; Legal Agent; Tort Liability; Product Liability Directive.

Charikleia Bertsia

07/02/2019

Preface

At this point, I would like to thank my fellow students for their feedback, cooperation and of course friendship. In addition I would like to express my gratitude to the staff of International Hellenic University for their support and for the last minute favors.

Nevertheless, I am also grateful to the Professor Ms Teresa Rodriguez De Las Heras Ballell, a truly inspiring supervisor and it would be my honor to cooperate with her again in the future.

I would like to thank my friends for accepting nothing less than excellence from me. Of course, I would like to thank my family: my parents and my brother for supporting me spiritually throughout writing this thesis and my life in general. Last but not least, a huge thank you to my cousin Christos Kaltsas, one of the most selfless and extraordinary human beings I've ever had the chance to have in my life. His help in carrying out this thesis was of great importance while at the same time, he guided me to reach the high standards I always worked for.

Contents

Introduction

Approach of concept and definition of Artificial Introduction

It is not always so obvious, but AI permeates our daily lives in numerous ways. Today, AI is able to perform tasks which, until quite recently, only humans with specialized knowledge or specific license could execute. The inevitable arrival of driverless cars on the consumer market will transform road transportation. Virtual personal assistants will help us organize our working day and even suggest products or restaurants that we might prefer or desire. Beyond making our lives easier, AI can execute complex financial transactions, treat chronic diseases[1], flag cyber security threats or even fight climate change. For example, in Denmark, AI is helping save lives by allowing emergency services to diagnose cardiac arrests or other conditions based on the sound of a caller's voice. At the same time, in Austria, it enables radiologists to detect tumors more accurately by comparing x-rays simultaneously with other medical data. Meteorology also benefits as AI-driven data analysis enables us to forecast the upcoming weather[2]. It is also used in agriculture. Many farms across Europe are using AI to monitor the movement, temperature, and feed consumption of their animals. The AI system can then automatically adapt the heating and feeding machinery to help farmers monitor their animals'welfare. Notably, its increasing and rapidly expanding potential has heralded immense private sector investment in AI projects. All the above paradigms are only scratching the surface of the real abilities of AI. Already, some of these complex tasks can be executed without active human control or even supervision[3]. Firms

[1] Andy Kessler, "Siri, Am I About to Have a Heart Attack?," *Wall Street Journal*, January 9, 2017.
[2] Andrew Culclasure, "Using Neural Networks to Provide Local Weather Forecasts" (master's thesis, Georgia Southern University, 2013).
[3] Neil Johnson et al., *Abrupt Rise of New Machine Ecology Beyond Human Response Time*, SCI. REPORTS, Sept. 11, 2013, at 1, 2; Aaron Kessler: Law Left Behind as Hand Free Cars Cruise (May 3, 2015).

such as Google, Amazon, Facebook and Baidu have invested large amount of money in order to prevail in this innovation race[4]. AI has started gaining footholds in new industries and becomes more interactive in our daily lives. This new reality seems to be the dominant trend for the foreseeable future[5].

But what truly is AI? It was the year of 1956, when the concept of artificial intelligent emerged through John McCarthy, an American computer scientist and cognitive scientist. The term artificial intelligence has taken many connotations during its history, with some relating to neural networks, machine learning and even data mining.

The European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, published a very important Communication Document in April 2018 where, *inter alia,* they provided a unified definition of "artificial intelligence". More specifically, they concluded that "[a]rtificial Intelligence refers to systems that display intelligent behavior by analyzing their environment and taking actions –with some degree of autonomy- to achieve specific goals". It continues by explaining that AI-based systems can be purely software-based systems, meaning that they exist only virtually (e.g. voice assistants, image analysis software), or AI can be embedded in hardware devices (e.g. robots, drones, autonomous cars)[6]. Although the EU tried to deliver this specific definition, AI doesn't appear to enjoy such a wide definition even among experts in the field, much less among lawmakers. The AI pioneer John McCathy stated that there is "no solid definition of intelligence that doesn't depend on relating it to human intelligence" because "we cannot yet characterize in general what kinds of computational procedures we want to call intelligent"[7]. While the conceptual of intelligence is so vague, it is inevitable to have various definitions of AI. Notions of intelligence focus on myriad interconnected human

[4]Yves Eudes, *The Journalists Who Never Sleep*, GUARDIAN (Sept. 12, 2014, 6:17 AM), http://www.theguardian.com/technology/2014/sep/12/artificial-intelligence-datajournalism-media [https://perma.cc/CES7-X58C] (discussing the increasing use of "robot writers" in journalism).

[5] *Artificial Intelligence: Rise of the Machines*, ECONOMIST (May 9, 2015), http://www.economist.com/news/briefing/21650526-artificial-intelligence-scarespeopleexcessively-so-rise-machines [https://perma.cc/B2LD-B4XS].

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

[7] See John McCarthy, What is Artificial Intelligence?, JOHN MCCARTHY'S HOME PAGE 2–3 (Nov. 12, 2007), http://www-formal.stanford.edu/jmc/whatisai.pdf [https://perma.cc/U3RT-Q7JK].

characteristics that are themselves difficult to define like, e.g., consciousness, language use, self-awareness, the ability to learn, the ability to adapt and the ability to reason[8].

Other approaches try to define AI in a more practical way. Experts supporting those approaches claim that the concept of intelligence is tied to the ability to perform particular intellectual tasks. One of the most leading textbooks on the definition of AI is Stuart Russell and Peter Norvig's *Artificial Intelligence: A modern approach.* In this textbook, the authors present eight different definitions of AI organized into four categories: thinking humanly, acting humanly, thinking rationally and acting rationally[9]. This definition inconsistency isn't happening on purpose, of course. Technological advantages allow computers to perform tasks that they previously could not. That affects the wording and concept of AI. John MacCathy defined intelligence as "the computational part of the ability to achieve goals in the world" and the AI as "the science and engineering of making intelligent machines, especially intelligent programs"[10].

Nowadays, the scientific approaches tend to define AI through the lens of machines and their ability to achieve specific goals. In their textbook, Stuart Russell and Peter Norvig, utilize the concept of a "rational agent" who basically i s the "one that acts so as to achieve the best outcome or, when there is uncertainty, the best expected outcome"[11]. However, the goal-oriented approach does not seem to constitute an absolute problem-solver with respect to regulatory perspective. In law, goal usually is synonymous with intention[12]. It is metaphysical to acknowledge intent to a machine. Rational action as a principle, would not,

[8] Some of these characteristics are, of course, present to various degrees in some other animals as well. See generally, e.g., DAVID PREMACK,INTELLIGENCE IN APE AND MAN (1976); Olivier Pascalis & Jocelyne Bachevalier, Face Recognition in Primates: A Cross-Species Study, 43 BEHAV. PROCESSES 87 (1998); Rachel Adelson, Marine Mammals Master Math, MONITOR PSYCHOL. Sept. 2005, at 22, http://www.apa.org/monitor/sep05/marine.aspx [https://perma.cc/DU3G-4VP8].

[9] RUSSELL & NORVIG, supra note 7, at 2.

[10] McCarthy, supra note 7; see also Stephen M. Omohundro, The Basic AI Drives, in ARTIFICIAL GENERAL INTELLIGENCE 2008 483, 483 (2008)

[11] RUSSELL & NORVIG, supra note 7, at 4.

[12] THE AMERICAN HERITAGE DICTIONARY and MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY both direct readers to the entry for "intention" for a list of synonyms of "goal." *Goal*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2000);*Goal*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2003).

standing alone, provide a sufficient legal definition for AI. Consequently, a goal-oriented definition has a lot of obstacles to tackle in its effort to effect a solid legal definition. Hence, Matthew U. Scherer, in his paper *Regulating Artificial Intelligence Systems: Risks, challenges, competencies and strategies,* opined that AI "refers to machines that are capable of performing tasks that, if performed by a human, would be said to require intelligence".

1. Entering the age of Algorithmic Society and Big Data

1.1. Obstacles to Regulating "AI"

Since the invention of the steam engine until the appearance of the Internet and now, the Algorithmic Society, technological progress has always played the role of innovation for liabilities systems.[13] But, what is the Algorithmic Society? It is a society organized around decisions which are made and eventually carried out by algorithms, robots and IoT devices. The latter connect wirelessly to a network and have the ability to transmit data while at the same time they can communicate and interact over the internet. This wouldn't be possible without the feature of Big Data. Paraphrasing Kant's famous statement, that "[t]houghts without content are empty, intuitions without concepts are blind"[14] we could say that algorithms without data are empty while data without algorithms are blind. It is crucial to always remember that robots are also met as cloud robots. Consequently, the handling of data is a very important issue as many AI systems will be connected to the Internet cloud, meaning that they will interact and absorb an immense volume of data.[15]

[13] As to U.S., the locus classicus is Morton J. Horwitz, The Transformation of the American Law, 1780-1860 (Oxford UP 1977) 67-108; also for a more nuanced view Gary T. Schwartz, "Tort Law and the Economy in Nineteenth-Century America: A Reinterpretation, 90 Yale L.J. 1717, 1734-1756 (1981)

[14] IMMANUEL KANT, CRITIQUE OF PURE REASON 193-94 [A51/B76] (Paul Guyer & Allen W. Wood eds., trans., Cambridge University Press 1998)

[15] Bob Violino, Big data and robotics: A long history together, ZDNet, August 12, 2016, at http://www.zdnet.com/article/big-data-and-robotics-a-long-history-together/

Furthermore, the rise of AI has so far occurred in a regulatory gap is an inescapable conclusion when considering the EU's current legal regime. This regulatory vacuum has much in common with the initial appearance of internet. During the mid-nineties, the Clinton administration, alongside the United States Congress, passed the Telecommunication Act of 1996, which specifically sought to avoid regulating the internet, like analog-era communications and media technologies. In addition, Section 230 of the Act exempted online intermediaries from tort liability for content which user might post on their platforms[16]. The spirit of this framework was that "the private sector should lead (and) the Internet should develop as a market driven arena not regulated industry"[17] and the American government should "avoid undue restrictions on electronic commerce".[18]

The central idea of this policy was to let Internet find its own ways and evolve alongside market needs notwithstanding the possibility of failure. America's political proclivity to risk embraced this market-driven policy which, at the very end, helped modern digital revolution and innovation and, in turn, labor prosperity and economic productivity. In Europe, on the other hand, "failure is regarded as a personal tragedy" according to German economist Petra Moser. Indeed, Europe's approach is rooted in a precautionary principle which broadly affects European regulatory processes. The European approach to technology focuses on privacy and data security, which had, and still does, jeopardize innovation to some extent. Restrictive policies in the 1990s and beyond decreased the likelihood of innovation while on the other side of the ocean, they are increased[19]. For example, the 1995 EU Data Protection Directive led into a restrictive set of regulations for online data collection and use[20] which affected companies, such as Google and Facebook, in deploying their commercial plans[21].

