MYKOLAS ROMERIS UNIVERSITY
FACULTY OF LAW
INSTITUTE OF INTERNATIONAL AND EUROPEAN UNION LAW

ARNAS AIDUKAS
(INTERNATIONAL LAW)

DATA PRIVACY AND ARTIFICIAL INTELLIGENCE: IS THE GENERAL DATA PROTECTION REGULATION THE RIGHT REGULATION IN THE AGE OF INTELLIGENT MACHINES?

Master Thesis

Supervisor –
Doc. Dr.
Laurynas Biekša

Vilnius, 2018

TABLE OF CONTENTS

INTRODUCTION

"It's going to be interesting to see how society deals with artificial intelligence, but it will definitely be cool."

Colin Angle[1]

The relevance and problems of this topic. When in autumn of 2015, the software called AlphaGo became the first computer to beat a professional human player in the Chinese cardboard game "Go", the world stood in awe and surprise. Even though, the notion, that artificial intelligence system could beat humans in many famous games was not new, as another artificial intelligence system called Deep Blue already in 1997 beat Garry Kasparov in a game of chess. However, this time was different.

The game of "Go" has simple rules, but is highly intuitive and complex in practice[2]. Therefore, the AlphaGo needed to use capabilities far beyond conventional computing powers, such as extremely accurate image, pattern recognition and insight, the skills, that we thought only humans posses[3]. The broader public was exposed to the reality and fast development of the artificial intelligence industry.

Calls for regulating artificial intelligence industry was starting to be heard. However, these calls were met with limited reaction from regulators and legal scholars alike. Part of the reason of this radio silence was that traditional methods of regulation - such as product licensing, research and development oversight, and tort liability seem particularly unsuited to manage the risks associated with intelligent machines[4]. Thus today artificial intelligence is still regulated by broader legal acts and regulation specific to artificial intelligence has yet to see the light of day.

This is especially troubling when you consider challenges, that artificial intelligence poses to data privacy around the world. Today, artificial intelligence pattern recognition abilities, which allows artificial intelligence to find correlations and insights are unparalleled and exceeds

---

[1] The co-founder of iRobot Corporation.

[2] Steven Borowiec, "AlphaGo beats Lee Se6dol in third consecutive Go game," *The Guardian,* March 12, 2016, https://www.theguardian.com/technology/2016/mar/12/alphago-beats-lee-sedol-in-third-consecutive-go-game

[3] Gonenc Gurkaynak, Ilay Yilmaz and Gunes Haksever, "Stifling artificial intelligence: Human perils," *Computer Law & Security Review: The International Journal of Technology Law and Practice* 32, 5 (2016): p. 1, https://www.researchgate.net/publication/303782217_Stifling_artificial_intelligence_Human_perils

[4] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", *Harvard Journal of Law and Technology* 29, 2 (2016): p. 356, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609777

human abilities in many instances. For example, artificial intelligence can using a supermarket shopping database determine a person's current and future health status with a degree of accuracy comparable to that of a medical examination[5]. This capacity of artificial intelligence to recognize patterns threatens to destroy the boundary between private and public information[6]. Recent scandal regarding Cambridge Analytica and their alleged use of personal data to influence political processes around the world and in Europe, just magnified this problem.

However, despite these problems, artificial intelligence industry holds potential to greatly benefit society by making decision making process much fairer and substantially improve healthcare systems all around the world. For example, artificial intelligence system such as Watson already is helping doctors to more efficiently diagnose diseases[7].

Thus, any good data privacy regulation needs to strike a right regulatory balance between protection of privacy and development of artificial intelligence industry. Only this way the society will rip the most benefits from this emerging and constantly improving technology. Therefore, there is a need for a serious debate about the current data privacy laws and whether they strike right regulatory balance.

This Master Thesis will attempt to do just that. By evaluating the most comprehensible data privacy regulation in the world - the General Data Privacy Regulation[8] - the author will try to settle the debate and answer the question - is General Data Privacy Regulation the right regulation in the age of intelligent machines.

The novelty of Master Thesis. Very few articles or books have been written in regards to artificial intelligence and General Data Privacy Regulation. Therefore, there is a lack of legal papers on this subject and, in this author's opinion, there is a clear need for comprehensive comparison.

Furthermore, not many attempts were made to provide a legal definition and elements of artificial intelligence for data privacy regulators. Another novelty of this Master Thesis will be

---

[5] Antoinette Rouvroy, ""Of Data and Men"". Fundamental Rights and Freedoms in a World of Big Data," Council of Europe, Directorate General of Human Rights and Rule of Law, T-PD-BUR(2015)09REV, 2016, p. 27, http://works.bepress.com/antoinette_rouvroy/64/

[6] Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap," *U.C. Davis Law Review* 51(2) (2017): p. 420-421, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/davlr51&div=18&start_page=399&collection=journals&set_as_cursor=0&men_tab=srchresults#

[7] Alfred NG, "IBM's Watson gives proper diagnosis for Japanese leukemia patient after doctors were stumped for months," *The New York Daily News*, August 07, 2016, http://www.nydailynews.com/news/world/ibm-watson-proper-diagnosis-doctors-stumped-article-1.2741857

[8] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," O.J.L (119) 46 (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

the recommendations or suggestions on how to improve each relevant article of General Data Protection Regulation.

Lastly, it is important to mention, that there is almost no case law regarding artificial intelligence technology and data privacy in Europe, therefore it is not clear how General Data Protection Regulation will be interpreted by courts and regulators.

The significance of this thesis. The General Data Privacy Regulation will become the main data privacy document in Europe and will set the rules of data privacy for many years to come. Therefore, careful scrutiny of this document is necessary, especially in regards to quickly developing technologies such as artificial intelligence. Hopefully, this Master Thesis will offer comprehensible analysis and provide necessary foundation for future discussions on this subject.

The object of this thesis. The object of this Master Thesis is the General Data Protection Regulation and artificial intelligence technology. It is important to note, that the scope of this Master Thesis will not include public sector or government surveillance and will only focus on private sector as the author is trying to determine the impact of General Data Protection Regulation to artificial intelligence industry and technology.

The aim of this thesis. To determine whether General Data Protection Regulation is a good regulation for data privacy in the age of intelligent machines. This purpose will be achieved in three steps: 1) determining what is artificial intelligence, 2) providing criteria for what is considered a good regulation, 3) evaluating articles of General Data Protection Regulation in order to decide whether General Data Protection Regulation meets the criteria for good regulation and is a good regulation for regulating artificial intelligence technology.

Tasks of this paper:

Crystallize the notion of artificial intelligence.

Determine the elements and symphony of artificial intelligence.

Analyze what kind of regulation could be considered as good regulation and determine criteria for evaluating regulations.

Analyze the challenges for regulators, who want to regulate data privacy in the era of artificial intelligence.

Analyze specific articles of General Data Protection Regulation to determine their compatibility with artificial intelligence technology and industry.

Provide conclusion as to whether the General Data Protection Regulation is proper regulation in regulating data privacy in the age of intelligent machines and determine the reasons for such a conclusion.

Formulate recommendations for improving General Data Protection Regulation or data protection system in general.

The defense statement. General Data Protection Regulation is not a proper regulation for protecting data privacy in the era of artificial intelligence.

The structure of the thesis: This Master Thesis will be divided into five chapters with separate subchapters and conclusions.

The first chapter analyses the notion of artificial intelligence, determines the elements of artificial intelligence, introduces historical development of artificial intelligence and provides some examples of legal documents designed to regulate artificial intelligence.

The second chapter determines what is considered a good regulation and provides the criteria for evaluating whether regulation is a good regulation. Also, this chapter addresses the challenges, that regulators face when trying to regulate data privacy in the age of artificial intelligence.

The third chapter will analyze specific articles of General Data Protection Regulation to determine compatibility between each specific article and artificial intelligence technology. Every subchapter of this chapter will address the scope of relevant article, challenges associated with artificial intelligence and some possible solutions.

The fourth chapter will determine conclusion as to whether General Data Protection Regulation is proper regulation for the artificial intelligence era and reasons for such a conclusion.

The fifth chapter will consist of possible recommendations for helping regulators solve the challenges associated with artificial intelligence.

Research methods:

Linguistic method was used in order to understand different notions such as “artificial intelligence”, “envisaged and significant consequences” and etc.

Analytical method was applied to divide the thesis into chapters in order to better understand separate chapters and then the synthesis was used to provide more generalized conclusions. Analytical method was also used to determine whether separate provisions of General Data Protection Regulation are compatible with artificial intelligence technology.

Critical method was used to determine whether General Data Protection Regulation is a good regulation for artificial intelligence technology and data privacy.

Analysis of scientific literature was applied then evaluating scientific literature, opinions of international legal scholars and problematic aspects of the topic.

Description method was used in order to present the scope of different articles and the elements of artificial intelligence.

Historical method was used to determine the scope of articles of General Data Protection Regulation.

Logical method was used to find common elements and links between various articles and documents with the help of induction, deduction and other logical operations.

Sociological methods were used to analyze the development of artificial intelligence and possible impacts of legal rules to actual society.

LIST OF ABBREVIATIONS

AI	Artificial intelligence
Article 29 Working Party	Article 29 Data Protection Working Party
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

1. CRASH COURSE ON AI

AI technology has truly embedded almost every aspect of our society. We have self-driving cars, computers, that can beat humans in chess and personal assistants such as Apple's Siri or Amazon's Alexa, which helps to make our lives easier and more comfortable. What is more, AI technology is helping many business around the world to be more cost efficient and provide better quality products to the consumer.

However, despite the common use of AI technology in both our daily lives and in business sector, the AI itself is still egzotic and rather foreign concept, which is difficult to grasp if you are not a researcher or a student in one of many AI fields. The often used terms in mainstream media, such as machine learning, neural network, narrow AI and others, are still beyond the understanding of average citizen and need to be explained in order to truly grasp the technology that is changing the world right now.

Therefore, this chapter will be devoted to looking behind the curtain of the notion AI to reveal elements of AI technology and understand it's correlation/relationship with the law. In first subchapter, the author will define the AI and describe the so called symphony of AI technology. In second subchapter, the history of AI will be discussed with special attention to different concepts, which developed through the years and now are widely used in contemporary AI systems. In third subchapter, impacts of AI technology will be discussed to show how many fields are encompassed by AI systems and to provide what might the future hold for this powerful technology and society in general. The fourth subchapter, will determine the current relationship between AI and the law.

1.1. Definition of AI and AI Symphony

Unfortunately, there is no widely accepted definition of AI even among experts of this field, much less a useful working definition for the purposes of regulation[9].

Dictionary defines AI as a theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision making, and translation between languages[10]. To put in simple terms AI is usually

[9] Scherer, *supra* note, p. 359

[10] Oxford English Living Dictionaries, „Artificial intelligence", https://en.oxforddictionaries.com/definition/artificial_intelligence

defined as the science of making computers do things that require intelligence when done by human[11].

Another definition of AI, which is widely used, defines AI as "*activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment.*"[12]

Some authors took a different turn and tried to provide not one definition of AI but several. For example, Stuart J. Russell and Peter Norvig summarized as many as eight definitions of Al differentiated by how they mirrored the expectations of human reasoning and behavior or by how they were able to rationally think and behave[13]. Other authors, on the contrary disputed the notion AI and offered to call these systems algorithm intelligence[14].

However, neither aforementioned notions of AI, which are rather vague and not very informative, nor many definitions of AI are helpful for this Master Thesis. Therefore, we need to define AI in workable terms. A good workable definition should have sharp boundary, should be faithful to the notion to be clarified, should lead to fruitful research and should be as simple as possible[15].

Therefore, better working definition would be the one suggested by Pei Wang, as she described AI as intelligence with adaption with insufficient knowledge and resources, which implies what such a system is finite, works in real-time, is open to novel tasks, learn from experiences and can achieve goals, which are different from traditional computer systems[16]. This definition will be used across this Master Thesis and will form the basis of this research.

One important thing to mention is term AI usually encompasses few different types of AI: narrow AI (sometimes called weak AI), strong AI and superintelligent AI.

Narrow or weak AI refers to AI that performs a useful and specific function that once required human intelligence to perform, and does so at human levels or better, and often these narrow AI systems greatly exceed the speed of humans, as well as provide the ability to manage

---

[11] Jack Copeland, "What is Artificial Intelligence?," Reference Articles on Turing, 2000, http://www.alanturing.net/turing_archive/pages/reference%20articles/what%20is%20ai.html

[12] Nils J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements,* (Cambridge, UK: Cambridge University Press, 2010), p. 13, https://ai.stanford.edu/~nilsson/QAI/qai.pdf
Rodney Brooks et al., "Artificial Intelligence and Life in 2030," One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA, September 2016. http://ai100.stanford.edu/2016-report.

[13] Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, (New Jersey, USA: Prestine Hall 2010), p. 1-5, https://www.pdfdrive.net/artificial-intelligence-a-modern-approach-3rd-edition-d32618455.html

[14] Stephen Mason, "Artificial intelligence: oh really? And why judges and lawyers are central to the way we live now – but they do not know it," *Computer and Telecommunications Law Review* 23(8) (2017): p. 213-225, http://stephenmason.co.uk/wp-content/uploads/2017/12/Pages-from-2017_23_CTLR_issue_8_PrintNEWMASON.pdf

[15] Pei Wang, "What Do You Mean by "AI"?," *Frontiers in Artificial Intelligence and Applications* 171(1) (2008): p. 9 https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf

[16] *Id.*, p. 13

and consider thousands of variables simultaneously[17]. This AI type exist today as "robotic" vehicles, speech recognition, autonomous planning and scheduling, playing games, dealing with spam, logistics planning, robotics and machine translation[18].

Current end goal of developing AI is to make computer programs that can solve problems and achieve goals in the world as well as human beings[19], that is to say make strong AI or artificial general intelligence. Artificial general intelligence refers to when a machine can do things in a way that is indistinguishable from human behavior[20], more precisely it defines the reverse engineering of the human brain, which means coming to understand human intelligence in information terms and then combining the resulting insights with increasingly powerful computational platforms[21]. This type of technology, as far as we know it, does not yet exist and nobody is even close to achieving it.

The last and ultimate type of the AI is artificial superintelligence. This type of AI is hard to imagine as it is more concept than reality at this point. Artificial superintelligence is an intellect that is much smarter than the best human brains in practically every field, including scientific creativity, general wisdom and social skills[22]. In more practical and science fiction terms, it could be defined as mega-brain, electric not organic, with an IQ of 34,597 with perfect memory and unlimited analytical power, this power thing or being could read all of the books in the USA Library of Congress the first millisecond you press "enter" on the program, and then integrate all that knowledge into a comprehensive analysis of humanity's 4,000 year intellectual journey before your next blink[23].

Before we determine elements of AI system, it is necessary to define what we consider as "intelligence" as this term is widely used in virtually every definition of AI, and this author believes, that the problem with defining the AI does lie with the term "intelligence". Therefore, for the sake of clarity we need to determine, what the term "intelligence" means.

Oxford dictionary defines "intelligence" as the ability to acquire and apply knowledge and skills[24]. Intelligence also could be understood as a set of factors, such as consciousness,

---

[17] Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York, USA: Viking, 2005), p. 204, http://www.grtl.org/Singularity-Is-Near.pdf

[18] Mason, *supra* note 14, p. 216

[19] John McCarthy, "What is Artificial Intelligence", Stanford University, 2007, http://www-formal.stanford.edu/jmc/whatisai/node1.html

[20] "A Six Minutes Intro to AI", Snips, https://snips.ai/content/intro-to-ai/#what-is-ai

[21] Ray Kurzweil, *supra* note 17, p. 85

[22] Nick Bostrom, "How long before superintelligence?," *Linguistic and Philosophical Investigations* 5 (2006), https://nickbostrom.com/superintelligence.html

[23] William Bryk, "Artificial Superintelligence: The Coming Revolution," Harvard Science Review, 2015, https://harvardsciencereview.com/2015/12/04/artificial-superintelligence-the-coming-revolution-2/

[24] Oxford English Living Dictionaries, „Intelligence", https://en.oxforddictionaries.com/definition/intelligence

self-awareness, language use, the ability to learn, the ability to abstract, the ability to adapt, and the ability to reason[25]. There is no universal definition of intelligence, however the aforementioned definitions best describe the necessary factors for determining what could be considered as "intelligence".

In order to better understand AI systems, which are currently used in the world, the author needs to describe and analyze the intricate parts of so called symphony of AI technology: machine learning, deep learning, natural language understanding, context awareness, cloud computing, Big Data and data privacy.

First of all, machine learning is a subset of AI[26], which means ability for an algorithm to learn from prior data in order to produce a behavior[27]. To put it plainly, machine learning is the science of algorithms that detect patterns in data in order to make accurate predictions for future data[28]. Machine learning programs automatically improve with experience[29] and can learn without being explicitly programmed to do so[30]. Machine learning technology was prominently shown in mainstream media, when, for example, IBM supercomputer Watson beat humans at the quiz show Jeopardy[31] or Google Deepmind's program AlphaGo was victorious against human opponent in Chinese game Go[32]. It is important to emphasize that machine learning teaches machines to make decisions in a situations they have never seen before.

Currently machine learning is being applied in developing autonomous vehicle technology, such as driverless cars. This technology is so prominent that several EU governments have proposed updating the 1968 Vienna Convention on Road Traffic, which determines that every moving vehicle or combination of vehicles shall have a driver[33] and every

---

[25] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, "Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence," *Vanderbilt Journal of Entertainment and Technology Law* 20(2) (2017): p. 393. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/vanep20&div=16&start_page=385&collection=journals&set_as_cursor=0&men_tab=srchresults

[26] Dimitra Kamarinou, Christopher Millard and Jatinder Singh, "Machine Learning with Personal Data," Queen Mary School of Law Legal Studies Research Paper No. 247/2016, (2016): p. 3, https://ssrn.com/abstract=2865811

[27] Snips, *supra* note 20.

[28] Ralf Herbich, "Session with Ralf Herbrich Director of Machine Learning and Managing Director of Amazon Development, Germany," Quora, 2016, https://www.quora.com/profile/Ralf-Herbrich/session/106/

[29] Parag Kulkarni, *Reinforcement and Systemic Machine Learning for Decision Making* (New Jersey, USA: John Wiley and Sons, Inc., 2012), p. 7, https://zodml.org/sites/default/files/Reinforcement_and_Systemic_Machine_Learning_for_Decision_Making.pdf

[30] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *op. cit.*, p. 3

[31] John Markoff, "Computer Wins on "Jeopardy!": Trivial, It's Not", *The New York Times*, February 16, 2011, https://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html

[32] "Google's "superhuman" DeepMind AI claims chess crown", *The BBC news*, December 6, 2017, http://www.bbc.com/news/technology-42251535

[33] Article 8(1) of "Convention on Road Traffic," United Nations Treaty Series 1042 (1968). https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&lang=en

driver shall at all times be able to control his vehicle[34]. The reasoning behind such proposals is that most of the traffic incidence happens because of human error.

Secondly, deep learning is a subset of machine learning. Deep learning in a nutshell is ability of artificial neural networks — algorithms inspired by the way neurons work in the brain — to find patterns in raw data by combining multiple layers of artificial neurons[35]. Deep learning was the core technology that Google's DeepMind used in their AlphaGo AI machine. Also, deep learning is being used in healthcare to identify patterns in health data and reveal hidden causal links between drugs and biological data[36]. Furthermore, the aforementioned Jeopardy champion Watson is being trained in diagnostics to help diagnose patients more accurately[37].

Third aspect of AI symphony is the natural language learning, which refers to AI ability to understand, interpret and manipulate human language[38]. Natural language processing includes many different techniques for interpreting human language, ranging from statistical and machine learning methods to rules-based and algorithmic approaches.

Fourthly, context awareness means that AI can only be as smart as the information you give access to it[39]. Context refers to the physical and social situation in which computational devices are embedded and the goal of context-aware computing is to acquire and utilize information about this context of a device to provide services that are appropriate to the particular setting[40]. Two aspects are important for context-awareness: 1) the information about the context of a service and 2) the issues in which way the information of the context is taken into account by adapting the service to be finally aware of the context[41].

Fifth of all, cloud computing enabled much faster, cheaper and more scalable processing of huge amounts of data, which means that AI can now take advantage of the vast sets of data and the unlimited resources of the cloud[42]. Cloud computing is being developed and applied by such tech industry giants as Amazon, IBM, Google, and Microsoft. They provide

---

[34] "Convention on Road Traffic," *supra* note 33, Article 8(5).

[35] Snips, *supra* note 20.

[36] David Schatsky, Craig Muraskin and Ragu Gurumurthy, "Demystifying artificial intelligence," Deloitte Insights, 2014, http://dupress.com/articles/what-is-cognitive-technology/

[37] Alfred NG, *supra* note 7.

[38] "Natural Language Processing, what it is and why it matters," SAS, accessed 2018 April 20, https://www.sas.com/en_us/insights/analytics/what-is-natural-language-processing-nlp.html

[39] Snips, *op. cit.*

[40] Jakob E. Bardram, "Applications of Context-Aware Computing in Hospital Work – Examples and Design Principles," Proceedings of the 2004 ACM symposium on Applied computing, p. 1574-1575, http://delivery.acm.org/10.1145/970000/968215/p1574-bardram.pdf?ip=152.118.150.218&id=968215&acc=ACTIVE%20SERVICE&key=580EBA767A7E72A7%2E2F107ED8A98F1C18%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1525842634_0c60a98dba3f5f3c02e768050f29011e

[41] Mario Pichler, Ulrich Bodenhofer and Wieland Schwinger, "Context-awareness and Artificial Intelligence," *OGAI Journal* 23(1) (2004): p. 5 https://www.researchgate.net/publication/200048737_Context-awareness_and_artificial_intelligence.

[42] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 4

cloud-supported machine learning services and tools, especially focusing on predictive analytics. Furthermore, cloud computing technology has allowed scientists and business sector to cooperate in machine learning processes and to recruit the assistance of many people in labeling that means describing the data in an effort to ensure learning[43].

Sixth of all, the Big Data does not have a single definition to describe, however, many authors agree[44], that Big Data refers to: 1) application and development of AI technology and 2) to the vast amount of digitized data currently available. Therefore, Big Data could be understood as the ability to deal with vast amounts of data[45]. This is very useful, considering that nearly all of the world's stored information is digital: about 2.7 zettabytes in 2012[46].

To better understand the concept of Big Data four V's were proposed: the **V**olume of data collected, the **V**ariety of sources, the **V**elocity with which analysis of the data can unfold, and the **V**eracity of the data which could be achieved through analytical process.[47] These V's help understand, that Big Data refers to huge amount of data from various sources, which could be analyzed through complex analytical processes.

Lastly, data privacy in regards to AI involves a situation where AI needs large amount of data to grow, get smarter and more efficient, however people will only give their personal data to companies controlling AI systems, if they know that their data is protected. This issue will be discussed more broadly in the third chapter of this Master Thesis.

---

[43] David Schatsky, Craig Muraskin and Ragu Gurumurthy, "Demystifying artificial intelligence. What business leaders need to know about cognitive technologies," Deloitte University Press, 2014 https://www2.deloitte.com/content/dam/insights/us/articles/what-is-cognitive-technology/DUP_1030-Cognitive-Technologies_MASTER.pdf

[44] Steve Lohr, "How Big Data Became So Big," *The New York Times,* August 11, 2012, http://www.nytimes.com/2012/08/12/business/how-big-data-became-so-big-unboxed.html?smid=pl-share
Elizabeth E. Joh, "Policing by numbers: Big Data and the Fourth Amendment", *Washington Law Review,* 89(1) (2016): p. 38, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/washlr89&div=5&start_page=35&collection=journals&set_as_cursor=0&men_tab=srchresults

[45] Alex Smith, "Big Data, Technology, Evolving Knowledge Skills and Emerging Roles," *Legal Information Management* 16(4) (2016): p. 3. https://login-westlaw-co-uk.skaitykla.mruni.eu/maf/wluk/app/document?&srguid=i0ad8289e00000163684d8f7dcf50b21a&docguid=I9F77F630D66C11E6B79983EFE7771BC7&hitguid=I9F77F630D66C11E6B79983EFE7771BC7&rank=3&spos=3&epos=3&td=14&crumb-action=append&context=4&resolvein=true

[46] Albert Pimental, "Big Data: The Hidden Opportunity," *Forbes*, May 1, 2012, http://www.forbes.com/sites/ciocentral/2012/05/01/big-data-the-hidden-opportunity/

[47] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review* 47 (4) (2017): p. 999-1000, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/shlr47&div=37&start_page=995&collection=journals&set_as_cursor=0&men_tab=srchresults
Bernard Marr, "Why only one of the 5 Vs of big data really matters," IBM Big Data and Analytic Hub, 2015, http://www.ibmbigdatahub.com/blog/why-only-one-5-vs-big-data-really-matters

1.2. History of AI Development

From the Ancient Greek times to science fiction books, humanity has always been fascinated with the thought of creating an artificial copy of a human being. Hephaestus and his lifelike automatons, Frankenstein, Malzel chess automaton are just but a few examples of imaginative or real attempts to create artificial systems, which are capable of intelligence.

However, the true quest for AI as a separate scientific field began to form right after the end of World War II when number of scientist independently started to work on intelligent machines. It is believed that English mathematician Alan Turing was the very first one to conduct research on this field[48].

In 1950 Alan Turing famously developed a so called Turing test, by which any machine could be considered as intelligent if it could trick a human being into believing that he is having text conservation with another human being[49].

The subsequent period between 1952 and 1969 was filled with enthusiasm and great expectations for development of AI. Important year for AI development was 1952, when Arthur Samuel developed a series of programs for checkers, that disproved the notion that computers can only do what they are told because his program started to learn and became better than it's creator[50].

By 1955 John McCarthy, a computer scientist known as the father of AI, developed a term AI and later defined it as "*the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable*"[51]

1956 marks the year when research in AI truly started with two month workshop at Dartmouth College in Hanover, New Hampshire. There were 10 participants in this workshop, as they tried to attempt to find out how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves[52]. This workshop did not lead to any breakthroughs, however it introduced all the major figures of AI

---

[48] John McCarthy, *supra* note 19.

[49] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 3;
Nils J. Nilsson, *supra* note 12, p. 61-63.

[50] Stuart J. Russell & Peter Norvig, *supra* note 13, p. 17-18.

[51] John McCarthy, *supra* note 19.

[52] Stuart J. Russell & Peter Norvig, *supra* note 13, p. 17;
Eliezer Yudkowsky, *Artificial Intelligence as a Positive and Negative Factor in Global Risk* (New York, USA: Oxford University Press 2008), p. 37-38.
https://intelligence.org/files/AIPosNegFactor.pdf

field to each other and these people, their students and their colleagues would dominate the AI research field for the next twenty years[53].

In 1958 John McCarthy published a paper called "Programs with Common Sense", in which he described a program designed to accept new axioms in the normal course of operation, thus allowing this programs to develop new competencies in different areas without being programmed to do so[54].

In these years AI researchers made bold predictions about possible AI capabilities, which turned out to be huge overestimations as AI systems failed to solve more complex problems[55]. These predictions and over confidence will come to bait back the researchers, as in 1970s due to failure to achieve goals AI industry entered a period called "AI winter"[56].

This period is marked with withdrawal of funds and stagnation in progress. The start of "AI winter" could be attributed to two triggers: 1) 1966 Automatic Language Processing Advisory Committee report by USA government, proclaiming that USA government's investment into Russian language translation systems yielded little result and 2) 1973 Lighthill report, commonly known as "Artificial Intelligence: General Survey", which proclaimed, that in no part of AI field have discoveries so far produced the major impact that was then promised[57]. Some scientists attempted to continue to develop their research by just renaming AI research with terms like machine learning or pattern recognition and looking for other sources of funding.

In the 1980 a new wave of funding in UK and Japan was motivated by development of expert systems[58]. Expert systems are computer programs aiming to model human expertise in one or more specific knowledge areas and they usually consist of three basic components: 1) a knowledge database with facts and rules representing human knowledge and experience, 2) an inference engine processing consultation and determining how inferences are being made and 3) an input/output interface for interactions with the user[59].

Japan with their "Fifth Generation" project, USA with Microelectronics and Computer Technology Corporation and UK with Alvey report, which reinstated funding for AI research, tried to kickstart the AI development, however in all three countries projects never met their goals[60]. However, the business sectors boomed with the application of commercial expert

---

[53] Stuart J. Russell & Peter Norvig, *supra* note 13, p. 18

[54] *Id*., p. 18.

[55] Stuart J. Russell & Peter Norvig, *supra* note 13, p. 21.

[56] Brian McGuire et al., "The History of Artificial Intelligence", History of Computing course at the University of Washington-Seattle, University of California-San Diego, and University of California-Berkeley, Washington, 2006, p. 17, https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf

[57] *Id*., p. 16-18.

[58] Francesco Corea, "A Brief History of Artificial Intelligence," *KD Nuggets*, April 2017, https://www.kdnuggets.com/2017/04/brief-history-artificial-intelligence.html

[59] Brian McGuire et al., *op. cit*., p. 12.

[60] Stuart J. Russell & Peter Norvig, *supra* note 13, p. 24.

systems and AI industry skyrocketed from few million dollars in 1980 to billions of dollars in 1988[61]. Soon after this prosperous period came another "AI winter" as companies felt short of delivering very ambitious goals.

The new advances and AI popularity led to the first International Conference on AI and Law in 1987 and in 1991 the International Association for AI and Law was created.

After development of Internet and World Wide Web, AI systems became so common in internet applications, that the notion "bot" entered everyday language and AI technologies were widely adopted in search engines, recommendation systems and planning systems[62]. In these years, the AI came back to public attention, some part thanks to a IBM supercomputer Deep Blue defeating the world chess champion Garry Kasparov in 1997[63].

21st marks few important events in AI history: IBM Watson won in quiz TV show Jeopardy[64], Google DeepMind's AlphaGo AI defeated the Go world champion Lee Sedol[65], chatbox AI Eugene Goostman passed the Turing test[66] and Google Brain computer cluster trained itself to recognize a cat from millions of images in YouTube[67]. These achievements of AI systems really captured the public's imagination and launched AI into mainstream media.

Furthermore, in 21st century, Big Data sets were started to be available as more as more data was being digitalized or gathered and could now be accessible for AI systems. Therefore, during this period researchers started to worry more about quality and amount of data rather than being obsessed with choosing the right algorithm as it was proved that better algorithm with less data was not as good as simple algorithms with more data.

This led to more progress in AI technology, as business started to develop AI and use Big Data in order to increase profits and productivity[68]. Therefore, the AI technology entered into the lives of majority of ordinary people as AI updated and improved many technologies we use today. These technologies will be discussed in the next paragraph.

---

[61] Stuart J. Russell & Peter Norvig, *supra* note 13, p. 24.

[62] Id., p. 27.

[63] Maad M. Mijwel, "History of Artificial Intelligence," *University of Baghdad* (2015): p. 1; 3. https://www.researchgate.net/publication/322234922_History_of_Artificial_Intelligence

[64] John Markoff, *supra* note 31.
Adam Gabbatt, "IBM computer Watson wins Jeopardy clash," *The Guardian*, February 17, 2017, https://www.theguardian.com/technology/2011/feb/17/ibm-computer-watson-wins-jeopardy

[65] Paul Mozur, "Google's AlphaGo Defeats Chinese Go Master in Win for A.I.," *The New York Times*, May 23, 2017, https://www.nytimes.com/2017/05/23/business/google-deepmind-alphago-go-champion-defeat.html

[66] "Eugene the Turing test-beating 'human computer' – in 'his' own words," *The Guardian*, June 9, 2014, https://www.theguardian.com/technology/2014/jun/09/eugene-person-human-computer-robot-chat-turing-test
Although for full clarity, this fact was highly critiqued as Eugene pretended to be 13 year old boy from Ukraine and was able to trick only 33% of judges.

[67] Liat Clark, "Google's Artificial Brain Learns to Find Cat Videos," *The Wired*, June 26, 2012, https://www.wired.com/2012/06/google-x-neural-network/

[68] Brian McGuire et al., *supra* note, p. 20.

1.3. AI Technologies Today and Possibilities for the Future

In this subchapter, the author will briefly review industry fields, where AI technology is applied and prominently used[69]. Furthermore, the future of AI technology will also will be discussed.

Before the author begins with the aforementioned discussion, it is important to note, that currently only seven for profit companies in the world hold powerful AI systems, which are superior to all others[70]. These companies are Google, Amazon, Facebook, IBM, Microsoft, Apple and Baidu (a lesser known Chinese company). There are few attempts to provide AI's capabilities for public use, like the project OpenAI[71]. However, these projects are not as powerful as for the profit ones. This information must be considered when the author discuses usage of AI technology.

First of all, the most prominent and well-known application of AI technology is the automobile industry. Recently Waymo, a subsidiary of Google parent company Alphabet, stated that they have taken out a human from their cars and allowed self-driving car to drive without supervision[72]. Furthermore, Uber's self-driving truck Otto was already making its first deliveries in Colorado[73]. These developments, prompted some automobile industry insiders, like Elon Musk to state, that in the future human driving cars will be banned[74]. So, it indeed could be the case as it is without a doubt, that self-driving cars will become more precise and more efficient than their human counterparts.

Another field, where AI is used constantly and successfully for many years is the financial sector. Using AI technologies or more precisely bots to buy stocks is not new, as quantitative analysis funds relied on computer algorithms for many years.[75] Recently, EquBot

---

[69] Because AI systems are deployed in a lot of fields, only the most prominent ones will be discussed in this subpart.

[70] Vinod Lyengar, "Why AI Consolidation Will Create the Worst Monopoly in US History," *Techcrunch*, August 25, 2016, https://techcrunch.com/2016/08/24/why-aiconsolidation-will-create-the-worst-monopoly-in-us-history
Erin Jang, "What Companies Are Winning the Race for Artificial Intelligence?," *Forbes*, February 24, 2017, https://www.forbes.com/sites/quora/2017/02/24/whatcompanies-are-winning-the-race-for-artificial-intelligence/#2af852e6fcd.

[71] About OpenAI. OpenAI is a non-profit AI research company, discovering and enacting the path to safe artificial general intelligence.
https://openai.com/

[72] Alex Davies, "Waymo has Taken the Human out its Self-Driving Cars," *The Wired*, July 11, 2017, https://www.wired.com/story/waymo-google-arizona-phoenix-driverless-self-driving-cars/

[73] Eric Newcomer and Alex Webb, "Uber Self-Driving Truck Packed With Budweiser Makes First Delivery in Colorado," *Bloomberg*, October 25, 2016, https://www.bloomberg.com/news/articles/2016-10-25/uber-self-driving-truck-packed-with-budweiser-makes-first-delivery-in-colorado

[74] Dave Altavilla, "NVIDIA CEO And Elon Musk On Autonomous Cars: Could Human Drivers Eventually Be Outlawed?," *HotHardware*, March 18, 2015, https://hothardware.com/news/nvidia-ceo-and-elon-musk-on-autonomous-cars-could-human-drivers-eventually-be-outlawed

[75] Paul J. Jim, "The First Ever Fund Managed by a Robot Is Here. So Far It's Beating the Market," *The Time*, October 25, 2017, http://time.com/money/4993744/robot-mutual-fund-beating-stock-market/

company started the first Equity Traded Fund to be managed using IBM Watson supercomputing AI technology[76]. Furthermore, many workers in financial sector are or going to be replaced by AI technology[77]. World Economic Forum's report on "The Future of Financial Services" also predicts, that in the future where will be less human involvement[78] and calls AI a disruptive trend, which alters financial sector[79].

Legal sector is also developing AI technologies in order to make their work faster and more efficient. Baker and Hostetler law firm became the first law firm to hire AI named ROSS, which uses supercomputing power of IBM Watson to comb through huge batches of data and over time learn how to best serve its clients.[80]

Consumer service industries are using AI technologies quite frequently. Traveler calling United Airlines in USA to book a flight could have his or her entire conversation guided by automated speech recognition and dialog management system[81]. The AI systems are also widely used to enhance human experience in video games and try to generate better and more unique gameplay[82].

However, the most famous examples of consumer service industries use of AI is the personal assistants and recommendations bots. Personal assistants such as Apple's Siri, Microsoft's Cortana or Amazon's Alexa are just but a few examples of AI technology applied in helping humans with everyday issues and challenges. Recommendation services, such Netflix and Spotify, are also been enhanced by application of bots[83].

There are also AI systems that can be creative. There are examples of AI systems creating music[84] and writing articles[85]. Facebook AI chat boxes even were able to create their own language for better communication between each other, which humans did not understood[86].

---

[76] Joe Ciolli, "2 Berkeley grads are using AI to make stock-buying decisions — and it could change investing forever," *The Business Insider*, November 28, 2017, http://www.businessinsider.com/ai-powered-etf-aieq-stock-market-machine-learning-investments-2017-11

[77] Nathaniel Popper, "The Robots Are Coming for Wall Street," *The New York Times*, February 25, 2016, https://www.nytimes.com/2016/02/28/magazine/the-robots-are-coming-for-wall-street.html?_r=0

[78] "The Future of Financial Services", World Economic Forum, Final Report, June 2015, p. 154, http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

[79] Id., p. 20.

[80] Chris Weller, "The world's first artificially intelligent lawyer was just hired at a law firm," *The Business Insider*, May 16, 2016, http://www.businessinsider.com/the-worlds-first-artificially-intelligent-lawyer-gets-hired-2016-5/?IR=T

[81] Stuart J. Russell & Peter Norvig, *supra* note 13, p. 28.

[82] Harbing Lou, "AI in Video Games: Toward a More Intelligent Game," *Harvard University Graduate School of Art and Sciences*, August 28, 2017, http://sitn.hms.harvard.edu/flash/2017/ai-video-games-toward-intelligent-game/

[83] Alexis Kleinman, "How Netflix Gets Its Movie Suggestions So Right," *The Huffington Post*, July 08, 2013, http://www.huffingtonpost.com/2013/08/07/netflix-movie-suggestions_n_3720218.html

[84] Bartu Kaleagasi, "A New AI Can Write Music as Well as a Human Composer," *The Futurism*, March 9, 2017, https://futurism.com/a-new-ai-can-write-music-as-well-as-a-human-composer/

[85] Joe Keohane, "What News-Writing Bots Mean for the Future of Journalism," *The Wired*, February 16, 2017, https://www.wired.com/2017/02/robots-wrote-this-story/

Talking about the future, it is important to address the concern expressed by many prominent scientists in AI filed that superintelligent AI is an imminent threat to humanity. This author share the opinion of the panel that contributed to the Stanford Report on Al titled "Artificial Intelligence and Life in 2030": "*Contrary to the more fantastic predictions for AI in the popular press, the Study Panel found no cause for concern that AI is an imminent threat to humankind. No machines with self-sustaining long-term goals and intent have been developed, nor are they likely to be developed in the near future*"[87].