[16] Derek Khanna, "The Law That Gave Us the Modern Internet—and the Campaign to Kill It," *Atlantic*, September 12, 2013.
[17] White House, *Framework for Global Electronic Commerce*.
[18] Ibid.
[19] Tal Z. Zarsky, "The Privacy-Innovation Conundrum," *Lewis and Clark Law Review* 19, no. 1 (2015).
[20] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, October 1995
[21] Avi Goldfarb and Catherine Tucker, "Privacy and Innovation," in *Innovation Policy and the Economy*, vol. 12, ed. Josh Lerner and Scott Stern (Chicago: University of Chicago Press, 2012).

Not to mention, while firms in EU countries find it very difficult to access venture capital[22], US firms are able to risk freely and invest considerable capital in the future of AI projects. Private investment in AI technologies has grown substantially in recent years, from $1.7 billion in 2010 to $14.9 billion in 2014[23]. A Booz & Company study in 2013 revealed that during that year, $13.8 billion of investment dropped at the healthcare industry, $9.7 billion to electronic manufacturers and finally $7.7 billion to software and web companies[24].

Analysts anticipate that AI health technologies are the ones which will benefit the most from the new market reality and will enjoy a huge market success. According to a McKinsey and Company report, investments in advanced robotics could range from $1.7 trillion to $4.5 trillion by 2025[25]. Market potentials are enormous; but, as the adage goes, predictions are difficult to make. One norm provides, of course, that technologies should succeed or fail on their own merits and not because of poor regulatory frameworks which create obstacles towards innovation. On the other hand, AI became subject to a lot of critics and gave rise to dystopian scenarios and tales of killer robots which destroys humanity[26]. Indeed, technological progress has always met resistance and hesitation in light of those scenarios.

There are scholars who propose, among other things, the passage of broad-based legislation in the US, such as an Artificial Intelligence Development Act[27], as well as the creation of a federal AI agency[28] or possibly a Federal Robotics Commission[29] or National

[22] Josh Lerner, "The Impact of Privacy Policy Changes on Venture Capital Investment in Online Advertising Companies" (White Paper for the Analysis Group, Menlo Park, CA, 2012).
[23] Chen et al.,"Global Economic Impacts."
[24] Gitta Rohling, "Facts and Forecasts: Boom for Learning Systems," Innovations newsletter (Siemens), October 1, 2014
[25] James Manyika et al., *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy* (San Francisco: McKinsey Global Institute, May 2013).
[26] For examples, see Ben Austen, "The *Terminator* Scenario: Are We Giving Our Military Machines Too Much Power?" P*opular Science*, January 13, 2011; John Markoff and Claire Cain Miller, "As Robotics Advances, Worries of Killer Robots Rise," *New York Times*, June 16, 2014.
[27] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies," *Harvard Journal of Law and Technology* 29, no. 2 (2016): 393–97.
[28] Ibid, 395–97.
[29] Ryan Calo, "The Case for a Federal Robotics Commission" (Brookings Institution, Washington, DC, September 2014).

Algorithmic Technology Safety Administration[30]. Most of this legislation would establish a certification process for AI usage. At the same time, those proposed laws and agencies would also require innovators to subject their technologies to a regulatory review in order to "ensure the safety and security of their A.I"[31]. Those agencies could also carry out an advisory role towards other federal, state, and local officials and organizations on how to craft policy for AI and robotics.

1.2. Autonomy and Foreseeability

These trends will provoke extensive economic challenges and distributions to the labor market[32]. So, which are the main challenges AI poses to legal system?

The problematic characteristics of AI occur from its ability to act autonomously. More specifically, AI systems are able to generate "outside-the-box" solutions to complex problems, meaning that humans could not expect such solutions. There is an excellent example which derives from the domain of health. C-Path is a cancer pathology machine learning program[33] which by "itself" found that the characteristics of the stroma constitute a better prognostic indicator comparing to cancerous cells themselves[34]. Even the most careful designers, programmers and manufacturers won't be able to fully control or predict what a

[30] Andrew Tutt, "An FDA for Algorithms," *Administrative Law Review* 69, no. 1 (2017).
[31] Scherer, "Regulating Artificial Intelligence Systems," 394.
[32] *See, e.g.*, Aaron Smith & Janna Anderson, *AI, Robotics, and the Future of Jobs*.
[33] Machine learning is a type of artificial intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can teach themselves to grow and change when exposed to new data." Margaret Rouse, *What Is Machine Learning*, WHATIS.COM, http://whatis.techtarget.com/definition/machine-learning [https://perma.cc/NCV5-83KF].
[34] *See* Andrew H. Beck et al., *Systematic Analysis of Breast Cancer Morphology Uncovers Stromal Features Associated with Survival*, SCI. TRANSLATIONAL MED., Nov. 9, 2011, at 1, 8.

solution an AI system will be able to generate, after it leave their supervision[35]. Thus, it is almost impossible for the AI's designers to foresee how it will evolve.

Therefore, the concept of foreseeability is crucial. If legal systems adopt the norm that the experiences of learning AI systems are a priori unforeseeable, it would be unfair to hold the systems' designers liable for harm that the systems cause. Consequently, the victims of this harm might be left uncompensated for the losses they suffer.[36]

1.3. Control issue

Apart from the risks created by the non-foreseeability of AI driven systems, control issues also arise. Machines are programmed to act with a considerable autonomy to achieve specific purpose. As I elaborate therein, AI does not act in a way that implies consciousness, but rather executes orders embossed by humans on its software or hardware. Nevertheless, in a number of cases where AI is designed with features that permit it to learn or adapt, it might be difficult for humans to maintain control. I cite here some examples of mechanisms which a loss of control may occur: a malfunction, such as a corrupted file or physical damage to input equipment; a security breach; the superior response time of computers as compared to humans;[37] or flawed programming.

The latter malfunction raises the most interesting issues because it creates the possibility that a loss of control might be the direct but unintended consequence of a conscious design choice. Control, once lost, might be unobtainable. AI would able to become more and more sophisticated through experience with unexpected consequences.

---

[35] *See* Pei Wang, *The Risk and Safety of AI*, A GENERAL THEORY OF INTELLIGENCE, https://sites.google.com/site/narswang/EBook/topic-list/the-risk-and-safety-of-ai.

[36] *See* RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIABILITY §§ 10–17 ("Liability of Multiple Tortfeasors for Indivisible Harm"); *id.* §§ 22–23 ("Contribution and Indemnity"); Calo, *supra* note 11, at 554–55; Balkin, *supra* note 49, at 53.

[37] *See* Johnson et al., *supra* note 3.

These characteristics make AI a potential source of public risk. It occurs when the humans legally responsible for its operation and supervision cannot control it anymore[38]. On the other hand, when no human can control AI system anymore, then a loss of *general control* is occurring. As mentioned above, AI's objectives are determined by its initial programming. Even if initial programming permits AI to alter its goals based on acquired experience, these alterations will occur in accordance the structure of the initial programming. Probably this outcome helps keep an AI driven system under control. Hence, many experts and commentators suggest that there is nothing to assure us that an AI system, programmed to achieve specific goal, will continue to work toward that objective in a public secure way. This is not happening because of an initial malfunction of course, but rather stems from the machine's fundamental indifference to the subject intent[39].

While the number of academics, tech entrepreneurs and futurists who warn that stronger forms of AI may resist all human efforts to govern their actions continues growing, we seriously consider that a sophisticated AI system could improve its own programming and hardware, exposing humanity writ large to serious public risks. If ultimately, this realization becomes a reality, a theoretical legal approach to this issue argues that an *ex ante* action would be necessary to ensure that the AI systems remain always under susceptible human control aligned with public interest.[40] Already, increasingly powerful, sophisticated and autonomous AI systems are executing commands pertaining stock trades on time scales that can be measured in nanoseconds.[41] Even here, AI manage immense fiscal risks that may lurk in these types of algorithmic trading systems[42]. Although these transactions are theoretically reversible, the need to retain means for controlling sophisticated AI systems is clearly illustrated during the Algorithmic Era.

---

[38] See Regulating Artificial Intelligent Systems/ Harvard journal of Law & Technology Spring 2016/p.367
[39] NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 196 (2014).
[40] See Regulating Artificial Intelligent Systems/ Harvard journal of Law & Technology Spring 2016/p.368
[41] *See* Johnson et al., *supra* note 3, at 1.
[42] *See, e.g.*, Nils Pratley, *The Trillion-Dollar Questions over the Flash Crash and the Hound of Hounslow*, GUARDIAN (Apr. 25, 2015, 11:00 AM), http://www.theguardian.com/ business/2015/apr/25/flash-crash-hound-of-hounslow-trillion-dollar-question [https://perma.cc/88QE-5FR4].

1.4. Research and Development of AI: problematic features

As explained supra, it would be irrational to blame AI itself for its problematic features. From a regulatory standpoint, the responsibility for tortuous AI behavior lie in the manner AI research and development works. But, how can we define this process? In his paper on how to regulate an AI system, Matthew U. Scherer, describes four parallel processes that are usually take place to wit:

> *"Discreetness* refers to the fact that AI development work can be conducted with limited visible infrastructure.
>
> *Diffuseness* means that the individuals working on a single component of an AI system might be located far away from one another. A closely related feature, *discreteness*, refers to the fact that the separate components of an AI system could be designed in different places and at different times without any conscious coordination. Finally, *opacity* denotes the possibility that the inner workings of an AI system may be kept secret and may not be susceptible to reverse engineering."[43]

The safeguarding of the public interest has always been the compass of justice and the rule of law. In the twentieth century, all sources of public risk –such as nuclear technology, mass-produced consumer goods, industrial-scale pollution, the production of large quantities of toxic substances- required massive investments. The high cost of starting a company, the building of the necessary facilities, like factories, the purchasing of the

[43] See Regulating Artificial Intelligent Systems/ Harvard journal of Law & Technology Spring /p.369 (2016).

necessary equipment, hiring experienced labor and so on, demanded lots of capital. Who would be able to provide all the recommended capital but the large corporations alongside with governmental entities? This phenomenon facilitated the regulatory processes. Why? Because the physical visibility of the corporation and of the people needed to operate it made it easy for the regulators to determine the "who" and "where" of potential sources of public risks.

By contrast, AI isn't characterized by the above features. AI research and development can be performed relatively *discreetly* meaning that artificial intelligence research can be done by many, not just via extremely wealthy institutions. Moreover, AO research and development does not require substantial recourses and facilities. Anyone with a modern computer can write a computer code and, with an Internet connection, contribute to AI- related projects.