AI technology will continue to make our life easier and more comfortable not only by ensuring better consumer services but also faster and more efficient research in fields such medical research[88]. However, these advancements in technology could come with the price. For example, Carl Benedikt Frey and Michael A. Osborne study stated, that about 47 % of jobs are at risk of being automated in the next two decades[89]. With some even stating, that there is a 50% chance of AI outperforming humans in all tasks in 45 years and of automating all human jobs in 120 years[90]. No matter the number, unemployment will be a big issue as AI is targeting all the sectors, which humans worked in throughout the history - agricultural, industrial and service sectors.

Another important issue is associated with personal data, as more and more devices, applications and things are collecting data, which in many cases are sensitive data of people. Research is being conducted for the internet of things and devoted to the idea that a wide array of devices, including appliances, vehicles, buildings, and cameras can be interconnected to collect and share their abundant sensory information to use for intelligent purposes[91]. Additional problem will arise when AI will collect data, which is not considered as private or personal data, but through analyses and processing will come up with data, which is of personal or deeply private nature. These privacy issues will be addressed more broadly in third chapter.

---

[86] Tony Bradley, "Facebook AI Creates Its Own Language In Creepy Preview Of Our Potential Future," *The Forbes*, July 31, 2017, https://www.forbes.com/sites/tonybradley/2017/07/31/facebook-ai-creates-its-own-language-in-creepy-preview-of-our-potential-future/#b892b97292c0

[87] Rodney Brooks et al., *supra* note 12, p. 4.

[88] Jen Clark, "Is Watson the best medicine? The impact of big data analysis on healthcare," *IBM*, January 3, 2017, https://www.ibm.com/blogs/internet-of-things/iot-and-healthcare/

[89] Carl Benedikt Frey and Michael A. Osborne, "The Future Of Employment: How Susceptible Are Jobs To Computerisation?," *Technological Forecasting and Social Change* 114(C) (2017): p. 1; 44, https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf
"Coming to an Office Near You," *The Economist*, January 18, 2014, https://www.economist.com/news/leaders/21594298-effect-todays-technology-tomorrows-jobs-will-be-immenseand-no-country-ready

[90] Aatif Sulleyman, "AI will be better than human workers at all tasks in 45 years, says Oxford University report," *The Independent*, June 1, 2017, https://www.independent.co.uk/life-style/gadgets-and-tech/news/ai-jobs-stealing-outperform-human-workers-all-tasks-oxford-university-report-a7767856.html

[91] Rodney Brooks et al., *supra* note 12, p. 5

1.4. AI and its Relationship with the Law

In 1942 Isaac Asimov developed rules that could be considered as fundamental principles for regulating future AI and robots: 1) A robot may not injure a human being or, through inaction, allow a human being to come to harm, 2) a robot must obey the orders given it by human beings, except when such orders would conflict with the previous law, 3) and a robot must protect its own existence as long as such protection does not conflict with the previous two laws.

As AI gets more complex and touch more and more sectors of our daily lives, the regulators started to think about regulating AI or even creating a different branch of law devoted to AI. In this subchapter, the author will discuss current legal efforts to regulate AI.

To start with, majority of the laws, which are currently in place today do not necessary target or address AI but have some provision, which could apply to AI. For example, General Data Protection Regulation, which will come in force in May 2018 do not address or even mention AI, however this regulation do state, that automated decision making process is prohibited[92] unless one of few exceptions apply. Other countries, such as Indonesia[93] or India, also applies their laws to AI without specifically mentioning or targeting them[94].

Countries around the world are realizing that aforementioned situation is not sufficient and started to discuss or pass laws specifically design to regulate AI technology.

Council of Europe in 1981 adopted Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[95], however this convention did directly mention neither AI nor Big Data. Therefore, in 2017, Council of Europe issued Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data[96], which were designed to provide a framework for countries to apply aforementioned convention in regards to Big Data technologies.

---

[92] Article 25 of GDPR.

[93] "Data Protection Laws of the World," DLA Piper report on Indonesia, 2017, https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf

[94] "The Future is here: Artificial Intelligence and Robotics," Nishith Desai Associates, October, 2017, p. 15-18, http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Artificial_Intelligence_and_Robotics.pdf

[95] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg". Council of Europe. European Treaty Series No. 108 (1981). https://rm.coe.int/1680078b37

[96] "Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data," Council of Europe, 2017, https://rm.coe.int/16806ebe7a

European Parliament in 2017 adopted resolution with recommendations on Civil Law Rules on Robotics[97], which includes AI, after many studies showed the need for such rules in the future[98]. The goal of this document is to lay down general and ethical principles governing development of robotics and AI for civil purposes.

USA's White House developed a report titled "Preparing for the Future of Artificial Intelligence"[99] and created a "National Artificial Intelligence Research and Development Strategic Plan"[100], which in part address legal challenges, that AI creates. Furthermore, in 2017 USA Congress made some regulatory steps in order to regulate AI: 1) the House of Representatives passed Self Drive Act, which addresses the safety of automated vehicles, 2) the AV Start Act, a bipartisan Senate companion that similarly tackles self-driving cars, and 3) the Future of AI Act, a bipartisan Senate bill that would create an advisory committee on AI issues[101].

Taking even more radical step, Estonia announced, that it plans to give AI a legal status in legal disputes. In would consider AI as an entity, which would have status between a separate legal personality and an object that is someone else property.

Despite all of the aforementioned legislative efforts, AI industry is still not properly regulated. For example, International Bar Association in their report on "Artificial Intelligence and Robotics and Their Impact on the Workplace" stated, that "*It would be desirable for the future laws, which will hopefully be secured at the international level by uniform standards, to be geared to the technological developments and the increased need for flexibility.*"[102] It is need the case as the current legal framework is not flexible enough in meeting AI challenges.

As it stands today many AI companies are taking steps to regulate themselves by creating code of conducts or ethical charters. One example would be Partnership on AI to benefit

---

[97] "European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics," 2015/2103 INL (2017), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN

[98] Please see: Nathalie Nevejans, "European Civil Law Rules in Robotics. Study," Directorate-General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs, European Union 2016, p. 5, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU%282016%29571379_EN.pdf

[99] "Preparing For The Future Of Artificial Intelligence," National Science and Technology Council, Executive Office of the President, 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

[100] "The National Artificial Intelligence Research and Development Strategic Plan," National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee, 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf

[101] Christopher Fonzone and Kate Heinzelman, "Should the government regulate artificial intelligence? It already is," *The Hill*, February 26, 2018, http://thehill.com/opinion/technology/375606-should-the-government-regulate-artificial-intelligence-it-already-is

[102] Denise Garcia, "Battle Bots: How the World Should Prepare Itself for Robotic Warfare," *Foreign Affairs*, June 5, 2015, https://www.foreignaffairs.com/articles/2015-06-05/battle-bots

people and society[103]. The founding partners of this partnership include Amazon, Apple, Deep Mind, Facebook, Google, IBM and Microsoft. The goal of this partnership is to benefit society and people, formulate best practices, advance public understanding of AI and to serve as open platform for discussion. Another example would be Future of Life Institute's Asilomar conference, which developed 23 Asilomar principles[104]. These principles include Principle 12, regarding protection of personal privacy, and Principle 13, regarding protection of privacy and liberty. However, this self-regulation on its own without proper government regulation is not very desirable as self-regulation is usually not obligatory, lack enforcement bodies and is not coordinated by central body, which would unify all the different principles and rules.

AI is and will be a very disruptive technology as it will bring structural changes to our society and economy. These changes are not be underestimated as they will touch every part of society. Therefore, discussions about many important changes, including about autonomous weapons[105], distributions of profits from AI[106] and etc., are already being held.

However, we live in a global world, where companies move between borders with ease, therefore any viable solution must also be global. United Nations and regional powers such as EU should and even must lead the debate about internationally accepted rules on AI in order to meet the challenges created by AI and to reap as much benefits from this technology as possible.

2. REGULATING DATA PRIVACY IN THE AGE OF AI

Regulators all around the world face a lot of challenges when they need to regulate new and constantly improving technologies. Like the internet before it, AI is changing the society and economy we live in. This technology needs to be regulated, however the regulations must be so that it would not stifle the development of the industry and allow citizens to rip the benefits of these intelligent systems.

Many authors agree, current regulatory mechanisms, especially in data privacy, are either unsuitable or cannot be applied to these new technological developments[107]. What is more,

---

[103] Founding partners of Partnership on AI to benefit people and society. https://www.partnershiponai.org/partners/

[104] Please see: "Asilomar AI Principles," Asilomar Conference, 2017, https://futureoflife.org/ai-principles/

[105] Rodney Brooks et al., *supra* note, p. 42-43.

[106] Benjamin Kentish, "Richard Branson calls for universal basic income because robots are taking people's jobs," *The Independent*, October 10, 2017, https://www.independent.co.uk/news/business/news/richard-branson-universal-basic-income-robots-taking-jobs-automation-threat-a7993006.html

[107] Michael Guihot, *supra* note 25, p. 414.

the complete uncertainty behind what the future holds for this technology and the impact to our society is putting another layer of challenges, when considering regulating AI[108].

Therefore, in this chapter the author will discuss, what should be considered as a good regulation by formulating universal criteria to evaluate every regulation and that criteria would be used in the third chapter when the author will evaluate the AI technology and GDPR. Furthermore, the challenges and problems which regulators face when determining rules of data privacy in association with AI systems will also be discussed.

2.1. What Constitutes a Good Regulation?

Even if regulators try to regulate simple and not complex areas of society, creating a good regulation is extraordinary difficult.[109] Therefore, in order to evaluate efficiency any regulation, legal scholars started to determine the criteria necessary to evaluate whether regulation is good or bad[110].

It could be argued, that any good government policy must maximize the wealth, utility, pleasure and/or happiness of society[111]. That is to say, that we should measure regulation and determine whether it is good or bad by determining whether the regulation maximizes welfare. This measurement is usually used by big corporations when they determine some policy's efficiency by performing cost-benefit analysis.

However, such a measurement is not a good benchmark to follow as it is very flawed. First of all, this approach do not take into account moral dilemmas[112], for example pollution of

---

[108] Gonenc Gurkaynak, Ilay Yilmaz, Gunes Haksever, *supra* note 3, p. 8-9.

[109] Bridget M. Hutter, "A Risk Regulation Perspective on Regulatory Excellence," in Gary Coglianese *Achieving Regulatory Excellence* (Washington, USA: Brookings Institution Press, 2017), p. 101-102. https://books.google.co.id/books?id=XdmACwAAQBAJ&pg=PA101&lpg=PA101&dq=Bridget+M.+Hutter,+A+Risk+Regulation+Perspective+on+Regulatory+Excellence,+in+ACHIEVING+REGULATORY+EXCELLENCE+101,+101&source=bl&ots=5EcvhEQJfN&sig=PKCo3nwbgRYxkwOXE04Xq_fxB3g&hl=id&sa=X&ved=0ahUKEwjjtri2yvraAhVKvI8KHS7VCl4Q6AEIJzAA#v=onepage&q=Bridget%20M.%20Hutter%2C%20A%20Risk%20Regulation%20Perspective%20on%20Regulatory%20Excellence%2C%20in%20ACHIEVING%20REGULATORY%20EXCELLENCE%20101%2C%20101&f=false Accessed: April 20, 2018

[110] Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation– Theory, Strategy, and Practice*, (New York, USA: Oxford University Press, 2012), p. 25 https://books.google.co.id/books?id=x_lcrqoqb9oC&printsec=frontcover&dq=Understanding+Regulation:+Theory,+Strategy,+and+Practice&hl=lt&sa=X&ved=0ahUKEwiNgInEqcjaAhUB6GMKHWvCDyAQ6AEIKDAA#v=onepage&q=Understanding%20Regulation%3A%20Theory%2C%20Strategy%2C%20and%20Practice&f=false Accessed: May 1, 2018.

[111] Please see: Michael Sandel, „Justice: What's The Right Thing To Do? Episode 02: "PUTTING A PRICE TAG ON LIFE", Harvard University course on Justice, uploaded in 2009. https://www.youtube.com/watch?v=0O2Rq4HJBxw
Jeremy Bentham, *Principles of Morals and Legislation* (1780), excerpt, Harvard University course on Justice, https://courses.edx.org/courses/course-v1:HarvardX+ER22.1x+2T2017/courseware/C_03/c6828de7461a416381457d1eced938dc/1?activate_block_id=block-v1%3AHarvardX%2BER22.1x%2B2T2017%2Btype%40vertical%2Bblock%40b0048dfca2ce4c0cbd3a5a976c771318

[112] Robert Baldwin, Martin Cave and Martin Lodge, *op. cit.*, p. 26.

the ocean in order to extract oil and generate wealth would be considered as a good regulation because it maximize welfare of the society. Second of all, there is no account for legitimacy of democratic process and rights of minorities. Therefore, if few people's rights could be sacrificed in order to achieve maximum welfare, it is justified by this approach. Third of all, it can be stated, that maximizing welfare provides no ethical basis for action and does not, and cannot justify any particular distribution of rights within society[113].

As shown above simple explanations of what constitutes a good regulation can not be taken account in this Master Thesis as it would be inherently unfair and vague. Thus, more detailed criteria must be established.

According to this author the following criteria must be evaluated when considering any regulation: necessity, transparency, growth support, effectiveness and efficiency, flexibility, certainty, capability and legitimacy[114]. All of these benchmarks will be discussed below.

First of all, necessity means that state must have a legitimate and rational reason to intervene. The regulation must respond to problems in the society or prevent future problems to arise. Furthermore, regulation must have clear goals, which it wants to achieve[115]. For example, in response to the 2008 financial crisis, the USA adopted Dodd-Frank Wall Street Reform[116] and Consumer Protection Act and EU created three new supervisory authorities[117].

Second of all, development, implementation and enforcement of regulation must be transparent as well as regulators must be able to justify decisions and be subjected to public scrutiny[118]. The transparency principle includes nondiscrimination, provision for appeals and sound legal basis for decisions[119]. Transparency is also concerned with guarantees that all concerned and interested parties are given the opportunity to comment and their comments will be duly noted and addressed[120].

---

[113] Please see: Steven Kelman, "Cost benefit analysis: an ethical critique (with replies)" in Robert N. Stavins, *Economics of the Environment*, (New York, USA: W. W. Norton and Company, 1981), p. 356-360.
https://www.unc.edu/courses/2009spring/plcy/240/001/Kelman.pdf

[114] Robert Baldwin, Martin Cave and Martin Lodge, *supra* note 110, p. 26-31;
Peter Mumford, "Best Practices Setting Targets and Detecting Vulnerabilities," *Policy Quarterly* 7(3) (2011), p. 31,
https://ojs.victoria.ac.nz/pq/article/view/4389/3882
Stavros B. Thomadakis, „What Makes Good Regulation," paper presented in IFAC Council Seminar, Mexico City, November 2007, p. 6-9,
http://www.ifac.org/system/files/downloads/30th_anniversary_Thomadakis_Pres_Nov_07.pdf

[115] Stavros B. Thomadakis, *id.*, p. 6.

[116] Helene Cooper, "Obama signs overhaul of Financial System," *The New York Times*, July 21, 2010,
https://www.nytimes.com/2010/07/22/business/22regulate.html

[117]"A comprehensive EU response to the financial crisis: substantial progress towards a strong financial framework for Europe and a banking union for the Eurozone", European Commission, March 28, 2014,
http://europa.eu/rapid/press-release_MEMO-14-244_en.htm

[118] Peter Mumford, *op. cit.*, p. 37;

[119] Peter Mumford, *id*., p. 39;
Robert Baldwin, Martin Cave and Martin Lodge, *op. cit.*, p. 28-29.

[120] Stavros B. Thomadakis, *op. cit.*, p. 7

Third of all, regulators must support rational growth of an industry and not stifle its development. The growth supporting criteria determines that economic objectives are weighted in regards to other objectives[121]. For example, data privacy protection would be weighed against impacts on competition, innovation, compliance costs and etc., when considering data privacy regulation. This principle is also important, when judging the regulation after it was adopting and was used for certain period of time.

Fourth of all, effectiveness and efficiency principle determines that any regulation's inputs and costs are outweighed by benefits of the regulation and achievement of its goals[122]. This principle goes even further - the effectiveness and efficiency of regulation must be higher than other possible alternative regulation.

Fifth of all, flexibility principle determines that industries, which are regulated, must be able to adopt least costly and innovative measures to meet legal obligations[123]. Furthermore, this principle also is supplemented by durability criteria, which means that any regulator must be able to respond to changes and amend or reform the regulation[124]. This means, that regulation must be able to keep up with technological and market changes in order to be relevant and effective.

Sixth of all, any regulated subject or industry must be able easily to know what the law requires from them now and in the future. The relevant institutions must be able to give advises and clarify any misunderstanding quickly[125]. Therefore, companies and people should know, that rights or obligations they have or who to call to determine these rights or obligations.

Seventh of all, capability requirement demands from regulation and regulators to create or have a capable human capital to execute and enforce regulatory regime set by regulation[126]. This means, that regulators have a necessary competence and abilities to understand the industry and enforce desirable behavior from regulated subjects. Furthermore, regulators must be able to adapt to technological changes and test regulation in the context of these changes.

Lastly, any good regulation must have legitimacy in a sense, that there is public support for it and regulation and regulators must be subject to democratic process[127]. Therefore, any good regulation must be accountable to democratic values and people's will.

---

[121] Peter Mumford, *supra* note 114, p. 39.

[122] Robert Baldwin, Martin Cave and Martin Lodge, *supra* note 110, p. 30-31.
Stavros B. Thomadakis, *supra* note 114, p. 8.

[123] Stavros B. Thomadakis, *id*., p. 9.
Peter Mumford, *op*. *cit*., p. 37-38.

[124] Peter Mumford, *id*., p. 37-38.

[125] Peter Mumford, *id*., p. 38.

[126] Robert Baldwin, Martin Cave and Martin Lodge, *op*. *cit*., p. 29-30;
Peter Mumford, *id*., p. 37.

[127] Robert Baldwin, Martin Cave and Martin Lodge, *id*., p. 27-28.

The aforementioned criteria is a good basis for analysis in this paper, however there is some aspects of this criteria, which still need to be addressed in order to have better evaluation of any regulation.

Often regulators have to lower the standard of one criterion in order to meet the standards of other criterion. This process is called regulatory trade-offs and one example of it would be when regulator allows lower the public participation in regulation making process in order to quickly adapt to changes in the society or markets. Despite of this sacrifice, such a regulation could still be considered as a good regulation if regulators address these trade-offs and tries to mitigate them. Taking the example we used in this paragraph, regulators could conduct public comment sessions or evaluation of regulation after the regulation passed in order to still allow public to participate. Furthermore, regulators must provide legitimate reasons supported by expert opinion and report why such trade-off happened and to explain it to the public.

What is more, the measurement of these criteria must also be addressed. Many governments assess the regulations quality, while the Organization for Economic Co-operation and Development performs evaluations of regulatory institution and tools after the regulation comes into effect[128]. According to this author the best way is to divide criteria into divisions: inputs, processes, outputs and outcomes.[129] Inputs assessment evaluates the resources devoted to for the execution and enforcement of regulation. Processes division addresses the ex post evaluation of regulation and analyses of the subsequent policies or guidelines. Outputs evaluate the achieved goals of regulation. Lastly, outcomes determine the impact of the regulation to the legal system and society. This division nicely supplements 8 point criteria and helps the author with making evaluation process much easier and more understandable to the reader.