Continuing analyzing the main differences of public risk as it was configured before and public risk of tomorrow, let us keep in mind that the potential of *diffuse* by public risk standards plays also a major role in evaluating putative legal regimes. What is happening is that participants in an AI-related project do not need to be part of the same organization or any organization at all. Already, many machine-learning libraries have been created and are catered with data by dispersed individuals who sometimes act anonymously. Thousands modifications can be made at these libraries on a day-to-day basis[44]. Then, it is at the creator's discretion to build an AI program using parts of -not only one but- multiple such libraries, each of which is developed *discretely* from the others.[45] By examining the legal capacity of the person who participates in the building of an open-source library, we notice that it is impossible to know beforehand what other individuals or entities might use this

[44] On April 2, 2015 alone, nine unique users made nineteen modifications to scikit-learn's code. According to the users' profile pages, two users are located in Switzerland, two more in France, one in the United States, and one in India; the remaining two users' profile pages give no indication of their geographic location. *See scikit-learn: Machine Learning in Python*, GITHUB, https://github.com/scikit-learn/scikit-learn/commits/master?page=57 [https://perma.cc/WV56-Z762].

[45] *Cf.* WALLACH & ALLEN, *"Moral Machines: Teaching Robots right from wrong (2009)* at 198.

particular library in the future. For that reason, it would be against the rule of law to hold these individuals liable for the future possible use of hers contribution to the library.

These open-source projects are not the only sources of available material. Commercial off-the-shelf, named "COTS", are used broadly by many modern computer systems. COTS usually are privatized hardware and software components.[46] Software components are maximizing the use of COTS mainly because of their low cost, while ignoring the potential security issues associated with the use of software wholly outside the software creator's control.[47] This results in the creation of a software and hardware eco-system where innumerable interactions and combinations among those components are taking place. This complexity seems likely to progress with the development of stronger forms of AI.[48] While some AI systems will be built with COTS, others will utilize programming and physical components designed and developed primarily for the AI project in question. This interaction may occur between numerous components in different geographic locations. Participants could be located in different countries and have no legal or formal contractual relationship with one another. Even if one country regulates their citizens' participation in an AI project, nothing can be done in a global range. Large firms which intend to avoid such regulation would easily move offshore, choosing a country with less strict regulatory regime. It would be also very confusing for the companies involved to know which regime is applicable when determining how to manage the risks associated with AI.

The final feature of an AI system is that its inner workings may be more *opaque* comparing to previous technologies. It seems unlikely that an AI system would be well understood, or even demonstrate transparency, in contrast with, for example,

---

[46] *See* Robert B.K. Dewar, *COTS Software in Critical Systems: The Case for Freely Licensed Open Source Software*, MILITARY EMBEDDED SYSTEMS (Dec. 9, 2010), http://mil-embedded.com/articles/cots-open-source-software/ [https://perma.cc/T5G5-PXAB].

[47] *See generally* Carol Woody & Robert J. Ellison, *Supply-Chain Risk Management: Incorporating Security into Software Development*, DEP'T OF HOMELAND SEC. (Mar. 15, 2010), https://buildsecurityin.us-cert.gov/articles/best practices/acquisition/supply-chainriskmanagement%3A-incorporating-security-into-software-development [https://perma.cc/UV6U-X64C].

[48] *Rayan* Calo,Robotics and the Lessons of Cyber Law, 103, Calif L. Rev. at 534.

automobiles, which constitute one of the great sources of public risk. Despite the complexity of the latter [they contain approximately 30,000 individual parts], its mechanics are well understood. Manufacturers and distributors cannot easily detect defects in the design of a complex AI system, let alone the consumers.[49]

Taken together, these difficulties complicate the ex ante regulating of AI. The individuals and firms who participate in the design, modification and incorporation of an AI system's components may be numerous, that legal systems encounter extreme difficulty in allocating responsibility among them. Hence, the efforts to compensate the suffered party *ex post* could be challenging. Courts might not hesitate to hold an AI designer responsible for the damage caused, arguing that he or she should have foreseen the harm that occurred. On the other hand, the opacity of AI systems may also make difficult for the courts to assign liability to the end user of an AI system that causes harm to a third party.

2. Concept of legal capacity in AI

2.1 Legal Capacity of natural persons

The classical discussion of the idea of legal personhood is found in John Chipman Gray's *The Nature and Sources of the Law*[50]. He argues that " in books of the Law, as in other books, and in common speech, 'person' is often used as meaning a human being, but the technical legal meaning of a 'person' is subject of legal rights and duties".[51] The bundle of rights and duties that accompanies legal personhood varies with the nature of the entity

[49] *David C.* Vladeck, *Machines With No Principles and Artificial Intelligence Liability rules*, at 148 .
[50] See JOHN CHIPMAN GREY, THE NATURE AND SOURCES OF THE LAW (Ronald Gray ed., MacMillan 1921) (1909).
[51] <http://www.independent.co.uk/life-style/gadgets-and-tech/news/saudi-arabia-robotsophia-citizenship-android-riyadh-citizen-passport-future-a8021601.html>.

exercising legal personhood. At this point, Gray offers us many examples about things that have possessed legal rights at various times in history. Temples in Rome and church buildings in the middle ages were subjects which granted legal rights. Gray further notes legal personhood is usually accompanied by the right to own property and the capacity to sue and be sued. The latter is extremely important and causes a lot of discussion among scholars, especially when it comes to criminal legal capacity. What I mean here is, how logical is it to punish a church, for example, or an artificial intelligence system if criminal capacity has been attributed to it by a human law? Even though criminal law is beyond the scope of this thesis, this example can help us understand the oxymoron in approaching the legal capacity of AI.

Hence, the greatest variety of rights and responsibilities are vested in natural persons, the most important category of legal person.[52] Jessica Berg argues that our society was developed by and for natural persons, and thus it is normal that legal rights focus on this group[53]. So, what does the concept of "natural persons" mean in depth and what characteristics does this category of legal persons possess?

When we are talking about "human" notion we essentially mean "natural person". These two notions are treated synonymously. The legal philosopher Frank van Dun, for example, indicated that "human beings are cited as the paradigmatic natural persons".[54] The key feature of a legal person is the ability to bear rights and duties and is commonly associated with human beings.[55] Things are going to become more complex however, as the artificial intelligent agents might have the ability "to act and speak for themselves" which, in the legal philosophers' view, is one of the main characteristics of a natural person.[56] Under this circumstance, should the concept of a natural person be restricted only to human persons or not?

---

[52] A. Dyschokant, "Legal Personhood: How We Are Getting it Wrong", "University of Illinois Law Review" 2015, (Vol.5, p.374).
[53] J. Berg, "Of Elephants and Embryos: A Proposed Framework for Legal Personhood" Hasting Law Journal, (Vol., p. 374).
[54] F. Van Dun, The Pure Theory of Natural Law, Part I, (2204), p.3
[55] Supra Note 52, p. 2076.
[56] Supra Note 54, p. 3.

Jessica Berg argues that, "to the extent that an entity matches the relevant characteristics of entities which have all the characteristics of persons -e.g. adult competent human beings- that entity should be afforded personhood protections because to do otherwise would both be inconsistent and would undermine the rights sought to be upheld"[57]. She also uses a comparison to slavery, analyzing that even though the Framers of the U.S. Constitution did not grant equal rights to the slaves as they did with other people, it was noticeable that between those two groups were existing significant similarities. The only difference was the skin color. Therefore, if we want to grant legal rights to non-human entities, we should search carefully for the similarity requirement, in order to avoid vast discrimination.

On the other hand, Frank van Dun reminds us again that "not all human beings are natural persons" and he adds that "some human beings are definitely and permanently incapable of functioning or acting as persons because of genetic condition, an accident or a debilitating disease".[58] However, when it comes to human fetuses and children, we should consider them as natural persons because of the fact that they will almost inevitably "develop their personal capabilities and become able to exercise them".[59] Of course, depending of their age, children have been given a set of rights. In a U.S. Supreme Court case, the judge had declared human fetus as legal person because of the same reasoning, "the potentiality of human life".[60] Regarding this matter though, national regulators are very cautious as only 9 states provide such legislation, which treats human fetuses the same as already born children.[61] If we want to categorize among different humans, we notice two alternative criteria of legal capacity: "whether an entity is a competent adult human or has significant similarity to him/her".[62] Children and human fetuses are considered to have these specific similarities.

---

[57] L. Solum, "Legal Personhood for Artificial Intelligences", North Carolina Law Review, (1192, vol.70).
[58] Supra note 54, p.4
[59] Id. P.5.
[60] Supra note 52, p.2082, citing Roe v. Wade (1973).
[61] Chile's Constitution of 1980 with Amendments through 2012, Chapter III, Article 19, paragraph 1: The law protects the life of those about to be born.
[62] Mindaugas Naucious: "Should fully autonomous artificial intelligence systems be granted legal capacity? p.118.

2.2 Legal Capacity of Judicial Persons

In contrast to "natural persons", the designation "juridical person" is used to describe an entity which does constitute a human being but at the same time society attributes some of the same legal rights and protections as to natural persons.[63] These types of entities are for example, corporations. But juridical persons may also be other inanimate things as well. More specifically, in Title 1, Section 1 of the U.S. Code, the notion of person includes -"corporations, companies, associations, firms, partnerships, societies, stock companies", etc.[64] Most of the jurisdictions of the world allow these type of entities to grant rights and responsibilities; in other words they grant legal capacity to these legal fictions.

While comparing the requirements to declare someone/or something as a human or juridical persons, we notice both similarities and differences. Of course, a juridical person is not a human being –even though it is created and operated by human beings. The scholar Dyschkant opines that "it is the capabilities of the human beings who control the corporation that actually constitute the personhood of the corporation".[65] Gray argues also that corporations are reducible to relations between the persons who own stocks in them and manage them.[66] When we call these types of entities as "person", we basically use fiction unless the entity possesses "intelligence" and "will". Juridical persons can own property, enter into contracts, sue and be sued and exercise both passive and active rights and responsibilities, except of course inherent human rights and responsibilities like the right and power to vote or enter into marriage. Tushar Kanti Saha states that the legal personality of a corporation was established to include five legal rights which are the

[63] Id. p. 120.
[64] Title 1, United States Code, § 1.
[65] Supra note 52, p.2084, 2085.
[66] John Chipman Gray: The Nature and Sources of the Law (Ronald Gray ed. MacMillan 1921).

following: the right to own property (including the right to a common treasury or chest), the right to a corporate seal (the right to make and sign contracts), the right to sue and be sued (the right to enforce contracts), the right to hire agents (and employees), and the right to make by-laws (self-governance).[67] However, juridical persons often relish limited liability. In practice that means that the owners are not liable for the debts of this entity. In any case, there are situations where the owners might be held liable. This occurs when the company breaches law and/or obligations. This is when we have what is called "piercing the corporate veil".[68]

2.3 Artificial Intelligence as Legal Agents

As I analyzed above, artificial intelligence is some activity which enables machines to act intelligently. Intelligence, on the other hand, is the quality that enables an entity to function appropriately.[69] Of course, this entity is created by humans and able to complete the given tasks while considering the environment around it. So, can autonomous machines be legally responsible for their actions? Based on Franklin's and Graessers' research, an autonomous machine can be reactive, self-controlling, goal-oriented, and temporally conscious. Stuart Russel and Peter Norvig endorse this argument. In their view, artificial intelligence is a way in making a computer, robot or even software act intelligently in a manner similar to humans. This is achievable by investigating how humans behave and trying to replicate those behaviors.[70] They are even able to communicate with other agents and adapt their behavior in line with previous experience.

[67] T. Kanti Saha, Textbook and Legal Methods, Legal Systems & Research, p. 79 (New Delhi: Universal Law Publishing Co, 2010).
[68] R. Thompson "Piercing the Corporate Veil: An Empirical Study", Cornell Law Review (1991 (Vol. 76, Issue 5), p.1036).
[69] N. Nillson, The Quest for Artificial Intelligence: a History of Ideas and Achievements p.13 (Cambridge, U.K.: Cambridge University Press, 2010).
[70] Mindaugas Naucious: "Should fully autonomous artificial intelligence systems be granted legal capacity?" p.122.

Basically, they can act in a way which gives an impression of the possession of individual character traits. In other words, they seem to possess, a “believable personality”.

By contrast, Nils Nillson states that AI in general does not need to possess the same, or even similar, intellectual capabilities as human beings. Moreover, AI does not need to communicate with humans or be independent from them[71].

There are two different views in relation to this matter: the ‘restrictivism’ and ‘permissivism’ approaches. In sum, the former denies the possibility of holding autonomous machines legally responsible for their actions while the latter argues the contrary. More specifically, the ‘permissivism’ approach imposes no restrictions on the possible legal liabilities and hence does not deny the responsibility of artificial autonomous agents. Both of these approaches have loopholes. While there is no other conceptual perception that is strictly humane, I will elaborate on the three different conceptualizations of human behavior: folk-psychological, scientific and legal.

The first concept argues that no matter how “intelligent” or “autonomous” machines are, they can never become legal persons and be legally responsible for their actions. This is based on the assertion that an AI cannot obtain the properties of the human being, such as intentionality, free will, autonomy or consciousness. These features seem to constitute the prerequisites of a legal and moral responsibility. No need to elaborate that a machine lacks all of these qualities, always though in a human perspective. On the other hand, through the permissivism spectrum, the law is a flexible tool, which is used to demarcate social interactions and apportion liability. From this point of view there is no obstacle to hold an autonomous machine responsible for its actions or even omissions. History of law has shown that this is possible. Some human beings, such as slaves in the past or children, are excluded from the pool of legal agents. At the same time, non human actors have been included in the pool, such as entities and corporations.

[71] Id. p.122

Hage J., in his study *Theoretical Foundations for the Responsibility of Autonomous Agents (2017),* rejects this concept on the grounds that humans made a "realistic mistake" in analyzing the legal concept. He observes that humans usually think of responsibility as requiring two things: intentionality and free will. According to Hage, this is a mistake. What we cannot conceive is that intention and free will are not "real things" but rather things we attribute to one another. We live and breathe inside a complex network of social interactions which is based on such attributions. Eventually, if intention and free will are not "real" phenomena but mere outcomes of our conceptual apparatus, then, they cannot constitute necessary conditions of legal responsibility. Hence, Hages' conclusion argues that there's nothing barring the ascription of responsibility to machines.

Restrictivism is based on an apparently mistaken ontological assumption while attributivism is more plausible and based on coherent social practice. But is it enough to make artificial agents legally responsible for their actions even if people tend to understand the actions of others in terms of intentions and free will? To what extent is that possible without having applied special tests determining whether AI has "real" intentions? Is the concept of legal responsibility so flexible that AI may be regarded as a legal agent?

Even if there are no conceptual limits to ascribing legal agency, it should be reasonable to attribute legal responsibility to anything or anyone which is not a human being. According to Hage, the attribution of legal responsibility to artificial agents should be justified only if its consequences are desirable. The reasoning here focuses on the avoidance of abuse of power and possible discrimination of the term. This danger is not a fiction, given our experience with legal persons such as corporations or international organizations. Bryson argues, following the same spirit, that while legal personhood is a fiction "the inherent characteristics of a thing are not determined of whether the [legal] system treats it as a legal person." Bryson et al. 2017". More specifically, he writes: "Trying to hold an electronic person to account, claimants would experience all the problems that have arisen in the past with novel legal persons. There almost inevitably

would arise asymmetries in particular legal systems, situations like that of the investor under investment treaties who can hold a respondent party to account but under the same treaties is not itself accountable." Id". What we identify here is that neither Hage nor Bryson believe that we should take under consideration conceptual barriers so as to not include autonomous artificial agents. They underline the need for the regulators to employ utilitarian criteria if eventually legal personhood is granted to anything, including machines.

On the other hand, Jessica Berg argues that the concept of "juridical personhood" can be used to grant particular rights to non-human animals. She states the following: "perhaps we should develop a system of lesser legal status for non-human animals. The fact that the law as it is currently written does not include nonhuman animals does not mean that it could be altered to recognize the rights of entities with varying moral status. Rather than do so by creating new categories <…> that is could be done with the concept of "'juridical personhood'".[72] In accordance with the professors' view, other non-human entities with a questionable morality, such as AI systems, could be categorized as "juridical persons", enjoying rights and responsibilities similar to other juridical persons without having rights which are inherent to human beings.

3. The concepts of Robots, Autonomous machines and IoT-Devises

3.1 The European legislative approach

[72] Supra Note 65.

The European Parliament Resolution of 16 February 2017 on Civil Law Rules on Robotics identified civil liabilities caused by robots as a 'crucial issue'.[73] The likelihood of damages caused by the actions of AI is real. Already there have been cases where the liability of a person is passed on to AI.[74] In front of this phenomenon, in 2012, the European Commission initiated a RoboLaw project with the main objective of investigating the ways in which bio-robotics flourishing (including AI) on the national and European legal system, challenging the existing legal regime and demanding a regulatory ground on which they can be developed and eventually launched. The final report "Guidelines on regulatory Robotics" addressed to the European Commission in order to establish a solid legal framework for the development of robotic technologies.

The European Commission submitted a proposal for a legislative instrument allocating the liability for harm caused by robots, either by their sole actions but also in relation to their interaction with humans. It is a matter of efficiency, transparency and consistency in the assurance of legal certainty for the benefit of citizens, consumers and businesses operating in EU. The European Parliament suggests a choice between two different approaches which are described as the "risk management" and "strict liability" approaches.[75] In order to maintain the strict liability rule, three elements are required in accordance to the Parliament namely: damage, a harmful functioning of the robot, and a causal link between the two.[76] Whether we refer to "harmful functioning" of a robot or autonomous system is equivalent to its malfunctioning *viz* in case of this scenario, it is said to focus on the individual who was able to minimize the risks and deal with possible negative impacts. I also analyzed how difficult it might be, especially as the technology grows, to find the person who carries this responsibility. After she found, another question arises. What will the requirements for finding a liability be?

[73] European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules of Robotics, P8_TA-PRVO(2017)0051, para 49.
[74] Eric J. Sinrod, "Perspective: Is GPS Liability Next?(CNETNEWS2008).
[75] Parliament (n3), P8_TA-PROV(2017)0051, para 53.
[76] Id, para 54.

The Commission, just a week before the adaptation of the above proposal, published its Communication on a European Data Economy[77] where it discussed liability issues with a view to IoT devises. While autonomous systems have been characterized as products rather than services, the existing framework of Directive 85/374/EEC on product liability[78] suffers many vacuums and uncertainties. What is more, there is a distinction between risk-generating and risk-management approaches, depending on whether the liability belongs to the party who initiated the risk or to the party who is in the best position to minimize the risk or avoid its realization altogether.[79]

3.2 The Responsible Parties and Liability Standards

There are various actors who are involved in the creation and the operation of autonomous systems and IoT-devices and it would be useful to sever them into two categories: the manufacturers and the users. The former group includes all actors who are taking part, usually businesses, in the development, design and production of autonomous systems, including software developers and programmers. The latter group comprises everyone who interacts with an autonomous machine or IoT device after its circulation to the market. A contractual agreement has always constituted an obvious tool for the re-allocation of the costs of liability within one of the groups. Already today, plenty of clauses are being used by the members of the group of manufacturers, especially in standard supply agreements, to allocate the costs of products recalls including other costs caused by defective components.[80]On the other hand, unlike other professionals, like lawyers,

[77] Communication of the Commission to the European Parliament, the Council, the European Economic. and Social Committee of the Regions " Building a European Data Economy" 10.01.2017 COM (2017) 9 final.
[78] Council Directive 85/374/EEC of July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210/29.
[79] Commission (n 9), COM (2017) 9 final, 15.
[80] Omri Ben Shahar & Schneider. "Auto Manufacturing Contracts", (2006) Rev. 953, 959-960.

engineers, doctors, courts have been unwilling to apply[81] to computer professionals the breach of malpractice[82] perhaps because of the lack of the license procedure for programmers.[83]

The same reasoning has been followed within the group of users, i.e. between the owners and operators. Using the paradigm of motor cars, it is notable that the keeper of the car is required to take out liability insurance under the applicable European Directives.[84] In case the car is rented to someone else, the cost of such insurance are shifted to the lessee-driver, as a component to the price he or she has to pay for the lease. The same can happen in case a business operates an IoT-machine in its production process. In the total price of the product manufactured by an IoT-machine, it will be included a component reflecting the expected costs of harm caused by the IoT-machine. There costs might be shifted within the group of entities that operate and enjoy the benefits from the use of the IoT devise. In the end though, the freedom of contracts is the norm through which all possible scenarios will be covered.