All in all, the author of this Master Thesis believes, that these 8 criteria and subsequent division are the best benchmark for determining whether any regulation must be considered good or not. The higher standard of each individual criterion regulation achieves the better quality it must be considered to be. Therefore, these criteria will be used throughout the Master Thesis to determine GDPR's value and benefits to society and whether this regulation is the right one in the age of AI.

[128] "Regulatory Performance: Ex Post Evaluation of Regulatory Tools and Institutions", OECD, Working Party on Regulatory Management and Reform, 60V/PGC/Reg, Paris, 2004, p 5-6.

[129] Robert Baldwin, Martin Cave and Martin Lodge, *supra* note 110, p. 35.

2.2. Challenges of Regulating AI in Data Privacy Laws

In this subchapter, the author will addressed the challenges and problems the regulators would have to face when trying to regulate AI in data privacy laws. As mentioned before, the AI is a disruptive technology, which changed and will continue to change the way society and markets work and operate. Therefore, in order to develop a good regulation, regulators must determine these challenges and address them in the data privacy regulations.

The key fear is that it may be too early to regulate AI and that any regulation adopted today "*may hinder developments that could prove essential for human existence.*"[130] This is one part of so called Collingridge Dilemma. The Collingridge Dilemma is associated and challenging for any regulator, which wants to regulate new technology and therefore must be addressed in this Master Thesis.

The Collingridge dilemma states, that early in the development of new technology, the gravity and character of their potential harms are not enough well known to support regulatory intervention and regulation[131]. However, once the technology develops and industry adopts it, the effective control becomes obstructed by constituencies that have been created around the technology with industry's interests in its continuance[132]. In short, we cannot regulate technology in early stages because of limited knowledge about it, while in later stages the technology is so entrenched in our daily lives that there would be resistance from users, developers, investors, companies and even governments.

It is important to mention, that we are no longer living in the early stages of AI development as the AI have already been deployed in society in a vast number of industries from medical diagnostics to criminal or other type of sentencing to social media and personal assistance, making the issue of regulating AI even more urgent[133] because most of the aforementioned fields collect and process insane amounts of personal information.

Therefore, the first challenge regulators faces is a race against time to create a comprehensible AI regulation as using generic laws from the past to regulate AI is no longer an option. And if one lets this technology to continue development without proper regulatory oversight, it would be very hard to regulate it later and get the desired results.

---

[130] Gonenc Gurkaynak, Ilay Yilmaz and Gunes Haksever, *supra* note 3, p. 8.

[131] Edward A. Parson, "Social Control of Technological Risks: The Dilemma of Knowledge and Control in Practice, and Ways to Surmount It," *UCLA Law Review Discourse* 64 (2016): p. 467, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/ucladis64&div=21&start_page=464&collection=journals&set_as_cursor=0&men_tab=srchresults

[132] *Id*., p. 468

[133] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, *supra* note 25, p. 422.

Other challenge of regulating AI in the age of AI is the problem of pattern recognition. AI is very good at analyzing vast amounts of data and recognizing patterns, which people themselves cannot recognize from that data. However, this ability could eventually eliminate the boundaries between what is considered private and public data. AI is increasingly able to derive the personal and private information from publicly available information[134]. For example, Target company's systems were able to determine from online searches, that a girl is pregnant and started sending her ads for things for babies, even though she did not even mention that fact to her parents[135]. The scary thought is that companies, governments or people who have AI with pattern recognition capabilities one day could be able to make predictions and learn very intimate things about a person. Any good data privacy regulation must address this problem associated with pattern recognition and force companies and other subjects to follow legal obligation, which limits the risks of such things happening.

Another challenge that regulators must address is bias inside the AI systems. This bias problem is different than the one associated with human management. As Kate Crawford explains such challenge could be associated with racism, sexism and discrimination, which is unintended[136]. Bias inside AI could be very difficult to detect and have a potential to become an intricate part of the logic by which AI reach decisions.[137] For example, programs designed to pre-select candidates for university places or to assess eligibility for insurance cover or bank loans are likely to discriminate against women and non-white applicants[138]. The problem is magnified by non-transparency of AI systems. However, this challenge could be met with regulation, which requires companies to carefully integrate safety features into the design of AI and have a good troubleshooting mechanism if problems are highlighted. Additionally, companies and regulators should develop testing systems, which would have capabilities of testing such AI systems before and after they are deployed.

What is more, any regulator who wants to regulate AI faces broad but distinct to AI ex ante and ex post problems. The ex ante problems are: 1) Discreetness problem - AI systems could be developed without the need for large scale, integrated institutional frameworks, 2)

---

[134] Ryan Calo, *supra* note 6, p. 421.

[135] Jim Sterne, *Artificial Intelligence for Marketing: Practical Applications* (New Jersey, USA: John Wiley and Sons, Inc., 2017), p. 234. https://books.google.co.id/books?id=cEozDwAAQBAJ&pg=PA234&lpg=PA234&dq=target+pregnant+artificial+intelligence&source=bl&ots=9e0Y_IGaMK&sig=kwm9KkItjTntItiHRgIQU0UiDUU&hl=id&sa=X&ved=0ahUKEwj9ieu-v83aAhXMPY8KHZ01DqMQ6AEIYzAH#v=onepage&q=target%20pregnant%20artificial%20intelligence&f=false Accessed: April 28, 2018.

[136] Kate Crawford, "Can an Algorithm Be Agonistic? Ten Scenes from Life in Calculated Publics," *Science, Technology, & Human Values* 41(1) (2016): p. 77, 82-83. http://journals.sagepub.com/doi/pdf/10.1177/0162243915589635

[137] Kate Crawford, "Artificial Intelligence's White Guy Problem," *The New York Times*, June 25, 2016, https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html

[138] Henry Bodkin, "AI robots sexist, racist, experts warn," *The Telegraph,* August 24, 2017, https://www.telegraph.co.uk/news/2017/08/24/ai-robots-sexist-racist-experts-warn/

diffuseness problem - AI systems could be created by a various set of subjects, working in different jurisdictions and locations, 3) Discreteness problem - AI systems "*will capitalize and make use of discrete technologies and components, the full potential of which will not be apparent until the components come together*" and 4) Opacity problem - the technologies underlying AI will be opaque to the majority of regulators[139]. On the flip side, ex post problems are: 1) Foreseeability problem is associated with the features of AI, which are intrinsically autonomous and mostly operates in ways, that are unforeseeable to original creators and 2) Control problem, which means that AI could potentially operate in such a ways, that human, whether it would be legally responsible persons (narrow control) or humans in general (general control) would not be able to control AI system.[140] Therefore, any good regulation must address these problems. Some possible solution could be an agency or mechanism which would test AI and certify them before they go into the market[141] and later on, in certain time periods test these AI systems to see if they are still performing up to the desired standards and are controllable.

The pacing problem also should be addressed in data privacy regulation. This problem arises if regulator does not keep up with the speed of innovation and thus technology outpaces the regulation. This leads to either too general and broad regulation, which is ineffective and do not provide any guidance,[142] or too strict regulation, which stifles the development of technology. This problem could be mitigated by having effective amendment mechanism and having an agency, which could develop, and change if needed, technical standards and guidance for such regulation.

Another challenge is more subtle but still necessary to be addressed is the consent of the person. Information gathering by big companies has reached such a level, that consumers have no ability to understand the consequences of sharing information[143]. Such a dilemma is amplified by unmatched ability of AI to spot patterns, which humans cannot. This author does not have a comprehensible solution or even recommendation because it is highly unlikely that consumers would ever keep up in this AI arms race. However, regulations maybe could address this issue by setting standards and strict rules for consent clauses in addition to notice clauses[144].

Regulators should also consider not only the ways, that the data is gathered but also how the data is used to influence and control decisions of individuals. Therefore, they need not only

---

[139] Matthew U. Scherer, *supra* note 4, p. 359.
[140] *Id*.
[141] *Id*., p. 394
[142] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, *supra* note 25, p. 421
[143] Daniel J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma", *Harvard Law Review* 126(7) (2013): p. 1880, 1889-93. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/hlr126&div=87&start_page=1880&collection=journals&set_as_cursor=0&men_tab=srchresults
[144] Ryan Calo, *supra* note 6, p. 422.

to address the question of how individuals can protect their data but also how much power should companies have over people. As Ryan Calo determines, companies already can manipulate other market participants through detailed understanding of individual and cognitive limitations of individuals, and politicians can target messages, including fake news, to sway the voters for voting for them or swift public debate[145]. You do not have to look further than recent scandal regarding misuse of personal data to influence election by data analysis company Cambridge Analytica[146]. Any good regulation must address this issue.

Monopolies of data are also a problem as big companies have access to large amounts of data and are not inclined to share such data. Access to data is important as the greater access to data a company has, the better positioned is to solve difficult problems with machine learning and ensure better quality AI[147]. Thus smaller companies have and will have trouble entering and competing in the marketplace. Companies, which have vast amount of data, uses consumer privacy excuse and invoke ethical codes of conduct to not share data[148]. It is indeed the case then you consider, that only several companies in the world can obtain vast amounts of data in the performance of their services and they are buying every possible AI start up out there. Therefore, regulators will have to strike a balance between allowing both small and big players to play the game and data privacy rules.

AI works best if it have access to vast amounts of data and can retain that data, however data privacy laws usually limit access to data and data retention. AI have a potential to be better at decision making process than humans, however it needs data to learn[149]. Therefore, regulators must again strike a balance between strict access to data and AI industry growth. Because limiting company's access to data could force companies to move to different jurisdictions and conduct their research outside EU.

Regulators must also design their rules in such a way, that AI companies would be incentivized to open their AI systems for scrutiny and accountability by regulating bodies. Most of today AI systems are not open for scrutiny and are protected by proprietary rights. For example, regulators must determine whether effective right to question decisions exists as individual do not know the intricate parts of AI and therefore their right to defence is somewhat

---

[145] Ryan Calo, *supra* note 6, p. 423.

[146] Eric Auchard and David Ingram, "Cambridge Analytica CEO claims influence on U.S. election, Facebook questioned," *The Reuters*, March 20, 2018, https://www.reuters.com/article/us-facebook-cambridge-analytica/cambridge-analytica-ceo-claims-influence-on-u-s-election-facebook-questioned-idUSKBN1GW1SG;
Rosie Perper, "Cambridge Analytica's parent company claimed it invented the tough guy image that got Rodrigo Duterte elected", *The Business Insider*, April 6, 2018, http://www.businessinsider.sg/cambridge-analytica-duterte-tough-guy-image-for-presidential-election-2018-4/?r=US&IR=T

[147] Ryan Calo, *supra* note 6, p. 424.

[148] *Id*.

[149] Jakob E. Bardram, *supra* note 40, p. 1; 3-6.

limited. Also, the AI is relatively opaque and not open, therefore it makes it easier for companies to hide a wrongdoing and evade regulation[150]. In analogical situation, Volkswagen was able to create specific code, which would allow them to trick emission tests, which were showing, that engines were emitting less toxic materials than it actually did. Therefore, regulators need to consider this problem and ensure, that companies have less incentives and are less able to abuse data privacy regulation.

Lastly, information asymmetry is a big issue, that needs to be addressed. As Michael Guihot, Anne F. Matthew and Nicolas P. Suzor state, information asymmetry happens where the AI companies hold all the relevant information about the technology and regulators do not have such an expertise[151]. Stanford one hundred year study on AI also noted this problem and stated, that governments should accrue greater technical expertise on AI[152]. Because regulators do not yet have the expertise or even enough information to create expertise, if we are ever to ensure Al is developed in a way that is beneficial for humanity, developers must acknowledge both their social obligation to share information (be transparent and accountable) with others, and the critical importance of collaborations with thinkers from other disciplines[153].

In summary, the regulators need to address Collingridge Dilemma, pattern recognition, bias, ex ante, ex post, pacing, consent, application of data, competition, development, accountability and expertise problems in order to create a regulation, which would be considered as a good regulation. In the next chapter the author will test the GDPR and determine whether it indeed meets these challenges in era of intelligent machines.

3. AI AND GDPR

The GDPR was passed in April of 2016, following a long process of negotiations and concessions. From the moment final version of GDPR has seen the light of day, business sector, citizens of EU, governments across Europe and beyond was trying to understand and adopt the framework which GDPR will require to be adopted from May 2018, the month the GDPR will officially come into effect[154].

This chapter will be dedicated to the evaluation of GDPR and its compatibility with AI technology. The author will have two tasks in this chapter: 1) to determine whether GDPR is a

[150] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, *supra* note 25, p. 426.
[151] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, *supra* note 25, p. 425.
[152] Rodney Brooks et al., *supra* note 12, p. 4; 10; 42; 43; 45; 48.
[153] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, *op. cit*., p. 456.
[154] Article 99 of GDPR.

good regulation by using the criteria determined in subchapter 2.1. of this Master Thesis and 2) to analyze how the GDPR meets the challenges stipulated in subchapter 2.2.

However, before the author goes on with the evaluation, one question needs to be answered: why GDPR was chosen for this evaluation? There are several reasons for that.

First of all, the impact and consequences of GDPR will surely be significant and long lasting. Some authors even called GDPR the most comprehensive and forward looking piece of legislation to address the challenges facing data protection in the digital age[155]. Whether it might be true or not, the GDPR, which replaces 1995 Data Protection Directive[156], is going to set the rules of data privacy protection throughout the next few decades. The author of this Master Thesis agree, that the GDPR is one of the comprehensible data protection legislation with years of legal jurisprudence behind it, thus making GDPR the perfect target for evaluation.

Second of all, the GDPR, despite never mentioning AI by name, GDPR still have a lot of articles, which directly affects operation of AI technology. For example, Article 22 of GDPR prohibits automated individual decision making, including profiling[157], which have potential to stifle or somewhat impact the development of the AI technology. Furthermore, other data privacy regulations in different countries around the world do not contain such clauses. Thus, the author believes GDPR is the perfect test subject to test the idea, that AI could be regulated by general laws without the need for laws specifically targeting AI.

Thirdly, the GDPR was also selected because of the so-called Brussels effect. Professor Anu Bradford states, that despite economic and political turmoil in Europe, the EU exerts vast amounts of influence of global markets through its regulatory and legal frameworks[158]. The EU usually sets high standards for any goods or services inside its internal markets and for importing goods and services originating from outside EU[159]. Therefore, countries, which wants to export their goods and services into EU must obey by those standards and in many cases change their laws. Therefore, GDPR could have a ripple effect around the world and countries would model their data privacy legislation as a copy of GDPR.

Lastly, from purely economic standpoint, EU is the economic powerhouse in the world. In 2016, EU was the second largest economy by gross domestic product based on purchasing

---

[155] Tal Z. Zarsky, *supra* note 47, p. 995.

[156] "Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," O.J. L 281/32 (1995), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046

[157] Article 22(1) of GDPR.

[158] Anu Bradford, "The Brussels Effect," *Northwestern University Law Review* 107(1) (2012): p. 3, https://pdfs.semanticscholar.org/2c55/404a1e09859c289644c517020aecd7fe48e4.pdf
Anu Bradford, "The Brussels Effect: The Rise of a Regulatory Superstate in Europe," Columbia Law School, 2013, http://www.law.columbia.edu/media_inquiries/news_events/2013/january2013/brussels-effect

[159] Alan Beattie, "Why the whole world feels the 'Brussels effect,'" *The Financial Times*, November 16, 2017, https://www.ft.com/content/7059dbf8-a82a-11e7-ab66-21cc87a2edde

power parity[160]. The rules set by EU for its internal market is important as they affect 20 billion dollar economic machine. Combine this number with Brussels effect and you have a truly influential player in the global markets.

All in all, despite long negotiations and years of jurisprudence, GDPR is not a perfect legislation and it indeed raises a lot questions in regards to AI. Many authors and legal scholars have been arguing that GDPR is not compatible with the age of AI and must be improved[161]. Thus, this Chapter in essence will address every relevant critical part of GDPR and determine whether the critique is justified. The third chapter of this Master Thesis will be divided as follows: 1) fundamental principles of GDPR, 2) right to notification and access and 3) automated decision making and profiling.

3.1. Fundamental Principles

GDPR establishes several fundamental principles for processing of personal data. These principles determine the foundation, which every processing of personal data should be based upon and follow.

Few of these fundamental principles directly or indirectly clashes with AI industry and technology, thus must be evaluated and analyzed. These principles are: 1) lawfulness, fairness and transparency (Article 5(1)(a) of GDPR), 2) purpose limitation principle (Article 5(1)(b) of GDPR), 3) data minimization principle (Article 5(1)(c) of GDPR) and 4) Special categories of personal data (Article 9 of GDPR). All the aforementioned principles and their compatibility with AI technology will be examined and analyzed below.

3.1.1. Lawfulness, Fairness and Transparency

Article 5(a) of GDPR determines, that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

For the sake of clarity and before we analyze aforementioned principle it is important to determine what we consider personal data in light of GDPR. Personal data in the GDPR is defined as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in*

[160] Abby Budiman and Dorothy Manevich, "Few see EU as world's top economic power despite its relative might," Pew Research Center, 2017, http://www.pewresearch.org/fact-tank/2017/08/09/few-see-eu-as-worlds-top-economic-power-despite-its-relative-might/

[161] Tal Z. Zarsky, *supra* note 47, p. 996.
Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26.

particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[162]

In order to analyze the above mentioned principles, it is necessary to divide this section into three separate subsections, which would be dedicated to evaluating each of these three principles: 1) lawfulness, 2) fairness and 3) transparency. This is necessary because each of these principles determine different types of issues and challenges in association with AI technological development and its uses in processing personal data.

3.1.1.1. Lawfulness

Lawfulness principle is very important for the GDPR as any and all processing of personal data must be done legally and according to the procedures set in the GDPR. Therefore, the author will try to determine what kind of processing should be considered as lawful, the issues and challenges which AI industry face when dealing with this principle and recommendations to help solve the issues.

To start with, two notions will be relevant when considering whether processing is lawful in the AI context - "processing" and "profiling". GDPR defines "processing" as: "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*[163].

Additionally, GDPR defines "profiling" as *"the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"*[164]. Article 29 Working Party further clarified this definition by stating, that profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar[165]. In essence, profiling is composed of three elements: 1) it has to be

[162] Article 4(1) of GDPR.
[163] Article 4(2) of GDPR.
[164] Article 4(4) of GDPR.
[165] Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (WP251rev.01, 17/EN, adopted on February 6, 2018): p. 7.
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

an automated form of processing, 2) it has to be carried out on personal data and 3) the objective of the profiling must be to evaluate personal aspects about a natural person[166].

It is important to mention, that profiling is very similar to automated decision making, therefore they are both mentioned in Article 22 of GDPR, which is the most relevant article for AI processing. The lines between profiling and automated decision making is blurry, as both of these processes can overlap. Easiest way to understand[167] the differences is to think, that automated decisions can be made with or without profiling, on the other hand profiling can take place without making automated decisions[168].

The rules regarding the legality of automated individual decision making and profiling were already determined in the 1995 Data Protection Directive, a predecessor of GDPR. These rules in essence determined, that individuals have a right not to be subjected to a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him[169].

The GDPR picked up these rules and somewhat extended them. Current version states, that the right to not be subjected to automated decision making includes not only profiling of data subjects but also any other type of automated processing[170]. What is more, both Data Protection Directive and GDPR contains clauses, that fully automated assessments of a person's character should not form sole basis of decisions that significantly impinge upon the person's interests[171]. This right in essence guarantees, that EU citizen would not be subject to decision making process, which is conducted solely on automated processing and results in legal effects concerning EU citizens or similarly affects them.