In sum, liability issues may arise under three scenarios: When a manufacturer and a costumer are connected by virtue of the sale of a product; when two parties are in direct contractual relationship; when the user relies on information supplied by the computer system.[85] The first scenario is contained negligence and strict liability under tort law and the third deals also with negligence. Negligence is the failure to use the care a reasonable person would use under similar circumstances[86]. In order to prevail on a negligence claim, the plaintiff must prove that there is "some reasonable connection between the act or omission of the defendant and the damage which the plaintiff has suffered".[87] As I will

[81] Chatlos Systems Inc. v. National Cash Register Corp. 479 F. Supp. 738 (D.N.J. 1979).
[82] W. Page Keeton et al, Prosser and Keeton on the Law of Torts ¶ 30 at 164-65 (5th ed. 1984).
[83] Susan Nycum, Liability for Malfunction of the Computer Program, 7 RUTGERS J. COMPUTERS, TECH & L. 1, 9 (1979).
[84] Art. 3 Directive 2009/103/EC of 16.09.2009 relating to insurance against civil liability in respect of the use of motor vehicles and the enforcement of the obligation to insure against such liability, OJ L 263/11.
[85] Raymond T. Nimmer, THE LAW OF COMPUTER TECHNOLOGY 5.16 at 5-59 (1985).
[86] BLACK'S LAW DICTIONARY 1032 (6th Edition 1990).
[87] Supra note 82 par. 41, at 263.

analyze below, in case of strict liability, the plaintiff does not require showing the defendant was negligent or at fault but rather the product was defective and unreasonably dangerous when used normally and in a foreseeable manner, and that defect caused plaintiff's damage or injury.[88]

4. The existing legal regime - Lack of direct legal regulation in the field of liability of damage

4.1. Article 12 of United Nations Convention on the Use of Electronic Communications in international contracts and AI-as-Tool in AI liability terms

Based on Article 12 of United Nations Convention on the Use of Electronic Communications in International Contracts, adopted in November 2005, contracts made by interactions with or between automated messaging systems are recognized as legal binding. More specifically, a contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied on the sole ground that no natural person reviewed or intervened in each action carried out by the automated machine or the resulting contract. An explanatory note by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts states that, as a general principle in Article 12, a person (whether a natural person or a legal entity) on whose behalf a computer was programmed should ultimately be responsible for any message generated by this machine.[89] The problem here is that neither national nor international law recognizes AI as a legal person. This is precisely the reason why some scholars raised the question of whether artificial agents should be recognized as legal persons. This is why the

[88] Restatement (Second) Of Torts § 402 (A) (1964).
[89] Ugo Pagallo, The Laws of Robots: Crimes, Contracts, and Torts, 98 (Springer 2013).

European Parliament is examinimg a special legal status for robots, i.e. their recognition as electronic persons.[90] If we seek for AI to be liable for its actions we should grant legal personhood to it.That means that while the tool (meaning AI) has no independent volition of its own, the above interpretation complies with the general rule that the person who is the principal of the tool is responsible for its results.[91]

Ugo Pagallo argues that strict liability in the field of contracts, rights and obligations established by AI have the tendency to be interpreted through the legal viewpoint defining robot as a tool. Consequently, the strict liability rules govern the behavior of that machine and bind the natural or legal person on whose behalf it acts.

4.2. National Tort Law as the Default System

Each Member State operates its own law of torts, in other words, the law of non-contractual liability. While it is impossible to undertake a comparative analysis of Member States' laws here, it can be stated with confidence that they share common principles.[92] Consequently, a general rule of liability for fault applies at the legal systems of all Member States. Thus, when due care and negligence lead to causing harm to another, or where a wrongdoer causes harm intentionally, this actor is liable to compensate the victim.

The general principle of fault-based liability applies when a set of fundamental interests of the person are harmed, i.e.life, health, bodily integrity, freedom of movement, and private property. This principle also covers harm done to the parties associated with the manufacture and the use of IoT-devises and robots. Hence, the Commissions' evaluation of Directive 85/374/EEC came to the conclusion that no fewer than 18 Member States are lacking rules on extra-contractual liability of service-providers must not be

[90] Parliament (n3), P8_TA-PROV(2017)0051, para 55.
[91] Pagallo at n. 77, 98.
[92] The Common European Law of Torts vol.1 (C.H. Beck, 1998) vol.2 (C.H. Beck, 2000).

taken literally.[93] It is true that many European legal regimes lack specific rules on extra-contractual liability protecting consumers from harm caused by defects of either software or services.[94] This obvious defect does not affect the applicability of the general rule of non-contractual liability, which can also be applied to providers of services, regardless the customer is a business or a consumer. What remains true is that there is a significant legal vacuum in many European legal systems towards service providers and premises liability on "defective" performance, rather than mere fault. Even if defective performance of service on the one hand and negligence in the carrying out of a service on the other have slight differences, it should be noted that fault-based liability applies to everyone involved in the manufacture and use of autonomous systems and IoT devices and its legal grounds come from the national legal systems of Member States.

4.3. The Products Liability Directive in EU and strict liability

Directive 85/374/EEC supplies European States a comprehensive framework for damages claims based on harm caused by products. In Article 2 of the Directive, these products are characterized as "movables". In order to claim compensation based on the Directive, there is no requirement that the victim demonstrate fault on the part of the manufacturer. The recitals of the Directive emphasize that under its provisions, the applicable regime is strict liability. Strict liability applies to "any product"[95] but it does not apply if the expert system is classified as a service.[96] Another important issue concerning when or whether strict liability applies in the AI context is determining whether the

[93] Commission Evaluation of 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, SWD (2018) 157 final, 51 .
[94] Commission (n 27), SWD (2018), 157 final, 5, emphasis added.
[95] Restatement (Second) of Torts § 402 (A) (1964).
[96] KEETON supra note 82, par. 99 at 695.

software was defective and thus unreasonably unsafe.[97] Liability without fault is based on the theory of risk. How is this connected with artificial intelligence? The theory is based on the fact that a person carries out activities that she or he cannot fully control; that is precisely what AI is, i.e. a specific object which can draw individual conclusions from gathered information and respond accordingly. So, the AI's activities are uncontrollable.[98] For this reason, AI meets the requirements for being considered a greater source of danger. Additionally, strict liability applies if a physical harm has occurred i.e. personal injury or property damage, from use of the product.[99] Hence, strict economic loss is not enough to establish liability.[100] In this case, it would be useful to employ the "deep pocket" theory which is met mainly in US. According to this theory, when a person is engaged in dangerous activities that are useful and profitable for the society, they should compensate for damage caused to society from the profit gained. Meaning, the producer or programmer, the person with "deep pocket" must guarantee his hazardous activities through the requirement of compulsory insurance of his civil liability.[101]

The concept of the defective product is defined in Art.6 of the Directive. In this particular article reasonable expectations regarding product safety and the circulation time of the product (Art. 6 (1 (c)) are described as two crucial factors required in the concept of defect. But, at important areas such as design defects and liability for failure to warm[102], the international comparative scholarship suggests that product liabilities regimes are co-extensive with fault-based liability.[103] Even in the event of a manufacturing defect, the Directive does not impose a pure form of strict liability, as it is developing for

[97] Supra note 95 par. 402 (A) (1964).
[98] Siri-in case of a virtual personal assistant.
[99] Nancy Birnbaum, Strict products liability and Computer software, 8, COMPUTER /L.J. at. 140.
[100] KEETON, supra note 82, at 140.
[101] Guido Calabresi, The Cost of Accidents: A Legal and Economic Analysis, 40-41 (Yale University Press 1970).
[102] Gert Bruggemeirt, Tort Law of the European Union (Wolters Kluwer 2015) para 306, 314; David G.Owen , Products Liability Law (3rd ed. West 2015) 315-334; Simon D. Whittaker, "The EEC Directive on Product Liability ´1985) 5 Yearbook of European Law, 234, 242-243.
[103] Gerhard Wagner "Robot Liability" p. 6.

example at the French doctrine of "Responsabilité de fait de choses" but rather a soft version of negligence liability.[104]

In sum, the Product Liability Directive does not cover the liability of all services providers and all efforts to supplement it with another legal instrument have failed so far in the AI context. However, it would be a mistake to conclude that service providers are exempt from extra-contractual liability. Service providers can be held liable through the diverse legal systems of the Member States, where fault-based liability is provided. Also, the responsibility of those actors that own, keep or operate a certain product remains subject to national liability regimes. The Commission proposal for a directive on the liability of service providers embraced the same principle of fault that has also been adopted by the jurisdictions of the Member States. As I elaborate above though, this approach probably is not the most suitable to apply to AI. Although no uniform European system of liability is applicable with regard to the "group" of owners, keepers and operators, I deem critical either the supplementation of the Product Liability regime or the creation of a new legal instrument in order to confront the problems which are about to emerge. David C. Vladech states that we should focus onto the creation of a new strict liability regime. In this way, "each entity within a set of interrelated legal persons may be held liable jointly and multiply for the actions of other entities that are part of the group".[105] Based on this liability, it would be enough for the persons involved to have worked towards a common end, such as designing, programming and manufacturing an AI without working jointly. This is happening because it is almost impossible to assign every aspect of wrongdoing to one party to another; it would be enough, in legal terms, to demonstrate all parties are responsible in wrong-doing.[106]

[104] Id. at 7.
[105] Paulius Cerka, Jurgita Grigiere, Gintare Sirbikyte, "Liability for Damages Caused by Artificial Intelligence".
[106] David C. Vladeck, "Machines Without Principles: Liability Rules and Artificial Intelligence", 89, Wash L.Rev. 117, 149 (2014).

5. Liability of the parties

5.1. The Shift from User Control to Manufacturer Control

It is reasonable to assume that AI technology will progressively lead to a shift of control away from users and towards manufacturers. Let us take automobiles for example. Manufacturers are responsible for determining the general design of the product, including its safety features, while the user is the one who uses the pedals, the steering wheels, etc; it is us the user who exercises control in real-world situations and determines the machines' behavior. Also, it is the user's responsibility to drive carefully and avoid impact with other cars. The manufacturers are not part of any accident scene. Continuing this example, autonomous cars will transform the user from a driver into a passenger. To the extent that manufacturers do or can exercise control, liability must also shift. This is obvious in cases where software cannot be altered by third parties, including the user, but only by the manufacturer.

When an object operates with hard- and software together, it represents the product or "movable" within the meaning of Article 2 of the Directive.[107] Thus, even if only the software was defective, in a case where AI causes harm, the manufacturer may be held liable because the Directive applies. The problems arise when software is distributed as a separate product from hardware. I already mentioned above the data/software libraries which have begun arising creating all over the world and can be bought and downloaded by an enterprise. In this case, there is no "movable" and, accordingly, the Directive may not be applicable. One solution is to operate with an expanded notion of "movable" that is neither real estate nor a service regardless of whether the object is tangible or intangible. Another option is to expand the interpretation of the concept of "movable"[108]

[107] Wagner, Munchner Kommentar Zum BGB vol. 6, 714-715. (7th ed., C.H. Beck 2017),
[108] Id., 717-718.

towards the digital products or to apply Art. 2 of the Directive by analogy in order to capture "quasi-things".[109] In Gerhard Wagneer's opinion, both options are problematic, while Art.2 is just giving some examples of the meaning of "movable". At the same time, Art.2 is listing, at its last sentence, electricity as a movable product, hence a corporate asset. The problem here is that we do not know if the law-makers included electricity explicitly or it was mentioned as an example of non-corporeal object. In that case, software would constitute an even better example than electricity itself.

5.2. The Concept of Defect

Although the Directive does not impose pure strict liability on manufacturers of movables, liability may be established if a product is defective. As I have already mentioned above, the concept of defect is defined in Art. 6 of the Directive and requires safety standards which a reasonable person is entitled to expect. This definition is quite vague. Even the provisions of the Consumers Rights Directive cannot ensure that current rules, i.e the right to receive essential information about the product or service, are enforceable. Under current Consumers' rules, "there is no obligation to inform the consumer about the relative importance of ranking parameters and why those criteria were chosen".[110] Consumers' expectations are often illusive or even lacking. Courts and commentators of products liability law in USA and Europe therefore have created the so called risk/utility test.[111]

Defectiveness can be found either in the area of so-called manufacturing or design defects. In order to have a demonstrable manufacturing defect, the product a manufacturer puts in circulation cannot fit the description of the manufacturer. There are various sources of program errors in conventional software and AI, i.e incorrect data

[109] Gerhard Wagner, "Robot Liability", p.11.
[110] BEUC Position Paper, The European Consumer Organization "Automated Decision Making and Artificial Intelligence- A Consumer Perspective".
[111] ECJ 21-12-2010, Case 495/10 para 39 (services are outside the scope of the Directive).

entry, hardware failure or electrical noise[112], or "bugs". Experts systems are subject to other errors, i.e. failure of the human expert to supply accurate and complete facts and rules[113]. Even though manufacturers have worked hard over the decades to minimize these manufacturing defects, it remains to be seen if digital appliances would be similarly successful.

While manufacturing defects are more identifiable, design defects are far more serious. If the layout of a product is found problematic, the court applies the risk/utility test. Under this specific test, the product is defective if the court, with the help of a technical expert, is able to identify an alternative software design which would have helped to avoid the accident in question. At the same time, the court examines whether the accident costs avoided by the better alternative design would have exceeded the added costs of the alternative design. In other words, the court should identify shortcomings of the software that could have been avoided by a better software program comparative to the one that led to the accident. The point is that the alternative software is exactly as good as the initial one but at the same time, is able to avoid the accident in question. If an autonomous system caused an accident which a reasonable human driver would have been able to avoid, the algorithm would be found defective in design. The critical point is that autonomous machines will not cause the kind of accidents that a reasonable driver would avoid.

There is no doubt that it is very difficult to develop a system which can identify the defect in a system and at the same time provide an improved algorithm. That means that under the "optimal algorithm test", the algorithm that causes an accident will always be found defective except for the safest of them all.[114] The outcome will be that only the manufacturer with the best algorithm would make it in the market while all the other would have to deal with immense costs of accidents caused by their products. As technology develops, fair competition in the technological product market will become

[112] Michael C. Gemignani, *More on the Use of Computers by Professionals 13.*
[113] Laurence H. Reece III, Defective Expert Systems Raise Personal Injury Liability Issues, NAT'L L.J. Oct 12, 1987 at 24.
[114] Wagner, 737-740.

fragile. A fair solution would be not to compare the performance of the algorithm involved in the accident with other algorithms operating in similar products.[115]

5.3. Burden of Proof for the Products Liability Directive

The European Commission's evaluation study on the Products Liability Directive reveals that the burden of proof poses serious difficulties for the victims in seeking compensation from manufacturers alleged to have created manufacturing or product defects.[116] The European Consumer Organization points out exactly the same issue, suggesting that the burden of proof is a key requirement for the enforcement of consumer rights, for example to invoke legal guarantee rights under the Sales Directive or to establish liability under the Product liability Directive.[117] More specifically, pursuant to Art. 4 of the Products Liability Directive, the person who suffers the injury is responsible for proving the defect, the damage, and the link between the two. As if it is not already hard enough for the injured person to establish the connection mentioned above after the use of a legacy product, image how difficult would that be in case of a digital product.[118] The sample of digital products in the market is yet too small to deduce safe results but it is justified enough to expect products even more complex than they previously were.[119] It will probably become very complicated to analyze and evaluate self-learning algorithms and complex operating systems. A different point of view could argue that digitalization offers the opportunity to extract storage information easier for the benefit of the victims. Even the initial opportunity to have access in these information constitutes strong argument whereas legacy product cannot offer it. The German Road Traffic Act already

[115] Supra Note 97, p.13.
[116] Commission (n27), SWD(2018) 157, 25-26.
[117] Supra Note 98.
[118] Jeffrey k. Gurney, "Sue my car not me: Products liability and accidents involving autonomous vehicle" (2013) 57, 61.
[119] Wagner, 747.

includes a right for victims of motor accidents to access the “black box” of a car which is driven autonomously (Section 63a (3) StVG).

There is no need to explain in exhaustive detail the importance of designing a legal regime whose main purpose is to ensure transparency and facilitate overcoming the obstacles the current regime poses to injured persons. Lawmakers should approach the matter rather cautiously. If they decide to sharpen the liability system, then this would probably create more problems rather than solving them. It is one of the virtues of legal systems and of the development of private law in general to let the system evolve on a case-by-case basis. An obvious disadvantage is the rather slow process of case-by-case adjudication while society is urging for easy solutions and early legislation. One solution would be to shift the burden of proof with regard to the requirement of defect, i.e. to reverse the Art. 4 Product Liability Directive to hold manufacturers liable in case of a defect (unless he proves that the product was not defective). Another option is to abandon the concept of defect and switch to a system of pure strict liability for autonomous systems and IoT-devices. Under such a system, the manufacturer of the autonomous system will always be the one responsible to compensate the injured person, unless the harm was caused through the fault of the victim. It sounds appropriate to abandon this system provided that the manufacturers shape the algorithm that determines and fully controls the “behavior” of the device. Alongside with a strict liability system, insurance companies are going to find space to grow.

5.4. Open and closed systems in autonomous machines

It is almost sure that the situation just described, where the manufacturer of an autonomous system fully controls its “behavior” would sustain dramatic changes. It is anticipated that there will be digital products whose hard- and software would remain closed to user interference. Where the user had acquired hard- and software separately,

and even from different suppliers, it may be difficult in the event of harm to establish liability for one of the parties, or to even try to allocate responsibility. Who was responsible for the mismatch that caused the accident when the user was not able to interfere at the autonomous machines' operation? Is the user who executed add-ons or alterations at the original software or is the initial programming of the software responsible for the accident? It remains innocent from the perspective of the liability system that the user added software that could not affect the program that operates the system, like i.e. entertainment software in an autonomous car. The crucial point is that the software that governs the safety features of the car or other device remains isolated from user interference. In this case, it is qualified as a closed system for purposes of product liability law.

The distinction between open and closed systems is of paramount importance with regard to manufacturer liability. Everything changes when hard- and software are manufactured by different suppliers and marked separately or the user is in a position to modify or supplement the safety features of the original software.[120] It is important for the liability system to provide incentives with regard all possible combinations while it would be unfair for the manufacturer to hold all responsibility.

Consequently, the characteristics of an autonomous system and IoT-device would be crucial with regard the responsible party in case of an accident. Everything mentioned above is concerned with hard- and software that remain closed to the user. For unbundled products, the proper solution is more complex. In theory, a remedy involving a combination of product liability for manufacturers of hard- and software and fault-based liability of users and third parties is viable.[121] The Product Liability Directive is providing exactly the same type of regime today. The Directive incentives are applicable not only to end-manufacturers but also to component suppliers of any layer (Art. 3 (1)), while users and third parties are liable for fault under national tort law. However, the current legal

[120] Supra Note 97, p.15.
[121] Id. P.15

system is based, as I mentioned before, in a very problematic burden of proof norm which poses serious obstacles towards recovery. The victim needs to prove who of the various actors involved in the accident does bears responsibility. In addition, the victim is the one who must investigate whether the accident was caused by defective hardware or software, taking into consideration the multiple combinations of the way the latter were manufactured, supplied, and check possible future alterations by someone apart the manufacturer. Under Art. 4 Product Liability Directive, if the court fails to identify the true cause of the accident, it is the victims' responsibility.

As a result, in case of an unbundled product, the responsibility must be allocated among various actors. It is not possible that, in most cases, only one party can be held entirely responsible for the damaged caused by the accident in question. Therefore, liability must be apportioned between all parties engaged with the device that caused the accident, at the time of the accident. Some scholars have already made a more entrepreneurial proposal in order to surpass the difficulties imposed by the complexity of the future products. They suggest that it would be a good idea to hold the system itself liable, in other words to create some form of "robot liability".

5.5. Liability of Users

It is impressive to notice that there is no European liability regime for users, not only with regard of autonomous systems but of any kind of product. Of course, they are still subject to the Member States' national tort law. As I've already mentioned, fault-based liability is the norm applicable to the legal reality of all Member States. Consequently, if the user misused or abused his or her autonomous machine in a way that harmed others, then he or she becomes answerable in damages. A simple example is when the user installs software subsequent to the purchase of the original system and this software is proved responsible for the accident. Again, in this case, the victim would find more

difficult to prove that it was the user the one who was responsible for the software malfunction beside the end manufacturer. Some legal systems have chosen to apply strict liability for harm caused in the operation of an installation, appliance or machine. This approach is mostly common in the category of motor cars.[122] Notably in UK, where fault-based liability is the norm, on the 19th of July 2018, the "Automated and Electric Vehicles Act" has been voted by the Parliament. Apart from other sections, it mainly focuses on the insurer's liability with regard to user's fair use. Pursuant to Part 1(4) possible unauthorized software alterations or failure to update software by the user, constitutes a reasonable right for the insurance policy to exclude or limit its' liability. France, on the other hand has created a system on mere involvement (implication) in a traffic accident.[123]

5.6. ePersons as "Liability Subjects"

Does it make sense, for the liability system to recognize autonomous software agents as legal entities who may be held liable in damages? I've already elaborate on the concept of legal capacity of natural and juridical persons (supra note Chapter 2). Apart from any further philosophical discussion, the obvious explanation is "no" while robots have no assets for paying off damages claims. If lawmakers use the analogy of the legal entities regime, victims would receive no compensation. In this context, all the actors "behind" the robot liability would be protected by the ePerson's liability. Besides, a corporation works as a shield against liability for the actors who created the entity, i.e. shareholders.[124] For shareholders this regime constitutes a shield in order not to lose more than the money they invested into the corporation.[125] In case of applying the principle of limited liability to ePersons, manufacturers and users of robots would be

[122] Cees Van Dam, European Tort Law (2nd ed. Oxford UP 2013), 408-420.
[123] Genevieve Helleringer & Anne Guedan-Lecuyer, Development of Traffic Liability in France.
[124] Frank H. Easterbook & Daniel R. Fischer, *The Economic Structure of Corporate Law 40-62 (Harvard UP 1991);* Stephen M. Bainbridge & M. Todd Henderson, *Limited Liability, 44-85*, *(Elgar 2016).*
[125] Id. Frank H. Easterbook & Daniel R. Fischer (69), 40.