When explaining the rules of automated decision making, Article 29 Working Party determined in 2013, that automated individual decision making, including profiling, should not only cover decision that produces legal effects or significantly affects data subjects but also the

---

[166] Article 29 Working Party, *supra* not 165, p. 6-7.

[167] Example: Imposing fines for speeding only using evidence from speed cameras would be considered an automated decision making process, which does not necessarily involve profiling. However, it would become a decision based on profiling if the individual habits of driving were monitored over certain period of time and speeding fine imposed would be the outcome conclusion of the assessment, which involve other criteria, such as whether it is a repeat offence or whether the driver has had other recent traffic violations.
Article 29 Working Party, *supra* note 165, p. 8.

[168] *Id*.

[169] Article 15 of Data Protection Directive.

[170] Article 22 of GDPR.

[171] Lee Bygrave, "Automated Profiling, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling," *Computer Law and Security Review* 17 (1) (2001): p. 13.
http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf

collection of data for the purpose of profiling and the creation of profiles as such[172]. Thus there is a strong need to discuss not only the legality of processing by automated means but also the collection of personal data and use of such data.

After brief analysis of history and definitions in regards to automated decision making process and profiling, the author will now evaluate three things regarding lawfulness of AI processing - 1) the legality of performing automated processing, which includes profiling, 2) the legality of reaching automated decisions in regards to such processing[173] and 3) the legality of use or deployment of collected data. These things are important to evaluate as any AI processing is made by automated means.

First of all, the performance of automated decision making is allowed if there are at least one of three exceptions determined in GDPR: 1) necessity of entering or performing the contract between data subjects and data controllers, 2) authorization by European Union or Member State law provided, that there are necessary safeguards for data subjects rights and 3) data subject's consent[174]. The problem with those exceptions arises then you start considering consent and implementation of safeguards.

Many legal scholars believe that consent clause is the most problematic of the exceptions provided in Article 22(2) of GDPR. Article 4(11) of GDPR determines, that consent is *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*. Generally, the consent must be made by informed data subject, who understands the nature and logic of algorithms behind AI systems, however, this understanding of consent goes against the nature of many AI systems with machine or deep learning capabilities.

Many types of algorithms are inherently non-transparent or understandable and even if they could be understood, the average data subject would find it hard to comprehend them[175]. Such inexplainability happened because developers prioritized predictive performance rather than interpretability[176]. Some AI systems are not even understood or even interpretable by their own designers, therefore companies would need to change their AI designs in order to make them more explainable for the average consumer. This could lead to a trade-off between performance and interpretability, as more complex AI systems are more efficient but less

[172] Article 29 Working Party, "Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation", adopted May 13, 2013, p. 3, http://ec.europa.eu/justice/article-29/documentation/other-document/index_en.htm

[173] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 7.

[174] Article 22(3) of GDPR.

[175] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *op. cit.*, p. 15.

[176] Lilian Edwards and Michael Veale, "Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for," *Duke Law and Technology Review* 16 (2017-2018): p. 26.

explainable[177]. Therefore, it could be argued, that many AI systems are not lawful as the consumer cannot make a specific, informed and unambiguous consent.

Furthermore, the information gathering by big companies, especially Big Data companies[178], has reached such a level, that consumers have no ability to determining the consequences of sharing information[179]. Thus further questioning ability to consent to automated decision making made by AI.

Even if consent is valid under data protection law, it might be that the data controller is required to obtain a separate consent for processing data subjects' personal data in specific situations, such as in an employment or medical context[180]. Therefore companies, which use AI, would not have an incentive to use AI on broad bases as it will always be hard to determine whether the information about the system is specific and would be understandable to the data subject.

All in all, Giulio Coraggio best describes consent situation with this question - "who would ever grant his consent to be subject to an automated decision?"[181] In his view, such a prohibition, which only could be circumvented with consent, should only apply for marketing purposes, as this field is mostly associated with intrusive to privacy measures[182]. Other fields could bear many benefits without the consent clause[183], such as medical research.

Talking about the lawfulness of reaching a decision by automated means, several problems arises when data subject wishes to exercise the right to express their point of view and to object the decision[184].

According to GDPR, data controller must let the data subject to express their point of view[185] before algorithm makes its final decision, therefore it is reasonable to say that data controller must have sufficient safeguards to prevent a machine from reaching a final decision after the data subject exercises the aforementioned right[186]. However, current types of AI reach

---

[177] Lilian Edwards and Michael Veale, *supra* note 176, p. 26, 59, 61, 64.

[178] For the sake of clarity, Big Data term refers to: 1) application and development of artificial intelligence technology and 2) to the vast amount of digitized data currently available.

[179] Daniel J. Solove, *supra* note 143, p. 1880, 1889-93.

[180] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 15.

[181] Giulio Coraggio, "Artificial intelligence and machine learning: what privacy issues with the GDPR?," *The Gaming Tech Law*, 2016,
http://www.gamingtechlaw.com/2016/10/privacy-gdpr-artificial-intelligence.html

[182] *Id*.

[183] Let's take insurance industry for example. Insurance companies needs automated decision making for faster and more efficient way to process personal health data, however if data subjects do not consent to such processing insurance companies will have to use others methods, which are much costlier and in the end the consumer will pay premiums. If there would be no prohibition insurance companies would process insurance risks by automatic means and it would make the process cheaper, thus the people would get lower insurance premiums.

[184] Article 18 and Article 21 of GDPR.

[185] Article 18 of GDPR.

[186] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *op. cit.*, p. 15.
Article 18(1)(d) of GDPR.

decisions almost instantaneously or are not designed to stop in the middle of processing. Thus making the processing conducted by these AI systems unlawful, if the data subject exercises the right to express his point of view.

In regards to the right to object, the Article 29 Working Party stated, that human intervention is a key element as any review must be carried out by someone who has the appropriate authority and capability to change the decision[187]. In some cases, reviewing the decision would be hard as automated decision making process could have been made based on third party algorithms, pre-learned models, opaque machine learning models or on data sets. Additionally, it is hard for human to understand how machine achieved one or another decision because, as it was stated before, sometimes even designers of machines do not know how AI reached one decision or another.

Furthermore, it could be argued, that to express his/her point of view or object the decision, the data subject must understand the AI system and how the system reached its decision. Only this way, data subject would be able to point out why he believes the possible decision is unfair or detrimental to his future situation. However, as it was discussed in the previous paragraphs, the data subject would struggle to understand the intrinsic parts of AI system and would have a hard time objecting the decision or expressing his/her view without understanding how the AI system reached the decision. What is more, most of the software behind AI is copyright protected or considered trade secret, even more restricting data subject's ability to gain information and understand his claims. Thus the effectiveness of aforementioned rights in the context of AI must be questioned.

Lastly, the author turns to discuss the legality of collection and deployment of obtained personal data. Recent headlines about Cambridge Analytica[188] or firms, such as Palantir[189], brought the debate about the legality of collection and using the data subject's personal data and the lawfulness of such usage. Companies already can manipulate other market participants through thorough understanding of data subject and cognitive limitations of data subjects and politicians can target messages, including fake news, to sway the voters for voting for them or swift public debate[190]. In this author's opinion, the GDPR lacks the necessary teeth and mechanism to prevent or catch companies who misuse data for notorious reasons and to question legality of this process. One reason why companies can do that is because they design their own

[187] Article 29 Working Party, *supra* note 165, p. 27.
[188] Erich Auchard and David Ingram, supra note 146.
Rosie Perper, *supra* note 146.
[189] Peter Waldman, Lizette Chapman, and Jordan Robertson, "Palantir Knows Everything About You," *Bloomberg,* April 19, 2018,
https://www.bloomberg.com/features/2018-palantir-peter-thiel/
[190] Ryan Calo, *supra* note 6, p. 423.

systems and regulators do not have proper tools to catch these companies. The best analogy would be the Volkswagen scandal, when they created algorithms to cheat emission testing devices[191]. Therefore, there is a need for innovative solutions.

In the last paragraph of this subsection, the author will provide solutions or recommendations to the aforementioned problems. One of the solutions, which regulators could consider would be a right to appeal to an AI. Some authors suggested[192] that AI can be much more objective and neutral in making decisions, because AI can make decision without considering or being biased toward factors such as race, religion, age and others. Furthermore, another AI could be much more equip in terms of computing power and speed to evaluate the work of another AI. Therefore, if AI could be more fairer and faster than their human counterparts, this option should be considered by regulators. Such an AI would help solve the efficiency issues of right to object and give tools to data subject to legitimize and explain his right to express his view, as he will have more information about the fairness of the process. However, as the law stands today, the AI appeal option would not be considered as lawful.

However, the aforementioned idea has its drawbacks. First of all, AI could have the subjectivity and moral compass of its creator or the AI could be biased and unintentionally racist, sexist or discriminatory in the outcomes of data analysis[193]. For example, algorithms performing predictive risk assessments of defendants committing future crimes were making errors with risk scores for black defendants[194], just because of data sets provided to it, which contained disproportional statistics. In any case, if AI would be designed in such a way to disregard such biases, such AI potentially would be much fairer than any human ever could. Some possible middle ground could be found in the idea, that regulators would take into account recommendations from this "appeal AI" and make decision.

Furthermore, some authors suggested[195] using "subject-centric" explanations in order to help data subject better understand the AI systems and thus to give more knowledgeable consent or more effectively exercise other rights. "Subject-centric" explanation means, what explanations would be restricted to particular regions of an AI model around a query[196]. Thus the explanation is restricted to region surrounding a set of data. This would allow data subject to explore and

---

[191] Russell Hotten, "Volkswagen: The scandal explained," *The BBC*, December 10, 2015, http://www.bbc.com/news/business-34324772

[192] Dimitra Kamarinou, Christopher Millard and Jatinder Singh, *supra* note 26, p. 15.

[193] Kate Crawford, *supra* note 137.

[194] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, *supra* note 25, p. 405.

[195] Lilian Edwards and Michael Veale, *supra* note 176, p. 81;
Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation," *International Data Privacy Law* 7(2) (2017), p. 43-44. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

[196] Lilian Edwards and Michael Veale, *id*., p. 81.

understand complex AI systems. However, these explanation models do not explain the AI system in its entirety and is still underdeveloped.

Similar explanation models, such as pedagogical model, could also be considered as they would allow avoiding the intellectual property rights or trade secrets wall. Pedagogical models create an explanation around a model rather than from decomposing it[197]. However, the quality of such explanation could be questioned and data subject would be quite far from understanding the AI systems in order to efficiently exercise his rights.

All in all, lawfulness requirement consists of determining legality of several processes included in GDPR, such as automated decision making. However, the practice, which companies engage today and AI development trends could be incompatible with the principle of lawfulness either because companies tend to misuse obtained data or because GDPR determines rules, that would be very hard for AI industry to follow. Ultimately, the AI holds potential to make processes fairer.

3.1.1.2. Fairness

Ensuring fairness is one the ultimate goals of data protection legislation and is necessary for data subject to trust any processing. However, striking a right balance between protecting this principle and further development of AI industry is quite a challenge. Therefore, in this subsection the author discusses what is considered fairness in the context of GDPR formulates some issues regarding relationship between AI and fairness principle and lastly, offers some solutions on how EU law could be improved in order to meet the challenges posed by AI.

The fairness requirement is enshrined not only in GDPR but also in other important EU documents, for example, Article 8 of EU Charter of Fundamental Rights provides, that personal data must be processed fairly. Despite fairness principle being mentioned in many legal documents, the notion of what is fair is quite an open term and therefore requires more explanation.

The best way to explain what is fair in context of GDPR and AI technology is to provide the understanding of what is unfair. Let's take the example of profiling. In case of profiling Article 29 Working Party stated, that profiling may be unfair when it creates discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products[198]. GDPR Recital 60 also states, that: "*The controller should provide the data subject with any further information*

[197] Lilian Edwards and Michael Veale, *supra* note 176, p. 65.
[198] Article 29 Working Party, *supra* note 165, p. 10.

necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore the data subject should be informed of the existence of profiling and the consequences of such profiling.". Additionally, Recital 71 determines, that: "*In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized,…."* Therefore, processing of personal information could be considered unfair if it discriminatory, the data subjects is not provided with necessary information and there are not enough safeguards.

In addition to aforementioned criteria, AI's processing of personal data could also be unfair if it display biases. Biases could be difficult to detect and if precautionary measures are not being taken could become part of the logic of everyday algorithmic systems[199].

There was a time when many experts believed, that AI systems could not display bias and could execute perfect decisions[200]. Even drafting documents of 1995 Data Privacy Directive acknowledge this and stated, that AI systems[201] has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities[202]. However, later it was proved in many situations, that AI might be biased.

Generally in the context of AI, there are two types of biases - direct and indirect. An indirect bias occurs when past prejudices are already built up in the data. For example, certain minority groups are mistreated in the past and therefore their data is inaccurately shown to the AI, which makes future decisions based on that data. For example, in a hiring application, if fewer women have been hired to executive positions previously, data about female employees might be less reliable than data about male employees[203]. However, these issues can be ameliorated with regulation that requires either careful design or prompt troubleshooting when the issues are identified[204].

---

[199] Kate Crawford, *supra* note 137.

[200] Christian Sandvig, "Seeing the Sort: The Aesthetic and Industrial Defence of "the Algorithm"," Journal of the New Media Caucus, 2015. http://median.newmediacaucus.org/art-infrastructures-information/seeing-the-sort-the-aesthetic-and-industrial-defense-of-the-algorithm/

[201] In that document referred as "machine" or "software".

[202] "Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," COM(92) 422 final-SYN 297, October 15, 1992, p. 26. http://aei.pitt.edu/10375/1/10375.pdf

[203] Joshua A. Kroll et al., "Accountable Algorithms", *University of Pennsylvania Law Review* 165(3) (2017): p. 681. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/pnlr165&div=20&start_page=633&collection=journals&set_as_cursor=0&men_tab=srchresults

[204] Michael Guihot, Anne F. Matthew and Nicolas P. Suzor, *supra* note 25, p. 405.

Direct biases happens when the AI follows the subjectivity and moral compass of the designer or when the AI is designed in such a way as to pursue the goals of the creator[205]. A bias might be also direct if designer of AI makes the algorithm to develop a model that filters people by race, gender, or religion, where there is no justification for doing so[206].

This introduction to fairness principle gives the reader some understanding about the possible impacts of AI technology to fairness of whole processing, however the author will now provide more in depth analysis of possible challenges in regards to AI and GDPR.

The first major problem associated with the direct and indirect biases is so called "black boxes". As Bjorn Erik Thon and Catharina Nes[207] explains the complex way in which algorithms reach their results may put them beyond the reach of individuals' understanding. These complicated systems may therefore become as "black boxes", which conceal the evaluations, analyses, decisions and choices made during the creation of the model. Therefore, if decisions are made in "black boxes", unfairness will be difficult to expose and as Bjorn Erik Thon and Catharina Nes concludes the regulators needs to find a way to look into these systems[208]. So in order to ensure the fairness of these systems the regulators need to have a mechanism determined in GDPR on how to access these systems and evaluate their objectivity without infringing on intellectual property rights and trade secrets of companies. As it stands now, it is difficult to say whether GDPR have this sort of mechanism to look into "black boxes" or will it require the companies to change the designs of AI systems, thus requesting privacy by design[209].

Second problem arises due to the nature of AI systems. More precisely, it will be very hard for regulators to establish liability by understanding and uncovering causal links for violating fairness principle. This is especially true, when considering data mining procedures.

Data mining involves the deployment of a set of continuously evolving research techniques, which have become available as a result of widely distributed access to massive, networked computing power and exponentially increasing digital data sets, enabling almost anyone who has the right level of skills and access to assemble vast quantities of data, whether as text, numbers, images or in any other form, and to explore that data in search of new insights and

---

[205] Kathleen Chaykowski, "Facebook News Feed Change Prioritizes Posts From Friends Users Care About," *The Forbes*, June 29, 2016, https://www.forbes.com/sites/kathleenchaykowski/2016/06/29/facebook-tweaks-news-feed-algorithm-to-prioritize-posts-from-friends-you-care-about/#585f2378da2e

[206] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 16.

[207] Bjorn Erik Thon and Catharina Nes, "Controlling the Algorithms," *European Data Protection Law Review* 3(1) (2017): p. 17, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/edpl3&div=7&start_page=16&collection=journals&set_as_cursor=0&men_tab=srchresults

[208] *Id*., p. 18.

[209] Article 25 of GDPR.

knowledge[210]. Or to put it into more understandable terms, data mining is a procedure by which large databases are mined by means of algorithms for patterns of correlations between data.[211] The correlations found by the algorithms through data mining procedure determines some type of relation between different data, however it does it without necessarily providing an explanation about what that relation really is or whether there is a causal link between the data.[212] Let takes an employment case for example, algorithm might determine, that female candidate is not suitable for being a CEO but the cause for this may be, that much less women there given a chance to reach CEO level in the past due to historical reasons and therefore the data "fed" to algorithm reflect this past injustices[213].

Locating and differentiating correlations and causation in data mining could help identify whether the biases are because of algorithms models was mistaken in interpreting and sorting data or because of company's unfair and discriminatory policies. This would help regulators evaluate what kind of degree of liability should be accorded in light of GDPR provisions, however the GDPR do not stipulate how such an issue could be solved.

In light of aforementioned problems, the author will suggest some solutions. One solution to problems mentioned above which could be adopted in later years, would be to create an obligation for companies using AI to develop measure to minimize and correct discrimination and biases[214]. These measures could include prompt troubleshooting mechanism or careful design[215]. Ensuring, that algorithms are fair could be done through EU courts also, as in CJEU Google Spain case the court determined, that Google algorithm must allow execution of right to be forgotten[216] and thus proving, that big AI companies could be forced to uphold the rights determined in GDPR.

Another way would be to force companies to develop so called explainable AI systems, which would allow human to understand how AI reached a certain decision. One example of such AI is usage of scoring algorithms that inject noise and score additional data points around

---

[210] "Standardisation in the area of innovation and technological development, notably in the field of text and data mining," European Commission, report from the Expert Group, 2014, p. 10, http://ec.europa.eu/research/innovation-union/pdf/TDM-report_from_the_expert_group-042014.pdf

[211] David Wright and Reinhard Kreissl, *Surveillance in Europe* (New York, USA: Routledge, 2015), p. 75, https://books.google.co.id/books?id=9amQBAAAQBAJ&pg=PA75&lpg=PA75&dq=Data+mining+is+%E2%80%98a+procedure+by+which+large+databases+are+mined+by+means+of+algorithms+for+patterns+of+correlations+between+data%E2%80%99&source=bl&ots=lCVufyexqx&sig=__dQGm7oh0yDbJNWhpkS3PFJkrw&hl=id&sa=X&ved=0ahUKEwipx_utu6zaAhVLuo8KHQtrD8EQ6AEIMjAB#v=onepage&q=Data%20mining%20is%20%E2%80%98a%20procedure%20by%20which%20large%20databases%20are%20mined%20by%20means%20of%20algorithms%20for%20patterns%20of%20correlations%20between%20data%E2%80%99&f=false Accessed: April 30, 2018.

[212] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 17.

[213] *Id*.

[214] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195, p. 37.

[215] Careful design part could be understood as obligation stemming from Article 25 of GDPR.

[216] Google Spain v. Agencia Espafiolade Proteccion de Datos (AEPD) and Gonzilez, Case C131/12, ECLI:EU:C:2014:317.

an actual data record being computed, to observe what features are driving the score[217]. This technique is called local interpretable model-agnostic explanations (LIME), and it involves manipulating data variables in infinitesimal ways to see what moves score the most[218]. This would allow understanding what kind of criteria was used by algorithm to determine one result or another.

However, above mentioned solution have its drawbacks. Forcing companies to make AI more explainable could have a chilling effect on the development of AI industry. Companies invested a lot of funds into developing the types of AI systems they have today and for them to change these types of intelligent machines would be very costly and time consuming. Going even further, the small companies would not be eager to go into AI market because they would need not only to spend a lot of money on development but also they will need to spend vast amounts of money in order to comply with the privacy laws. Regulators must ensure, that small companies would have a chance to compete and that all companies must be held accountable. Lastly, making AI more explainable could cost the company performance efficiency of such systems as more complex systems are better at decision making but are hard to explain.[219].

Lilian Edwards and Michael Veale proposes another solution on how to create a fair and unbiased AI system[220]. They suggest emitting characterization such as gender or race from the data, which is "fed" to the algorithm. However, this would not be a perfect solution as in many situations gender and race have a predictive value as thus emitting such characterizations could cost better representation of data subject and would not be so accurate.

All in all, fairness principle should be the most important principle for the AI industry to achieve and uphold. However, as it stands now the GDPR is not addressing many issues associated with the fairness principle, whether it is because of a lack of mechanisms or specific rules inside GDPR. In essence, the regulators in EU need to ensure, that AI industry continues to develop inside EU without stifling its growth and without lowering the standards of fairness.

3.1.1.3. Transparency

Transparency is often regarded as a fundamental requirement of the GDPR to promote openness and this principle forms an important part of Article 8 of EU Charter of Fundamental Rights. As the author discussed earlier, the process of AI is often invisible to the data subject and

[217] Scott Zoldi, "GDPR: time to explain your AI," *The Financier Worldwide*, August, 2017, https://www.financierworldwide.com/gdpr-time-to-explain-your-ai/#.WvgGjIiFPBU
[218] *Id*.
[219] Lilian Edwards and Michael Veale, *supra* note 176, p. 26
[220] *Id*., p. 29

would be very hard for him to understand. However, after GDPR will come into effect, the companies will be required to be transparent and explain the operation of their AI systems.

Understanding how those AI systems work will be absolutely necessary for data subject to effectively exercise many of the rights bestowed upon him in the GDPR. Regulators themselves will also need to understand the process involved in AI systems to make sure the operation of AI is transparent and clear. Therefore, in this subsection the author will discuss what kind of transparency obligations are determined in the GDPR, provide some problematic aspects of the relationship between GDPR and AI technology in this matter and lastly, the author will provide some suggestions on how to solve these issues.

To start with Article 29 Working Party explains, that transparency in the context of Article 5(1)(a) of GDPR means that data controllers must provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data.[221] However, Article 29 Working Party concede, that individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision making processes[222].

Other relevant articles associated with transparency principle are Article 13 and Article 14 of GDPR. Article 13 of GDPR determines information to be provided where personal data are collected from the data subject and Article 14 of GDPR determines information to be provided where personal data have not been obtained from the data subject. Recital 60 of GDPR explains those rights by stating that: *"The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed."*

Transparency guidelines determine, that transparency obligation in light of Article 5(1)(a) of GDPR applies to three central areas: 1) providing information to data subjects to ensure fair processing, 2) how data controllers communicate with data subjects in relation to their rights under the GDPR, and 3) how data controllers facilitate the exercise data subject's rights[223].

[221] Article 29 Working Party, *supra* note 165, p. 9.
[222] *Id*., p. 9.
[223] Article 29 Working Party, "Guidelines on transparency under Regulation 2016/679" (WP260 rev.01, 17/EN, adopted on November 29, 2017): p. 4.
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

All in all, the principle of transparency requires that any information and communication relating to the processing of personal data be readily accessible and easy to understand, and that clear and plain language would be used.

It is important to note, that transparency applies not only at the point of collection of personal data but throughout the whole processing process, irrespective of the information or communication being conveyed[224], thus data controller must be transparent in all stages of AI processing and thus must be able to shine a light on what AI is doing every step of the way. As it will be seen later, this is no easy task to accomplish.

For automated decision making, including profiling, the rules about what information to provide are a little bit different. Information, that data controller must provide to data subject include meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject[225].

After brief overview of transparency principle, the author now turns to challenges and problems associated with the problematic relationship between transparency and AI technology.

The first problem is associated with the nature of AI technology. Jenna Burrell has stated that machine learning applies to problems for which encoding an explicit logic of the decision making functions could be done very poorly[226]. This is true as algorithms do not always behave in a predictable way[227] and are not inherently transparent. Bjorn Erik Thon and Catharina Nes rises a similar question which really digs deep into the core issue of AI systems - "*Just how transparent can an algorithm-based decision making process be*"[228]. Currently, many AI systems are very difficult for users or even developers to understand[229].

Of course it is dependent on the AI computational learning model company or other entity uses. For example, some models can act as, already discussed in previous chapters, "black boxes". The decision making process of these "black boxes" are not easy to understand and in many cases it is impossible to track their work. This is especially true when discussing neural network type of algorithms, such as algorithms with deep learning capabilities. Usually conclusions, that are reached by neural networks are not deductible and therefore cannot be explained through deductive measures by highlighting the impact of various factors at the input

---

[224] Article 29 Working Party, *supra* note 223, p. 6, 10, 16.

[225] Article 13(2)(f) and Article 14(2)(g) of GDPR.

[226] Jenna Burrell, "How the machine "thinks": Understanding opacity in machine learning algorithms," *Big Data and Society* 3(1) (2016): p. 6.
http://bds.sagepub.com/content/spbds/3/1/2053951715622512.full.pdf

[227] Kate Crawford, *supra* note 136, p. 77, 82-83.

[228] Bjorn Erik Thon and Catharina Nes, *supra* note 207, p. 2.

[229] Robert van den Hoven van Genderen, "Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics," *European Data Protection Law Review* 3(3) (2017): p. 348,
http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/edpl3&div=62&start_page=338&collection=journals&set_as_cursor=0&men_tab=srchresults

stage to the ultimate conclusion[230]. Therefore, it would be nearly impossible to try to explain the logic involved in making decisions by AI to data subject as even the data controller could hardly fathom the intricacies of this type of AI system.

The second problem with transparency arises, when considering online learning AI systems. These algorithms are able to update their prediction models after each consequent decision, incorporating each new observation as part of their training data, even knowing their source code and the inserted data is not nearly enough to replicate or to predict their behavior.[231] Therefore, it would be very hard or nearly impossible to satisfy the criteria of explaining possible significant and envisaged consequences of the AI decision making process as these consequences are reached by complex learning and updates.

The third problem is associated with the core of many AI businesses. The AI algorithms and models usually are protected as intellectual property or are considered as trade secrets. This pre-establishment creates several issues. Firstly, how can a company operate in transparent fashion if its software, AI algorithms or models are essentially hidden and protected from public scrutiny and regulators cannot access them. Secondly, in a situation where a data subject disagrees with the decision of the AI and wants to use his right to object and sue the company for discrimination or for another reason, how could he effectively exercise such a right without knowing precise inputs and outputs to any AI system with machine learning capabilities[232]. Furthermore, are the judges have enough expertise and are they ready to analyze complex AI models of companies in order to decide whether AI system made a right decision or who is at fault.

But the higher degree of AI algorithms transparency could also not be the key. As Kate Crawfords puts it there are two problems with algorithms transparency[233]. First of all, companies such as Facebook, Google or Amazon would not reveal their a proprietary workings of their AI systems for fear of losing their competitive edge and of fear that users could try to game the system[234]. Secondly, there is a transparency paradox: revealing how an algorithm works, even if it were possible to predict consistently, would mean revealing information, handling practices in ways that are relevant and meaningful to the choices individuals must make and if one did so, describing every flow, condition, qualification and exception, we know that it is unlikely to be

---

[230] David R. Warner Jr., "A Neural Network-based Law Machine: the Problem of Legitimacy," *Law, Computers and Artificial Intelligence* 2(2) (1993): p. 138, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/infctel2&div=17&start_page=135&collection=journals&set_as_cursor=0&men_tab=srchresults

[231] Joshua A Kroll and others, *supra* note 203, p. 17.

[232] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 19.

[233] Kate Crawford, *supra* note 136, p. 87.

[234] *Id*., p. 87.

understood, let alone read by the data subject[235]. In the end, this could not result in more transparency.

The fourth problem arises, then considering definitions described in GDPR. It is not clear what the regulators meant by the phrase "meaningful information about the logic". Dimitra Kamarinou, Christopher Millard and Jatinder Singh rises an important question which is yet still unanswered - does the term "logic" refer to the data set used to train the algorithm, or to the way the algorithm itself works in general, for example the mathematical / statistical theories on which the design of the algorithm is based, or to the way the learned model worked in the particular instance when processing the data subject's personal data?[236] These questions are not answered neither in Article 29 Working Party guidelines on transparency nor in Article 29 Working Party guidelines on automated decision making. Therefore, after GDPR comes into effect in May, there will be a lot of legal uncertainty as to what the aforementioned phrase really mean and what the company should be transparent about.

The fifth problem arises when considering the use of cloud computing technology and third party providers. AI's with machine learning capabilities chain of supply could be consistent of models and algorithms which are created by third party suppliers. So, for example, number of companies could be using cloud computing services without even having a specialist which understand AI with machine learning or deep learning capabilities. Therefore, these companies will need to hire such an experts in order to comply with GDPR obligations and to explain the data subject about automated decision making process.

The sixth problem is associated with transparency fallacy. As Lilian Edwards and Michael Veale state individuals are mostly too time-poor, resource-poor and lacking of specific expertise to meaningfully make use of their individual rights. Or in more extreme situations more transparency could lead to cynicism about entire industry and less caring about unfair practices. Imagine a situation where an individual seeks more information, analysis it only to come to conclusion, that he have little power to change it[237]. For example, if you find out about some strange data collection practices by Facebook, you would still need to use Facebook for social networking purposes.

Now the author will discuss possible solutions for transparency problems. One solution to the aforementioned problems would be to make documentation of the AI's decision making process. The documentation must set out, at the very least, the data categories which are applied,

---

[235] Kate Crawford, *supra* note 136, p. 87.

[236] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *op. cit.*, p. 20

[237] Mike Annany and Kate Crawford, "Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability," *New Media and Society* 20(3) (2016): p. 1, 5, 6, http://journals.sagepub.com/doi/abs/10.1177/1461444816676645

together with information about the role these categories play in the decision or decisions concerned[238]. However, documentation is not easy or sometimes possible to obtain, for example in cases where neural networks or so called "black boxes" are used for decision making.

Another option would be to reveal certain information about the logic of algorithm because many parts of AI decision making process could not considered as intellectual property right or trade secret. As Nicholas Diakopoulos have argued, that information regarding human involvement, quality of data, including its accuracy, completeness and uncertainty, to some limit the model, including the input, features or variables that are used in algorithm and etc could be made available without infringing on propriatory rights[239]. However, companies of course will be afraid to release any information regarding the model, as even if individual parts of algorithm might not be an important part, there is always a probability that somebody from competitive companies could piece this information together and thus learn more about competitor's AI system[240].

More radical fix to the problems would be to lower the intellectual property rights and trade secrets standard for AI systems. This would allow mounting a better challenge against the companies using AI and would create better "name and shame" mechanism[241] against unfair practices or manipulation of the market.

All in all, in this authors opinion transparency requirement for AI rises a lot of issues and uncertainties as the nature of AI is inherently not transparent. Furthermore, there is a big risk of creating a chilling effect for the development of AI[242]. The best strategy according to this author would be to ensure the transparency and fairness of the AI technology by using the advice of Association for the Advancement of Artificial Intelligence: "*it is critical that one should be able to prove, test, measure and validate the reliability, performance, safety and ethical compliance – both logically and statistically/probabilistically – of such RAI*[243] *systems before they are deployed.*"[244]. One of the ways to do so would to test trained model for unfair

[238] Lee Bygrave, *supra* note 171, p. 10.

[239] Nicholas Diakopoulos, "Accountability in Algorithmic Decision Making," *Communications of the ACM* 59(2) (2016): p. 57-58.
https://cacm.acm.org/magazines/2016/2/197421-accountability-in-algorithmic-decision-making/abstract

[240] Lilian Edwards and Michael Veale, *supra* note 176, p. 64.

[241] Tal Z. Zarsky, "Transparency in Data Mining: From Theory to Practice" in *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Toon Calders et al. (Berlin, Germany: Springer, 2013), p. 312-313.
https://books.google.co.id/books?id=Ricr1ZHnlWcC&pg=PA303&lpg=PA303&dq=Transparency+in+Data+Mining:+From+Theory+to+Practice&source=bl&ots=xgmXtUrxuM&sig=Z5MOEgUKKHbN6g6r31WlNGEnEQA&hl=id&sa=X&ved=0ahUKEwiQurCavoTbAhVJKFAKHTNtBPsQ6AEIRTAE#v=onepage&q=Transparency%20in%20Data%20Mining%3A%20From%20Theory%20to%20Practice&f=false Accessed: April 30, 2018.

[242] Robert van den Hoven van Genderen, *supra* note 229, p. 351.

[243] RAI means robotics and artificial intelligence.

[244] Joint written evidence submitted by the Association for the Advancement of Artificial Intelligence and the UK Computing Research Committee for robotics and artificial intelligence inquiry by Science and Technology Committee of UK House of Commons.

discrimination against a number of discrimination testing datasets and AI's, or by assessing the actual outcomes of the machine learning process to prove that they comply with the lawfulness, fairness and transparency requirements[245]. So if regulators and companies could work together through testing and ex ante checking on AI capabilities, this could potentially ensure transparency, fairness and lawfulness of any AI system.

3.1.2. Purpose Limitation

In essence, purpose limitation principle ensures that processing of data is conducted for only specified purpose. However, this principle in many cases clashes with the trends in AI and more broadly Big Data industries. Generally, AI systems and Big Data analytics are based on the idea of limitless retention and collection of all data, the N=all[246]. Therefore, in this section, purpose limitation principle will be analyzed with regards to AI and Big Data.

To better evaluate purpose limitation principle, this section will be divided into several parts: 1) legal aspects of purpose limitation principle, 2) arguments for and against having this principle in the age of AI and Big Data, 3) issues and challenges of the relationship between Big Data and AI and 4) solutions, which could be adopted to solve those issues and challenges.

To start with, purpose limitation principle states that, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[247]. In order to determine if the additional processing is compatible with the original purpose, several factors must be assessed. These factors include:

- the relationship between the purposes for which the data have been collected and the purposes of further processing;
- the context in which the data were collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the data;
- the impact of the further processing on the data subjects;
- the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.[248]

---

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/robotics-and-artificial-intelligence/written/32533.html

[245] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 22

[246] Lilian Edwards and Michael Veale, *supra* note 176, p. 32.

[247] Article 5(1)(b) of GDPR.

[248] Article 29 Working Party, *supra* note 165, p. 11.

Purpose limitation is and was one of the fundamental principals of EU data protection regime for quite a long time. It was already included into Data Protection Directive[249]. Furthermore, purpose limitation concept is enshrined into EU Charter of Fundamental Rights as Article 8(2) reads: "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*" Therefore, it can be clearly seen, that purpose limitation principle was supposed to be in GDPR, otherwise it could have created a lot of legal uncertainty and clashes with other important EU legislation.

Even though as it will be later shown in this Master Thesis, that purpose limitation principle clashes with development of AI and Big Data environment, some legitimate rationale could be find in applying this principal in the age of AI and Big Data.

First of all, Article 29 Working Party in their opinion on purpose limitation stated, that the purpose limitation principle is necessary in preserving trust and legal certainty because then the data subject shares it's personal information, he or she has a legitimate expectation about the purposes for which the data will be used[250]. Therefore, such a principle promotes trust in data analytic environment as well as competition[251], as purpose limitation principle weakens data companies monopoly on the market and allow smaller companies or start-ups to compete in the free market environment.

Secondly, purpose limitation principle allows data subjects to exercise at least some amount of control over their own personal data. Therefore, when they share their data with the data controller, they know, that data controller will not use the personal data for whatever purpose they want but only for the purpose the data subject consented to. Thus ensuring that power over personal data stays with the data subject all the time.

However, Tal Z. Zarsky believes[252], that both of these arguments for purpose limitation are not beyond debate and have some issues in the age of AI and Big Data, therefore they must be carefully scrutinized and evaluated.

First of all, it could be said, that in this technological age, where we share our personal information on multiple digital public forums without even reading terms and services, data subjects objectively surrendered control over their own personal data. For example, Jonathan Obar and Anne Oeldorf-Hirsch, created a new social network NameDrop, which terms of services stated, that the user agrees to give their first born child to NameDrop. Only quarter of

[249] Article 6(1)(b) of Data Protection Directive.
[250] Article 29 Working Party, "Opinion 03/2013 on purpose limitation" (00569/13/EN, WP 203, adopted on April 2, 2013), p. 4.
[251] Tal Z. Zarsky, *supra* note 47, p. 1007.
[252] *Id*., p. 1007.

new users read the terms of services[253] and even fewer of them noticed the strange clause. Furthermore, Eurobarometer survey on personal data showed, that 31% of EU citizens feel, that they have no control over their personal data online, while 50% more believed they only have partial control[254]. Therefore, it could be said, that people on the internet know that they have little control over their personal data and are not generally concerned with protecting their own privacy rights and information, if they get something beneficial in return like using social media.

Secondly, other options could be used to promote trust and competition in data markets and environment. For example, closely monitoring and tracking data usage by companies, rather than blocking analyses ex ante.[255] It could be also argued, that sometimes purpose limitation principle could even act to the contrary of promoting competition and disincentives start-ups to compete with big Big Data companies. Start-ups could lose the ability to compete in secondary data markets and to use it as a foundation to enter new areas of business[256]. This is because purpose limitation principle guarantees that only the Big Data monopolies that already have an established base of clients, can eventually receive proper authorization from the data subjects to proceed with the data analysis because those data subjects are already clients of the monopoly and want to continue using their services[257].

All in all, in order to understand how to improve purpose limitation principle or whether this principle is even necessary to apply for AI technology in the age of Big Data, the author needs to look and analyze the issues, that this principle create for AI technology.

First of all, it must be stated, that purpose limitation principle is clearly at odds with the way Big Data analyses are conducted[258]. In today's world, AI analytical capabilities are applied to evaluate huge data sets and this analysis is very different from how scientific method was used in the past. If usual scientific method begins with a question or hypothesis, then the collection of relevant information in order to answer the question or prove the hypothesis right or wrong, then the Big Data analysis is very different. In Big Data analyses, the data is being collected and

---

[253] David Berreby, "Click to agree with what? No one reads terms of service, studies confirm," *The Guardian,* March 3, 2017, https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print

[254] "Data Protection Eurobarometer", European Commission, June 2015, https://perma.cc/3XLK-VKA6

[255] Tal Z. Zarsky, "Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society," *Maine Law Review* 56(1) (2004): p. 33, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/maine56&div=7&start_page=13&collection=journals&set_as_cursor=0&men_tab=srchresults

[256] Tal Z. Zarsky, "The Privacy-Innovation Conundrum," *Lewis and Clark Law Review* 19(1) (2015): p. 136, http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/lewclr19&div=7&start_page=115&collection=journals&set_as_cursor=0&men_tab=srchresults

[257] Tal Z. Zarsky, *supra* note 47, p. 1007.