exempt from liability as "they qualify as quasi-shareholders of the robot".[126] Then, no one of the actors would be liable as the "behavior" of the robot would no longer be ascribed to them. This outcome would be acceptable only if the new legal entity was capable of responding to this externalization of risk. It seems that under the proportion of ePerson liability no actor would be exposed to the equitable financial incentives as the harm caused to third parties would remain with the victims.[127]

However, in case of limited shareholder liability the corporation is not immune from liability. But robots however "intelligent" they might become, will never be able to respond to incentives generated by the liability system. Thus, potential ePersons are immune from financial incentives. This fact raises serious concerns with a view to deterrence, even if minimum asset requirements or insurance mandates apply. Therefore, advocates of ePersons propose similar remedies to the ones employed in corporate law. They argue that the law could require a minimum asset in order for the robot to qualify as a legal entity. These funds would then be held to the robot's name and be used to pay off damages claims. The essential point about entity status for robots is to shield manufacturers and users from liability. These actors should be protected from excessive liability. Corporate law can be used as a tool for the creation of a legal entity which will limit the exposure of individuals involved in the creation of the particular entity and thus, spur them to take on more risk at lower cost.[128]

An alternative option is the mandatory liability insurance. Lawmakers may mandate an insurance scheme as a precondition for incorporation of a robot as an ePerson.. It is very common for large business enterprises to use liability insurance even if the law doesn't require it. The main advantage of using insurance contracts as the preferable legal path of dealing with risk externalization is that the assets remain liquid and the victim's compensation is assured. Whatever tool would be chosen by the legal system, the crucial issue is as to who will be held liable to contribute. Again, natural and legal persons who

[126] Supra Note 109, p.21.
[127] Id. P.21
[128] Stephen M. Bainbridge & M. Todd Henderson (n.69) 2, 47-49, 69.

put the robot into circulation or operate it are responsible to prove the existence of the mandatory liability insurance. At any case, market insurance is usually more efficient than self-insurance. That means that solely through the spectrum of the liability system, mandatory liability insurance seems more attractive over minimum asset requirements.

Closing, the issue of limited liability should be addressed and discussed head-on and separately from the ePerson issue. The Article 16 (1) of Product Liability Directive provides a cap with regard to the liability of the manufacturer which is set to 70 million ECU. This is applicable also for the manufacturers of robots and the IoT-devices. On the other hand, the fault-based liability of users does not provide any fiscal limit.

Conclusions

In near future**,** autonomous machines will be capable to exercise activities that are still impossible for us to predict. As I have already analyzed in my thesis, artificial Intelligence is different from conventional computer algorithms while it constitute systems that are able to train themselves, store and accumulate experience. This ability is a unique feature that enables “AI” to act differently in the same situations, depending on its previous actions. Many experts argue that this progress stimulates to the brain’s activity processes.

The lack of direct legal regulation in the field of liability for damage caused by AI has created ground for many different legal approaches and theories to flourish. The main question is whether the problems posed by new technologies can be handled within the framework of the existing laws or humanity needs new, comprehensive legal framework to accompany the development in the area of artificial intelligence.

While international and national law does not recognize AI as a legal person yet, a question arises in the context of the legal relationship between AI and its developer. As I have elaborate above, legal norms provide that in case of damages, which had been caused by unlawful actions of another person, must be compensated. In Roman law but also in civil codes of various civil law tradition countries provide that damages have to be compensated by the offender or a person who is responsible for the actions of the offender. This is a crucial point while, if we recognize that "AI", as fully autonomous, is aware of its actions, then it must also be liable of its actions. AI's autonomy in law means that AI has rights and duties. Therefore, many scholars suggest ascribing legal personhood to AI in order to be liable for its actions. However, in my opinion, it would be very confusing to suggest that AI systems are capable of obtaining some of the characteristics only human beings can have and express, like motion, morality, free will and so on. There is a huge debate between scholars who believe that autonomous machines can be granted the status of legal agents and others argue that such an attribution would remain a mere "law in book" and never materializing as "law in action". The latter, examines the issue through a more descriptive and conceptual spectrum, whilst, legal personhood as a norm, would be able to establish a very useful law-creation tool, in the hands of a specialized government institution but also by the courts, with regard the allocation of responsibility among the parties involved in the creation, distribution and end-use of the autonomous machine. Already, in RobotLAW project (full title: Regulating Emerging Robotic Technologies in Europe: Robotics Facing Law and Ethics), funded by the European Commission, various crucial subjects were examined, *inter alia*, the possibility of attributing legal personhood to robots and expert systems. It is not an easy task considering that today's perspective does not allow us to examine how far the project of the artificial intelligence's might go while the amount of information the humanity possesses at present are not enough.

In any case, technological innovation cannot pause its evolution waiting for the law to find an ex post solution, calming down the societies' second thoughts and fears about this new era. For that reason, I strongly believe that an always wise option is the creation of a

regulatory regime for artificial intelligence. Taking into consideration all the legislature obstacle that I have analyzed in the Introduction and in previous Chapters of this thesis, the starting point for regulating AI should focus on the fact that we need laws that control and direct human beings, who create, design and employ expert machines, AI agents and algorithms. While addressing this issue, scholars and society should avoid the *homunculus fallacy*[129].

We should keep in mind that while algorithms without data are useless, these laws should also take into account the methods used by the parties mentioned above, for the collection, collation, use, distribution and sale of the data that eventually, make these algorithms work. Europe with its General Data Protection Regulation (GDPR 2018) leads globally towards this direction. Taken together, an Artificial Intelligence Regulation or Act for example should define, apart from its general principles, provisions about the humans who make and use robots and the data that robots use. We should keep in mind that people use algorithms to classify and govern populations of people. The configured relationship is one of the governance, and the obligations are fiduciary –of good faith, non-manipulation and non-domination.

In the Algorithmic Society, the way of governing populations will involve relationships of informational power. What we notice is that there is an asymmetry of power and an asymmetry of information between operators and those acted on or governed. There is an asymmetry of knowledge and of power between the public and the private governors and those who are governed by them. Fiduciaries have two central duties, the duty of care[130] and the duty of loyalty and are people like lawyers, doctors, engineers who also work under a license.[131] When fiduciaries collect and process information about their clients, they suggest information fiduciaries.[132] Large online businesses like Google, Facebook and

[129] It is a phrase used tp describe what people tend to think about robots, AI agents and algorithms. In other words they believe that there is a little person inside the program who is making it work, it has intentions, good or bad.
[130] Id. At 1207-08.
[131] Id. At 1208.
[132] Id. At 1208.

Uber constitute information fiduciaries; hence, they should be trustworthy towards their end users. Apart from possible constitutional issues, States should focus that it is not the robot or the expert system responsible for any kind of maltreatment or damage toward the user or a third party, but it is the companies behind the expert systems. For that reason, current law does not and possibly, fairly, treat these digital businesses like fiduciaries while these huge companies that employ algorithms in their operations may still cause harm to people who are not their clients or customers and with whom they have no contractual obligation.

As we are referring to "AI" mainly as a product, consumer law is vital. European's Consumer Organization Position Paper and its policy recommendations approached the matter in another way.[133]More specifically, according to ECO, artificial intelligence must be developed and used in full respect of EU data protection rules and the principals of fairness, transparency, purpose limitation, data minimization, accountability and privacy by design. In order to tackle global asymmetry of information and cover the liability matter, it is essential to inject much more transparency into AI systems and processes. Before courts, and with regard the legal regime which exist nowadays, asymmetry of information is a huge obstacle for consumers and their effort to overcome the burden of proof regime.

On the other hand, tort law constitutes a mode of indirect regulation and its strengths and weaknesses are developed at a case-by-case basis on which the tort system mainly operates. Tort systems employ a wide variety of legal standards and influence future behavior. But while tort cases are brought only under ex post situations, meaning, after the harm has occurred, courts have a limited liability to be proactive. As a result, in a tort case, the courts tend to focus on the procedural and evidentiary rules in order to verify the specific facts that led to harm in that specific case. The ex post nature of tort system suggests that the legal regime develops quite slowly, a fact that would create legal uncertainty in an algorithmic society. I believe that on specific cases tort law solution

[133] Supra note 110.

continues to constitute the best possible solution. Courts are well equipped and will gradually familiarize with cases arising from specific past and possible harms artificial intelligence might caused or provoked.

In my opinion, we can't deny legal personhood to artificial intelligence but we should use this legal tool only to certain and very complex legal relationships whereas gradually humans would intervene less and less between the user and the expert machine. In any case, time will show us problematic areas of law that right now are either blur or even impossible to predict. A new era is ahead of us and almost all domain of law will be affected while at the same time, new opportunities for research will appear for researchers and scholars.

Bibliography

1. Aaron Smith & Janna Anderson, *AI, Robotics, and the Future of Jobs*.
2. Andrew Culclasure, "Using Neural Networks to Provide Local Weather Forecasts" (master's thesis, Georgia Southern University, 2013).
3. Andrew Tutt, "An FDA for Algorithms," *Administrative Law Review* 69, no. 1 (2017).
4. Andy Kessler, "Siri, Am I About to Have a Heart Attack?," *Wall Street Journal*, January 9, 2017.
5. Art. 3 Directive 2009/103/EC of 16.09.2009 relating to insurance against civil liability in respect of the use of motor vehicles and the enforcement of the obligation to insure against such liability, OJ L 263/11.
6. *Artificial Intelligence: Rise of the Machines*, ECONOMIST (May 9, 2015), http://www.economist.com/news/briefing/21650526-artificial-intelligence-scarespeopleexcessively- so-rise-machines [https://perma.cc/B2LD-B4XS].
7. Avi Goldfarb and Catherine Tucker, "Privacy and Innovation," in *Innovation Policy and the Economy*, vol. 12, ed. Josh Lerner and Scott Stern (Chicago: University of Chicago Press, 2012).
8. BEUC Position Paper, The European Consumer Organization "Automated Decision Making and Artificial Intelligence- A Consumer Perspective".
9. BLACK'S LAW DICTIONARY 1032 (6th Edition 1990).
10. Bob Violino, Big data and robotics: A long history together, ZDNet, August 12, 2016, at http://www.zdnet.com/article/big-data-and-robotics-a-long-history-together/
11. Carol Woody & Robert J. Ellison, *Supply-Chain Risk Management: Incorporating Security into Software Development*, DEP'T OF HOMELAND SEC. (Mar. 15, 2010), https://buildsecurityin.uscert.gov/articles/bestpractices/acquisition/supplychainriskmanagement%3A-incorporating-security-into-software-development [https://perma.cc/UV6U-X64C].
12. Cees Van Dam, European Tort Law (2nd ed. Oxford UP 2013), 408-420.