[258] *Id*., p. 1005;
"Big data, artificial intelligence, machine learning and data protection", UK Information Commissioner's Office, 2017, p. 37-39, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf;
Elizabeth E. Joh, *supra* note 44, p. 40-41.

stored all the time, thus research questions or hypothesis do not have to shape or limit data collection at all[259]. More data for AI means more chances and ways to find hidden correlations between sets of data, which were not imagined before gathering the data. Therefore, compared to scientific method this Big Data process is upside down.

As Viktor Mayer Schonberger and Kenneth Cukier argues, today with so much data around and more to come, hypothesis are no longer crucial for correlational analysis[260]. Therefore, it could be said, that hypothesis and search for causality are no longer important given the insights that can be derived from correlations found in Big Data[261]. For example, Google's mathematical models have identified 45 search terms most associated with historical flu data[262]. The resulting systems of Google Flu Trends has became very precise in matching the historical surveillance data collected by the USA Centers for Disease Control[263]. Thus, the company can predict flu outbreaks by simply identifying correlations, much in the same way that Amazon's algorithms can predict that you might like a product based on it's analysis of your shopping data without caring why[264]. Therefore, a serious discussion must be held by regulators to determine whether this change in processing is more beneficial than strict purpose limitation principle.

The second problem arises in regards to aforementioned analysis of Big Data process. The Big Data analyses involve methods and usage patterns which neither the data controller who collects the data nor the data subject even imagined before it started. Therefore, Big Data companies, in order to comply with purpose limitation requirements, will have to notify data subjects about what kind of processing they will engage in the future and closely monitor AI systems to abide by this principle, and not exceed what the GDPR permits them to do. Carrying out any of these tasks might prove costly, difficult or even impossible[265]. Thus, purpose limitation principle could have a chilling effect on Big Data industry and AI technologies development in Europe. GDPR should strive to promote data subjects data protection rights without infringing on the development of the industry.

Even if companies try to circumvent this limitation by stating a rather broad and vague purpose for the future processing of personal data, it would not help them as such practice would be considered against the law and illegitimate. Purpose limitation principle states that any

---

[259] Elizabeth E. Joh, *id*., p. 40.

[260] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data - A Revolution That Will Transform How We Live, Work, and Think* (New York, USA: Houghton Mifflin Harcourt Publishing Company, 2013): p. 61, https://books.google.lt/books?id=HpHcGAkFEjkC&printsec=frontcover&hl=lt&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[261] *Id*., p. 2.

[262] *Id.*

[263] Miguel Helft, "Google Uses Searches to Track Flu's Spread," *The New York Times*, November 11, 2008, http://www.nytimes.com/2008/11/12/technology/internet/12flu.html

[264] Elizabeth E. Joh, *supra* note 44, p. 42

[265] Tal Z. Zarsky, *supra* note 47, p. 1007.

purpose must be specific and explicit, therefore vague purpose would be seen as infringing upon the GDPR and not legitimate[266].

However, there is a some sort of solution to this problem. If one reads the purpose limitation text in the GDPR carefully, one could see that the phrase "*and not further processed in manner that is incompatible with those purposes*"[267]. This means, that even if further processing goes beyond the original purpose, it still could be in accordance to the obligations of GDPR as further processing is allowed if it is compatible with the purposes of original processing.

When assessing compatibility of Big Data processing, Article 29 Working Party stated, that the aforementioned factors should be considered: 1) the relationship between the purposes for which the data have been collected and the purposes of further processing, 2) the context in which the data were collected and the reasonable expectations of the data subjects as to their further use, 3) the nature of the data and the impact of the further processing on the data subjects, 4) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects[268]. These factors are determined in Article 6(4) of GDPR and they state what safeguards could be used to establish compatibility in regards to purpose limitation principle. However, as it will be later seen, they are not easy to follow for companies, which use Big Data analysis and AI systems.

Let's consider some of these factors as examples. First of all, data controller must consider the context in which personal data was collected[269]. However, such safeguard is hard to be followed in Big Data world as AI systems collects and analyzes data in different and distant contexts. Secondly, data controller must consider the nature of personal data[270], but this is difficult to do as nature of data is constantly in flux when applying Big Data measures and thus not easy to determine[271]. Lastly, data controller must consider pseudonymisation[272]. This suggestion also creates some challenges for the Big Data companies, as this measure could really hurt the quality of the data and without identifiable features the results of Big Data analysis could become much less precise, efficient and accurate, thus hurting all the Big Data industry in the process as consumers would not trust industry, which is not efficient. Each of these safeguards are difficult to execute, somewhat complex and could hurt the precision of AI systems. For example, Article 29 Working Party clearly states, that when the processing involves health data, further processing for different purposes is strictly limited and the data controller

[266] Article 29 Working Party, *supra* note 250, p. 17, 52.
[267] Article 5(1)(b) of GDPR.
[268] Article 29 Working Party, op. cit., p. 23-27.
[269] Article 6(4)(b) of GDPR.
[270] Article 6(4)(c) of GDPR.
[271] Tal Z. Zarsky, *supra* note 47, p. 1008.
[272] Article 6(4)(e) of GDPR.

must define clear compatible and legitimate purposes of the data processing[273]. However, in order for AI to be efficient in medical fields it needs as much information about medical history of as many people as possible.

Furthermore, the Article 29 Working Party identified two scenarios associated with further using of personal data for analytics and determined relevant safeguards associated with these scenarios. First scenario: the organizations processing the data want to detect trends and correlations in the information. Second one, the organizations are interested in individuals[274].

In case of first scenario, data controller would need to guarantee confidentiality and security of data. Furthermore, he would need to take all necessary technical and organizational measures to ensure functional separation.[275] Functional separation "<...> *means that data used for statistical purposes or other research purposes should not be available to 'support measures or decisions' that are taken with regard to the individual data subjects concerned (unless specifically authorized by the individuals concerned).*"[276] Therefore, in the first scenario, security, confidentiality and functional separation would be the key for ensuring compatibility of further processing with purpose limitation principle. However, a lot of AI processing is associated with making decisions or is being used as recommendations for decisions.

In case of second scenario, when organization wants to analyse or predict behaviour, attitudes or personal preferences consent would be the key to ensure compatibility. Free, specific, informed and unambiguous "opt-in" consent would almost always be required and most importantly, consent should be required, for different types of processing like for tracking and profiling for purposes of behavioural advertisement, direct marketing, data-brokering, location-based advertising or tracking-based digital market research[277]. As we already discussed in lawfulness section, to obtain specific and informed consent is almost impossible in the age of AI.

In any case, if Big Data company would further process personal data for statistical purposes, such purpose would satisfy compatibility requirement and will be in accordance to Article 5(1)(b) of GDPR. However, appropriate safeguards in accordance with Article 89(1) of GDPR must still be applied even if Big Data company wishes to use statistical purpose exception. Article 89(1) of GDPR states, that: "*safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data*

[273] Article 29 Working Party, "Annex – health data in apps and devices", February 5, 2015, p. 6, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

[274] Article 29 Working Party, *supra* note 250, Annex 2, p. 46.

[275] *Id*.

[276] *Id*., p. 30.

[277] Article 29 Working Party, *supra* note 250, Annex 2, p. 46.

minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

Despite all of these challenges according to Tal Z. Zarsky greatest challenge to relying on statistical purpose exception could be found in Recital 162[278]. Recital 162 determines, that "*The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person".* Because substantial portions of Big Data processes are directly impacting individuals and providing them specific treatment or are supporting decision making, whether it would be for direct marketing or for other reasons, statistical purposes exception would not apply to these Big Data companies. Therefore, purpose limitation principle would still apply in all of its powers.

In any case, some solutions could be considered to help ease the pain of regulation to Big Data and AI industry. First of all, fairness test could be considered with regards to data subjects expectations.[279] This would help ensure, that purpose limitation principle do not hurt the development and efficiency of the Big Data and AI industry. However, this process would be very subjective and hard to technologically adopt as it would require complex testing systems.

Second of all, purpose limitation principle could be adopted narrowly, however, this would really hurt this principle's application to other industries and might lower protection and control of personal data. Therefore, there would be a need for a new AI specific regulation to help adopt this narrow application. However, even with this new regulation, the narrow application of purpose limitation principle could be incompatible with other EU legal documents.

All in all, purpose limitation principle could potentially limit the precision, efficiency and effectiveness of AI industry, as AI needs a lot of data to learn and provide good analysis. The regulators need to reevaluate this principle and to determine what scope and how it will be applied in the age of AI and Big Data.

3.1.3. Data Minimization

Data minimization is very important and fundamental principal of data protection law inside the EU and is used as an example for other countries who want to protect their citizen's data from broad processing. However, this principle also clashes with AI technology in the age

[278] Tal Z. Zarsky, *supra* note 47, p. 1008.
[279] UK Information Commissioner's Office, *supra* note 258, p. 37-39.

of Big Data and thus must be carefully scrutinized to reveal challenges and problems associated with this principle.

Therefore, in this section the author will determine what is data minimization principle, what elements it includes, arguments for and against data minimization principle in the age of AI, what kind of challenges and problems are associated with this principle and lastly, the author will try to determine possible solutions or some recommendations in order to limit the impact of data minimization principle to AI development in EU.

Article 5(1)(c) of GDPR determines, that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In short, this principle is called data minimization principle and it is designed to limit the overreach of companies who want access personal data of EU citizens.

Compared to purpose limitation principle, the data minimization principle is not enshrined in EU Charter of Fundamental Right, thus giving regulators much greater autonomy to define what we consider data minimization and to determine the edges of this principle. This leniency will be taken into account then considering recommendations.

Even though data minimization principle is not mentioned in EU Charter of Fundamental Rights it was an important part of Data Protection Directive. Article 6(1)(c) of Data Protection Directive stated, that personal data must be: "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*". This provision is quite different from the one in GDPR. The main difference is that Data Protection Directive have a phrase "not excessive in relation" rather than "limited to what is necessary in relation". Detlev Gabel and Tim Hickman argues, that this change expanded the reach of data minimization principle as the language used in GDPR allows and requests more scrutiny over how the data controller is handling personal information[280].

As Tal Z. Zarsky explains this principle pertains several dimensions: it relates to the scope and categories of data initially collected, and it also refers to the limited duration during while personal data may be retained and the requirement that such data be deleted after it intended use[281].

European Data Protection Supervisor reaffirms such dimensions and states, that data controller must retain the data only for as long as is necessary to fulfill that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it

[280] "GDPR Handbook: Unlocking the EU General Data Protection Regulation", White and Case, Chapter 6: Data Protection Principles, 2017, http://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-dataprotection

[281] Tal Z. Zarsky, *supra* note 47, p. 1009.

only for as long as they need it[282]. The limited retention principle is very important in EU case law and it was upheld numerous amounts of time, including in the famous Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others[283].

The underlining rationale for the data minimization principle was what data subject will get more control over their personal data. And it is indeed the case as the data controller due to this principle will have only limited uses over personal data and for a not very long period of time. Thus the data controller will have fewer chances to overreach and misuse personal data.

Furthermore, limited retention of data also insures that data subject's data has less chances of being hacked or stolen. If companies would retain personal data for unlimited periods of times and for any purpose they want, this would increase the possibility of data subject's personal data being stolen or hacked by either internal personnel or external sources. This is especially troubling if these companies are allowed to amass huge amounts of personal data in one place. This could hurt data subjects very badly. For example, recently there was a huge scandal over massive data breach of USA citizen's personal data. Consumer credit reporting agency Equifax was hit with a massive hacking attack. Hackers potentially got access to sensitive information of 143 million USA citizens. The information included medical histories, bank accounts and employee accounts[284]. This scandal proves that it is not safe to amass a lot of personal data in one place for unlimited period of time.

However, this argument for data minimization principle has its drawbacks. First of all, it could be argued, that data controllers in many cases do not have sufficient incentives to have top notch cyber security in place for protecting personal data if they only retain small amounts of data for a short period of time. Providing such regulatory incentives by allowing companies to retain more data could increase the security of data and ensure data subjects that sufficient mechanisms are in place to protect their personal data against hacking attempts. Secondly, another mechanism is already in place to minimize the risk of security of personal data - ex post enforcement. This means that if data controller's systems are breached, when the data controller

---

[282] European Data Protection Supervisor, "Data Minimization", Glossary, https://edps.europa.eu/data-protection/data-protection/glossary/d_en

[283] Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Case C-293/12, ECLI:EU:C:2013:845.

[284] Tara Siegel Bernard et al., "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *The New York Times*, September 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html;
Alyssa Newcomb, "Massive Equifax Data Breach Could Affect Half of the U.S. Population," *The NBC News*, September 8, 2017, https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686;
"Equifax under pressure after data breach update", *The BBC*, February 12, 2018, http://www.bbc.com/news/technology-43033202

have to announce the breach without undue delay[285] and will face harsh penalties and fines, which should theoretically send signal to other data controllers - comply or you will get punished.

Starting with problems and challenges, it could be argued, that Big Data companies must retain data for as long as possible because of the nature of AI systems and future prospects. First of all, it will help them provide much more efficient and fairer process, if they have vast amounts of data to feed learning algorithms. The more data AI system has the better and more precise the processing of data is. Secondly, in the future retained data could be useful for analyses with much better and smarter AI. Therefore, if the company disposes that data, the society would lose the possible knowledge, that could be extracted from that data in the future. Third of all, huge amounts of personal data today could help teach complex AI how to be better in vital parts of society. For example, helping AI to solve judicial disputes[286] and becoming better doctor to determine what kind of disease a person have[287]. By not retaining this data we might be setting back years of developing such efficient systems in various fields.

Talking about the clash between data minimization principle and Big Data, it must be noted, that complying with the principle of data minimization, even at the time of the processing itself, could be quite problematic because the effectiveness of any machine learning algorithms is dependent on the access to big amount of data[288]. As already we discussed in the first chapter of this Master Thesis, context awareness is very important factor of any AI as AI can only be as efficient and smart as the access of information about its surroundings. Therefore, it could be said that data minimization principle directly clashes with potential awareness of any AI system.

Dimitra Kamarinou, Christopher Millard, and Jatinder Singh takes this idea even further and states, that as the algorithm is tasked with finding patterns within data and specifically for profiling purposes to assess data subjects based on such profiles, providing the algorithm with more data about data subjects could lead to clearer and more representative picture of him[289]. However, now data controller will only try to collect the personal data, which is necessary for specific purpose and retain such data only for a short period of time. This could lead to situation

---

[285] Article 33 and Article 34 of GDPR.

[286] Please see: Francisco Andrade et al. "Online dispute resolution: an artificial intelligence perspective", *Artificial Intelligence Review* Vol. 41(2) (2012).
https://link-springer-com.skaitykla.mruni.eu/content/pdf/10.1007%2Fs10462-011-9305-z.pdf
Andrew Griffin, "Robot Judges Could Soon be Helping with Court Cases," *The Independent*, October 24, 2016,
https://www.independent.co.uk/life-style/gadgets-and-tech/news/ai-judge-robot-european-court-of-human-rights-law-verdicts-artificial-intelligence-a7377351.html

[287] "Deep Learning for Healthcare", Nvidia, accessed 2018 April 28,
https://www.nvidia.com/en-us/deep-learning-ai/industries/healthcare/

[288] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 14.

[289] *Id*., p. 18.

where data controller will try to avoid penalties and fines by sacrificing better representation of data subject and possibly better decision making process.

Lastly, the author will provide so recommendations or solutions to the aforementioned problems in order to help ease regulatory burden on AI technology and industry.

First of all, some exceptions in the GDPR could be used to avoid full effect of data minimization principle. For example, pseudonymization, as determined in Article 25 of GDPR, could be considered. However, this option has its drawbacks, as Big Data need identifiable information to be efficient and make better decisions. If AI has a lot of identifiable data, this would help to ensure quality of data and allow AI to aggregate different datasets and use them to provide better decisions.

Secondly, data minimization principle could be applied narrowly. This could happens if new AI specific regulation would be adopted as it would be very difficult to apply data minimization principle differently to separate industries through GDPR.

All in all, GDPR data minimization principle clearly clashes with AI in the Big Data era. However, this principle is essential in ensuring, that the rights of data subjects are respected and that the data subject has at least some control over his personal data. Maybe good solution would be to interpret the data minimization principle narrowly, when considering the use of AI technology, as this technology's benefits could be enormous for society and EU citizens in the future.

3.1.4. Processing of Special Categories of Personal Data

In this section, the author will discuss special categories of Personal Data and their compatibility with AI technology. Special categories of personal data creates a strict regime for processing this type of personal data, however the stricter regime might be damaging to the benefits that the AI systems could bring to society. Therefore, this section will be designed to evaluate such a claim and will be divided into several parts: 1) the scope of special categories of personal data, 2) the issues associated with these categories and AI systems and 3) possible solutions.

To start with, Article 9(1) of GDPR determines, that "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*". Article 29 Working Party further provides, that if data are considered as health data, but mistakenly treated as "ordinary" personal

data, there is a risk that the high level of protection deemed necessary by the European legislator is undermined[290].

Even thought, Article 9(1) of GDPR prohibits processing of special categories of personal data, the Article 9(2) of GDPR provides some exceptions to this rule in situations where: 1) there is a consent from data subject, however this consent in some cases is not absolute, 2) processing is necessary for carrying out obligations or exercising specific rights in the field of employment and social security, 3) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent, 4) processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim, 5) processing relates to personal data which are manifestly made public by the data subject, 6) processing for legal reasons or then courts are acting in judicial capacity, 7) substantial public interest, 8) for some specific medical reasons, 9) for reasons of public interest in the area of public health, 10) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. These reasons are very specific and much stricter than was seen in other principles such as data minimization or purpose limitation. Most of these exceptions are based on necessity, where there is an absolute need to help individual for, for example, medical reasons.

Compared to Data Protection Directive, GDPR introduced several additional types of special categories, such as genetic data, biometric data and data relating to sexual orientation.

Justification for special categories rule is that the special categories determined in Article 9 of GDPR are something that most of the people would consider as very private information. Therefore, leaking such information or collecting this kind of information would affect data subject very negatively and could potentially harm the person the most. Additionally, due to technological and digital advances in medical technology, GDPR took a right step and included medical information into special categories, because in the current era medical information are more and more digitized and used for Big Data analysis.[291]

The first problem arises because, as stated previously, the less information and data the AI system has, the less efficient it will be and slower it will learn. Improving AI systems is especially important in field of medical science and patient care. World Health Organization reports, that medical errors and healthcare related adverse events occur in 8% to 12% of

[290] Article 29 Working Party, *supra* note 273, p. 2,

[291] Norman A. Paradis, "The Golden State Killer case shows how swiftly we're losing genetic privacy," *Vox*, May 5, 2018, https://www.vox.com/the-big-idea/2018/5/3/17313796/genetic-privacy-killer-golden-state-serial-killer-genealogy-genome

hospitalizations[292]. This is a very high number, which AI systems could help to substantially reduce if it would have a lot of personal data to improve upon.

Secondly, it must be noted, that special categories term is a slippery slope. AI capabilities to find patterns and correlations that seem unrelated are unparalleled. For example, Antoinette Rouvroy states, that it is possible, using a supermarket shopping database, to determine a person's current and future health status with a degree of accuracy comparable to that of a medical examination[293]. These profiles could be used to determine data subject's probability to get such diseases as diabetes, cancer, smoke related cancer, heart diseases, depression and etc.[294]. These abilities of algorithms could potentially infringe data subject's rights and violate Article 9 of GDPR.