13. *Cf.* WALLACH & ALLEN "*Moral Machines: Teaching Robots right from wrong (2009)* at 198.
14. Chatlos Systems Inc. v. National Cash Register Corp. 479 F. Supp. 738.
15. Chen et al.,"Global Economic Impacts."
16. Chile's Constitution of 1980 with Amendments through 2012, Chapter III, Article 19, paragraph 1: The law protects the life of those about to be born.
17. Commission (n 9), COM (2017) 9 final, 15.
18. Commission Evaluation of 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, SWD (2018) 157 final, 51 .
19. Communication of the commission to the European Parliament, the Council, the European Economic. and Social Committee of the Regions " Building a European Data Economy" 10.01.2017 COM (2017) 9 final.
20. Competencies, and Strategies," *Harvard Journal of Law and Technology* 29, no. 2 (2016): 393–97.DC, September 2014).
21. Council Directive 85/374/EEC of July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210/29.
22. David C. Vladeck, "Machines without Principals: Liability Rules and Artificial Intelligence", (2014) 89, Wash L.Rev. 117, 149.
23. *David C.* Vladeck, *Machines With No Principles and Artificial Intelligence Liability rules*, at 148 .
24. Davies M, Stone T (eds) (1995) Folk psychology: the theory of mind debate. Blackwell, Oxford
25. Dennett D (2008) The philosophical lexicon. http://www.philosophicallexicon.com. Accessed 12 Apr. 2017
26. Derek Khanna, "The Law That Gave Us the Modern Internet—and the Campaign to Kill It," *Atlantic*, September 12, 2013.

27. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,
28. ECJ 21-12-2010, Case 495/10 para 39 (services are outside the scope of the Directive).
29. Eric J. Sinrod, “Perspective: Is GPS Liability Next?(CNETNEWS2008).
30. European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules of Robotics, P8_TA-PRVO(2017)0051, para 49.
31. F. Van Dun, the Pure Theory of natural Law, Part I, (2204), p.3 (2015).
32. Fischer JM, Ravizza M (2000) Responsibility and control: a theory of moral responsibility. Cambridge University Press, Cambridge
33. Frank H. Easterbook & Daniel R. Fischer, *The Economic Structure of Corporate Law (Harvard UP 1991) 40-62;* Stephen M. Bainbridge & M. Todd Henderson, *Limited Liability (Elgar 2016), 44-85*.
34. Genevieve Helleringer & Anne Guedan-Lecuyer, Development of Traffic Liability in France.
35. Gert Bruggemeirt, Tort Law of the European Union (Wolters Kluwer 2015) para 306, 314; David G.Owen , Products Liability Law (3rd ed. West 2015) 315-334; Simon D. Whittaker, “The EEC Directive on Product Liability ´1985) 5 Yearbook of European Law, 234, 242-243.
36. Gitta Rohling, “Facts and Forecasts: Boom for Learning Systems,” Innovations newsletter (Siemens), October 1, 2014
37. Guido Calabresi, The Cost of Accidents: A Legal and Economic Analysis (Yale University Press 1970) 40-41.
38. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN
39. Humanoid Robot (IJHR) World Sci 3(3):393–412.
40. Hutchison A (2014) The Whanganui river as a legal person. Altern Law J 39(3):179–182.

41. IMMANUEL KANT, CRITIQUE OF PURE REASON 193-94 [A51/B76] (Paul Guyer & Allen W. Wood eds., trans., Cambridge University Press 1998)
42. J. Berg "Of Elephants and Embryos: A proposed framework for Legal Personhood" Hasting Law Journal, p. 374.
43. Jack M. Balkin, "The Three Laws of Robotics in the Age of Big Data"
44. Jack M. Balkin, Information Fiduciaries and the First Amendment, 49, U.C. DAVIS L. REV. at 1207-1208 (2015)
45. James Manyika et al., *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy* (San Francisco: McKinsey Global Institute, May 2013).
46. Jeffrey k. Gurney, "Sue my car not me: Products liability and accidents involving autonomous vehicle" (2013) 57, 61.
47. John Chipman Gray: The Nature and sources of the law (Ronald Gray ed. MacMillan 1921).
48. JOHN CHIPMAN GREY, THE NATURE AND SOURCES OF THE LAW (Ronald Gray ed., MacMillan 1921) (1909).
49. John McCarthy, What is Artificial Intelligence?, JOHN MCCARTHY'S HOME PAGE 2–3 (Nov. 12, 2007), http://www-formal.stanford.edu/jmc/whatisai.pdf [https://perma.cc/U3RT-Q7JK].
50. Josh Lerner, "The Impact of Privacy Policy Changes on Venture Capital Investment in Online Advertising Companies" (White Paper for the Analysis Group, Menlo Park, CA, 2012).
51. Kelsen H (1945) General theory of law and state. Harvard University Press, Cambridge
52. L. Solum, "Legal Personhood for Artificial Intelligences", North Carolina Law Review, (1192, vol.70).
53. Laurence H. Reece III, Defective Expert Systems Raise Personal Injury Liability Issues, NAT'L L.J. Oct 12, 1987 at 24.
54. Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges,

55. Michael C. Gemignani, *More on the Use of Computers by Professionals 13.*

56. Mindaugas Naucious: "Should fully autonomous artificial intelligence systems be granted legal capacity? p.118.

57. Mindaugas Naucious: "Should fully autonomous artificial intelligence systems be granted legal capacity? p.122.

58. N. Nillson, The Quest fot Artificial Intelligence: a history of Ideas and Achievements p.13 (Cambridge, U.K.: Cambridge University Press, 2010).

59. Neil Johnson et al., *Abrupt Rise of New Machine Ecology Beyond Human Response Time*, SCI. REPORTS, Sept. 11, 2013, at 1, 2; Aaron Kessler: Law Left Behind as Hand Free Cars Cruise (May 3, 2015).

60. NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 196 (2014).

61. Nils Pratley, *The Trillion-Dollar Questions over the Flash Crash and the Hound of Hounslow*, GUARDIAN (Apr. 25, 2015, 11:00 AM), http://www.theguardian.com/ business/2015/apr/25/flash-crash-hound-of-hounslow-trillion-dollar-question [https://perma.cc/88QE-5FR4].

62. O'Connor T (2010) Free will. The stanford encyclopedia of philosophy. https://plato.stanford.edu/entries/freewill. Accessed 12 Apr 2017

63. Okita SY, Schwartz DL (2006) Young children'sunderstanding of animacy and entertainment robots. Int.

64. Omri Ben Shahar & Schneider. "Auto Manufacturing Contracts" (2006) Rev. 953, 959-960.

65. Parliament (n3), P8_TA-PROV(2017)0051, para 53.

66. Paulius Cerka, Jurgita Grigiere, Gintare Sirbikyte, "liability for damages caused by artificial intelligence".

67. Pei Wang, *The Risk and Safety of AI*, A GENERAL THEORY OF INTELLIGENCE, https://sites.google.com/site/narswang/EBook/topic-list/the-risk-and-safety-of-ai

68. Pound R (1910) Law in books and law in action. Am Law Rev 44:12–36.

69. R. Thompson "Piercing the Corporate Veil: An Empirical Study" , Cornell Law Review (1991 vol 76, Issue 5), p.1036.

70. *Rayan* Calo,Robotics and the Lessons of Cyber Law, 103, Calif L. Rev. at 534.

71. RAYMOND T.NIMMER, THE LAW OF COMPUTER TECHNOLOGY 5.16 at 5-59 (1985).

72. Regulating Artificial Intelligent Systems/ Harvard journal of Law & Technology Spring 2016/p.367.

73. Regulating Artificial Intelligent Systems/ Harvard journal of Law & Technology Spring 2016/p.368.

74. RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIABILITY §§ 10–17 ("Liability of Multiple Tortfeasors for Indivisible Harm"); *id.* §§ 22–23 ("Contribution and Indemnity"); Calo, *supra* note 11, at 554–55; Balkin, *supra* note 49, at 53.

75. Robert B.K. Dewar, *COTS Software in Critical Systems: The Case for Freely Licensed Open Source Software*, MILITARY EMBEDDED SYSTEMS (Dec. 9, 2010), http://mil-embedded.com/articles/cots-open-source-software/ [https://perma.cc/T5G5-PXAB].

76. Ryan Calo, "The Case for a Federal Robotics Commission" (Brookings Institution, Washington,

77. Scherer, "Regulating Artificial Intelligence Systems," 394.

78. *See* Andrew H. Beck et al., *Systematic Analysis of Breast Cancer Morphology Uncovers Stromal Features Associated with Survival*, SCI. TRANSLATIONAL MED., Nov. 9, 2011, at 1, 8.

79. Sparrow R (2007) Killer Robots. J Appl Philos 24(1):62–77

80. Stephen M. Omohundro, The Basic AI Drives, in ARTIFICIAL GENERAL INTELLIGENCE 2008 483, 483 (2008).

81. Stich S (1983) from folk psychology to cognitive science. MIT Press, Cambridge

82. Stich S, Ravenscroft I (1992) What is folk psychology? Cognition 50:447–468.

83. Summers RS (2006) Form and function in a legal system: a general study. Cambridge University Press, Cambridge.

84. Susan Nycum, Liability for Malfunction of the Computer Program, 7 RUTGERS J. COMPUTERS, TECH & L. 1, 9 (1979).

85. T. Kanti Saha, Textbook and Legal Methods, Legal Systems & Research, p. 79 (New Delhi: Universal Law Publishing Co, 2010).

86. Tal Z. Zarsky, "The Privacy-Innovation Conundrum," *Lewis and Clark Law Review* 19, no. 1.

87. THE AMERICAN HERITAGE DICTIONARY and MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY both direct readers to the entry for "intention" for a list of synonyms of "goal." *Goal*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2000); *Goal*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2003).

88. The Common European Law of Torts vol.1 (C.H. Beck, 1998) vol.2 (C.H. Beck, 2000).

89. Ugo Pagallo, The laws of robots: crimes, contracts, and torts (Springer 2013) 98.

90. United States Code Art.1 "Words denoting number, gender, and so forth".

91. W. Page Keeton ET AL, Prosser and Keeton on the Law of Torts par. 30 at 164-65 (5th ed. 1984).

92. Wagner in: Munchner kommentar zum BGB vol. 6 (7th ed., C.H. Beck 2017), 714-715.

93. White House, *Framework for Global Electronic Commerce*.

94. Yves Eudes, *The Journalists Who Never Sleep*, GUARDIAN (Sept. 12, 2014, 6:17 AM), http://www.theguardian.com/technology/2014/sep/12/artificial-intelligence datajournalism-media [https://perma.cc/CES7-X58C].