AI can effortlessly shift from normal personal data to special categories of personal data. Therefore, to protect special categories of personal regulators would need real time analysis of what kind of data company, more precisely AI system, is processing. Therefore, the need to distinguish between the processing of normal and special categories of personal data encumbers AI processes that might inadvertently shift from one category to another, every one of which requires the application of a different set of legal rules[295]. The regulators need to ensure, that companies do not obtain or use such a data, however it is not clear whether GDPR establishes a sufficient mechanism to do that.

What is more, Big Data analyses could undermine the distinction between personal data and special categories of personal data. As Big Data analyses could quickly cross the lines between these two categories without an effort, the whole notion of special protection for this kind of personal data could become pointless. This ability of AI could create one of two consequences: 1) GDPR rules are imposed strictly and companies' ability to analyze in the age of Big Data would be impeded because the whole processing process will have to be controlled very strictly or 2) the rules are somewhat loosened, but in this case the whole notion of special categories becomes sort of obsolete.

Furthermore, Antoinette Rouvroy argues, that the Big Data age has given substantially different challenge of protecting from discrimination[296]. In the previous years, discrimination was happening because of intent of some agent or company, however today in the age of Big

[292] "Patient safety. Data and statistics", World Health Organization, http://www.euro.who.int/en/health-topics/Health-systems/patient-safety/data-and-statistics
"10 facts on patient safety", World Health Organization, updated March 2018. http://www.who.int/features/factfiles/patient_safety/en/

[293] Antoinette Rouvroy, *supra* note 5, p. 27.

[294] Aaron Rieke, David Robinson and Harlan Yu, "Civil Rights, Big Data and our Algorithmic Future, A September 2014 report on social justice and technology by Robinson + Yu", Robinson + Yu (2014): p. 6, http://centerformediajustice.org/wp-content/uploads/2014/10/Civil-Rights_Big-Data_Our-Future.pdf

[295] Tal Z. Zarsky, *supra* note 47, p. 1013.

[296] Antoinette Rouvroy, *supra* note 5, p. 16-17.

Data more and more discrimination happens because of data analyses mistakes and does not necessary involve intent[297]. Furthermore, practice of establishing discriminatory factors and intent are most of time unpredictable and not very stable, as the effect of discrimination might grow gradually because of analysis is compounded over time[298]. Therefore, there is the need to approach this problem differently than using old fashion methods and determining different types of categories of personal data. The focus should be on testing the AI systems before and their deployment because real time control of AI systems to see what kind of personal data they are processing is enormous regulatory burden on both companies and regulators alike.

Additional problem, which must be considered, is cost of having special categories in the age of Big Data. First of all, both regulators and courts will need to weigh in, when and if the Big Data companies processed data, which must be considered as special categories of personal data[299]. Regulators will need to use complex mechanisms and hire additional staff, which understands how AI systems operate, therefore regulation will become very expensive. Furthermore, small Big Data companies will have fewer chances two compete in such a regulator environment. This because of three reasons: 1) small Big Data companies will have to hire costly legal services in order to determine what kind of personal data they are processing and whether they are processing this type of personal data according to the law, 2) big Big Data companies can survive one or two fines if they engage in unlawful conduct, the thing that small Big Data companies cannot do, 3) if legal uncertainty continues to exist, startups will think twice to do their business in Big Data industry because of probability of breaking the law and having to pay substantial amount of fines.

Tal Z. Zarsky also believes that protection for special categories of personal data might be diluted. He states, that "*If almost all data might fall under the "special" category, the signal and message this regulatory framework provides regarding the higher level of privacy due to special categories is subsequently diluted*"[300]. It is certainly could be the case if the AI systems would start to process data, which seemingly do not fall into the special categories of personal data but ends up finding patterns and correlations which falls into special categories of personal data or comes up with results, which were reached by taking special categories of personal data into consideration.

Obvious solution to issues associated with the special categories of personal data would be to erase such a provision. Some authors already argue that this distinction between types of personal data is no longer meaningful, as it is more and more unclear whether data are sensitive

[297] Antoinette Rouvroy, *supra* note 5, p. 16-17.
[298] Tal Z. Zarsky, op. cit., p. 1014.
[299] *Id*.
[300] Tal Z. Zarsky, *supra* note 47, p. 1014.

and the focus should be on whether the use of such data is sensitive.[301] It is indeed the case as given the practical needs this type of data will be process more often in the future. However, such a solution could be misused by Big Data companies and they could obtain a lot of sensitive information about individuals. This potentially could be used to manipulate individuals or consumers into satisfying the needs of big corporations.

All in all, in the opinion of the author of this Master Thesis, regulators must evaluate and determine the impact of Big Data and AI to the GDPR rules and decide whether keeping the term special categories of personal data is still a necessity in today's society.

3.2. Right to Notification and Access

Right to notification and right to access forms an important part of data protection framework in EU. It ensures that data subject at any point of personal data gathering and processing knows what is happening and can exercise his rights effectively. Even though the author already discussed in some form these two rights when analyzing the fundamental principles, it is still necessary to delve deeper into them and determine how those rights could be effectively exercised in the era of AI and Big Data. Therefore, in this subchapter the author will determine what is the scopes of these rights, what possible problems could these rights create in the era of AI and Big Data and lastly, some possible solutions to solve the problems of these rights.

To start with the right to notification and right to access are determined and mentioned in three separate articles of GDPR: Article 13 (Information to be provided where personal data are collected from the data subject), Article 14 (Information to be provided where personal data have not been obtained from the data subject) and Article 15 (Right of access by the data subject).

These articles determine very similar rule as to the information that must be provided to the data subject. The one major difference is that Article 13 and 14 of GDPR determines, what information data controller must provide to data subject in order to ensure fair and transparent processing, and Article 15 of GDPR determines, the right to access information. All of these article determine, that data subject must be provided with information about: "*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and*

[301] Lokke Moerel and Corien Prins, "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things," *Wolters Kluwer* (2016): p. 11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123
Tal Z. Zarsky, *id*., p. 1015.

the envisaged consequences of such processing for the data subject"[302] So the two major aspects of these provisions are that the data controller must provide meaningful information about the logic involved and significance and the envisaged consequences of processing.

Article 29 Working Party noted, that Article 13 and 14 of GDPR must be used to ensure, that the fact, that the processing is for the purposes of both (a) profiling and (b) making a decision based on the generated profile, must be made clear to the data subject.[303] Article 29 Working Party also explains, the elements of Article 13 and 14 of GDPR: 1) meaningful information about the logic involved and 2) significant and envisaged consequences[304].

Meaningful information about the logic involved means, that data controller must find ways to explain the process in simple and understandable ways to the data subject about the rationale or criteria used to come up with the decision. Furthermore, the data controller do not have to provide full explanation of his algorithms, as it could be protected by intellectual property rights or it could be considered as a trade secret. All in all, information must be sufficiently comprehensible to the data subject as to how the machine reached one decision or another[305].

Talking about significant and envisaged consequences in light of Article 13 and Article 14 of GDPR, Article 29 Working Party states, that data subject must be provided with information about intended and future processing and how the automated decision-making might affect the data subject[306]. Analogically, paragraph 75 of Draft Explanatory Report on the modernized version of Council of Europe Convention 108 states, that: "*Data subjects should be entitled to know the reasoning underlying the processing of their data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated-decision making including profiling*"[307]. The significant and envisaged consequences must be presented in such a way, that examples of real effect must be shown to the data subject.

In regards to Article 15 of GDPR, the Article 29 Working Party mentions, that the data controller must make available the data used as input to create the profile as well as access to

---

[302] Article 13(2)(f), Article 14(2)(g) and Article 15(1)(h) of GDPR.
[303] Article 29 Working Party, *supra* note 165, p. 16.
[304] *Id*., p. 25-26.
[305] *Id*., p. 25.
[306] Article 29 Working Party, *supra* note 165, p. 26.
[307] Council of Europe, "Draft Explanatory Report on the modernized version of CoE Convention 108", 2016, paragraph 75: "<…> For instance in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a 'yes' or 'no' decision, and not simply information on the decision itself. Without an understanding of these elements there could be no effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority."
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2

information on the profile and details of which segments the data subject has been placed into[308]. The controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective "weight" on an aggregate level), which is also useful for him or her to challenge the decision[309]. The controller should at the time of the start of Article 15 of GDPR obligations have already been given data subject information about existence of automated decision making, meaningful information about the logic involved and significant and envisaged consequences of such processing[310].

Furthermore, Article 15 of GDPR establishes a so called two step framework. In first step data subject must be presented with the information about whether his personal data is processed and in second step, if his/her personal data is being processed, the data controller must present the data subject with information about what kind of data is being used and information about envisaged consequences. This framework is created in order for the data subject to ensure that processing of his personal information is lawful and fair.

Legal scholars, like Sandra Wachter, Brent Mittelstadt and Luciano Floridi, separate the content of these rights into two categories:

- **System functionality** - the logic, significance, envisaged consequences and general functionality of an automated decision making system. This information includes but is not limited to decision trees, predefined models, criteria and classification structures.
- **Specific decisions** - the rationale, reasons, and individual circumstances of a specific automated decision.[311]

Also, the same authors establish another category on how these rights, determined in Articles 13, 14 and 15 of GDPR, could be usefully separated:

- An **ex ante** explanation - explanation before an automated decision making took place. This explanation can only address system functionality, as specific decision has not been yet made.
- An **ex post** explanation - explanation after the automated decision making took place. This explanation can include explanation about the system's functionality and reasons behind specific decision[312].

[308] Article 29 Working Party, *op. cit.*, p. 17.
[309] *Id*., p. 27.
[310] *Id*.
[311] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195, p. 6.
[312] *Id*.

These categories will be used throughout this subchapter, as they clearly and efficiently delineate the differences between the two separate arguments as to regards the scope, that Article 13, 14 and 15 of GDPR might have.

Turning to the scope of the Article 13, 14 and 15 of GDPR, it is important to know what the legal limits of these rights are and more importantly, whether these articles determine an obligation upon data controller to provide explanations about rationale behind specific decisions. The supposed right would force data controllers to explain how AI system reached its decisions. The problem is that automated systems can have many unintended and unexpected effects[313]. However, this author doubts the existence of a right of explanation regarding automated individual decision made about a person.

First of all, the main argument of the proponents of the idea that these three articles create an obligation for the data controller to explain the decision reached to the data subject is the Recital 71. Recital 71 reads: "*In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision."* Compared to Articles 13, 14, 15 and 22 of GDPR, Recital 71 further determines, that data subject has a right to obtain an explanation of the decision reached after such assessment however such a sentence is clearly missing from articles in the GDPR.

It is important to mention, that recitals by themself do not create a legally binding obligation to follow but rather provides guidance on how to interpret the articles[314]. Recitals have no positive powers and thus cannot create legitimate expectations[315]. While recitals may cast light on interpretation of the legal rule, however it cannot be the rule themselves[316]. Because there is no ambiguity in Article 13, 14, 15 or 22 of GDPR, one cannot say, that Recital 71 creates any obligation to explain the decision reached by automated decision making process.

---

[313] Brent Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate", *Big Data and Society* 3(2) (2016): p. 16, 27, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2909885

[314] "<…> Recitals explain the background to the legislation and the aims and objectives of the legislation. They are, therefore, important to an understanding of the legislation which follows."
"Guide to the Approximation of European Union Environmental Legislation. Annex I. How to interpret environmental legislation," European Commission, August 17, 2015,
http://ec.europa.eu/environment/archives/guide/annex1.htm
Judgment of May 15, 1997 of P Textilwerke Deggendorf GmbH (TWD) v Commission of the European Communities and Federal Republic of Germany, European Court of Justice C-355/95, p. 21.

[315] Tadas Klimas and Jurate Vaiciukaite, "The Law of Recitals in European Community Legislation," *ILSA Journal of International and Comparative Law* 15(1) (2008): p. 32-33,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604

[316] Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung, Case 215/88, ECLI:EU:C:1989:331.

Historical analysis also supports this idea, because there was a proposition to include the right to obtain an explanation of the decision reached after such assessment[317]. However, such an inclusion was dropped. The European Parliament's preferred text included the right to obtain an explanation of the decision reached after such assessment and thus such safeguard would have been part of Article 22 of GDPR, which would be legally binding[318]. Clearly, this shows the intention of legislators not to include such a right into final text of GDPR.

What is more, Article 29 Working Party stated, that "*the controller should provide the data subject with information about the envisaged consequences of the processing, rather than an explanation of a particular decision*"[319]. This means there is no right of explanation for decision already made by automated decision making process.

Furthermore, previous Data Protection Directive also did not provide this right. Data subjects were entitled to receive additional information about the system functionality of an automated decision making system, but very little or no information about the criteria or rationale of a specific decision[320]. The European Commission report in 2010 also reflects this, noting that the language used in the Data Protection Directive reflects a very narrow scope of applicability for the right of access due to a number of exceptions and limiting or overriding interests[321]. This shows, that even from previous legislation, it is clear, that law makers did not intend to create a right to explanation for specific decision.

However, there is a legitimate argument that companies should explain how they reached a decision. This argument is associated with the right to contest decisions[322]. Without an explanation of how did the AI reached its decision, it would be very hard or nearly impossible for the data subject to object decisions in courts because data subject would not have any evidence or decision itself. This directly would clash with the right to fair trial and effective remedy, determined in Article 47 EU Charter of Fundamental Rights and Articles 6 and 13 of European Convention of Human Rights.

All in all, in this authors opinion because the language in the Article 13, 14 and 15 of GDPR do not determine the right to receive explanation about specific decision and because the law makers scrapped such suggestion from the official text and only left it in Recital 71, it would be logical to believe, that the GDPR does not determine the right to receive explanation about

---

317 Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195, p. 12.

318 *Id*.

319 Article 29 Working Party, *supra* note 165, p. 27.

320 Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *op. cit*., p. 21.

321 Douwe Korff, "New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments", European Commission DG Justice, Freedom and Security Report, 2010, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638949

322 Article 22(3) of GDPR.

specific decisions. The following paragraphs will reflect this logic and will not take this right into consideration.

Talking about problems associated with notification and access duties determined in Article 13, 14 and 15 of GDPR, it is important to mentioned, that notification duties have a lot of loopholes, which could be and are misused in the era of AI and Big Data. First of all, it is not clear whether the loophole, through which automated processes that merely produce evidence for decision making, rather than actually making decisions, and thus are not subject to the right of access[323], have been fixed. For example, if AI comes with some evidence about person's creditworthiness and human makes a decision, are the notification duties still apply.

Secondly, the notification duties are limited by the data controllers right to protect his intellectual property and trade secrets. Recital 47 of GDPR states, that these rights should be protected. Recital 61 of GDPR goes even further and determines: "*That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.*" Most of the AI software, which companies uses are protected by intellectual property and are not shared with anybody, therefore data subjects right to information could be very limited and if one goes even further his right to object would be basically useless. The important thing to note here is that Recital 63 only states that data controller must not deny all the data, which is not very protective of data subjects rights.

Thirdly, the notion of solely made is very vague and could potentially rise a lot of issues. As Lee Bygrave noted decisions made by humans but coming from automated data processing operation the result of which is not actively assessed by either that person or other persons before being formalized as a decision, would not fall under the scope of automated decision making.[324] How the notion of solely will be interpreted in the future is not very clear.

In this regard, Article 29 Working Party stated, that solely automated decision making is the ability to make decisions by technological means without human involvement[325]. In any case, data controller is not allowed to pretend, that there is a human involvement. For example, if a person just applies decisions made by machines, it will not count as human interference and all the relevant articles to automated decision making process would still apply. Furthermore, to qualify as human involvement, the data controller must ensure that any oversight of the decision is meaningful rather than token gesture[326] and the oversight should be conducted by someone who

[323] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195, p. 27.
[324] Lee Bygrave, *supra* note 171, p. 9.
[325] Article 29 Working Party, *supra* note 165, p. 8.
[326] *Id*., p. 21.

has the authority and competence to change the decision made by machine[327]. However, many companies could have such a person, who can change the decisions, but what happens if he/she only applies recommendations made by AI and how to control such a misuse. Note, that there is a psychological phenomenon called "automation bias", where person, who makes decisions, either over rely or under rely on the recommendations provided by the AI[328]. It is not clear how this human involvement would be controlled and regulated. Despite these explanations by Article 29 Working Party, the notion of solely made remains quite vague and could potentially create lot of problems and generate legal uncertainty, especially in the era of Big Data and AI.

Some solutions to the aforementioned problems should be considered whether as an amendment of GDPR or by explanation of existing provisions by Article 29 Working Party. This is very important as the companies which operate in Big Data age and have AI systems must be certain of what the law requires from them. If the law requires explanation of specific decision, the companies must try to change their AI infrastructure and ensure that AI is indeed explainable, that is to say, build explainable AI. Without legal certainty these companies might bear heavy fines or forego severe and costly changes to their AI systems. Furthermore, it could stifle the growth of AI and Big Data industries as the startups or new companies would not be so eager to go to this field of industry and compete due to legal uncertainty. Therefore, in the following paragraphs below the author will try to provide at least some recommendations or solutions as to how the aforementioned problems could be solved.

First of all, law makers should decide and end the debate whether right of explanation of individual decisions made by automated decision making process exist or not. Including this right into Article 13, 14, 15 or 22 of GDPR would be one way to go. Another way would be for Article 29 Working Party to state, that such a right does not exist. Recital 71 is really confusing when read with Article 13, 14, 15 and 22 of GDPR, and thus creates legal uncertainty, which is never good thing for data controllers, data subjects and regulators alike. One more way, would be to allow Member States to implement the law on top of the GDPR that requires an explanation of specific decisions, that is to say provide stricter rules. Furthermore, precise and clear requirements should be developed to determine what exact information data controller must provide to the data subject if right to explanation of specific decision indeed exists.

Second of all, meaning of meaningful information about the logic should be explained. For example, the text in the Article 15(1)(h) of GDPR is quite vague and should be clarified even more. Language should be added to clarify that Article 15 of GDPR is intended either as a counterweight to Articles 13 and 14 of GDPR, and thus provides a limited right to be informed

[327] Article 29 Working Party, *supra* note 165, p. 21.
[328] Lilian Edwards and Michael Veale, *supra* note 176, p. 45.

about the existence of automated decision making as well as system functionality, or as a right to explanation of specific decisions[329].

Third of all, some clarification should be made as to what constitutes decisions that are solely made by automated decision making process. This notion of solely is not very clear in practice. Article 29 Working Party explanations is this case does not help as it needs more guidance and practical examples for data controllers to follow. The legal loophole by which if a human at least at any stage of processing interferes into automated process means, that process is not based solely on automated decision making, should be closed[330]. One solution to this problem would be change the notion "solely" to "predominantly or solely", and determine what is considered predominantly by providing specific examples.

Fourth of all, Sandra Wachter, Brent Mittelstadt and Luciano Floridi offers an interesting solution to limitation of intellectual property rights and trade secret. These legal scholars suggest that an external auditing mechanism for automated decision making should be introduced, or internal auditing requirements for data controllers must be set[331]. Any right of notification could be severely limited by trade secrets and intellectual property rights, therefore there is a need to ensure the protection of data subject rights and personal data without infringing upon data controllers intellectual property rights or trade secrets.

Another option would be a third party evaluation. The third party could be provided with explanations about individual decisions and ensure that the process was fair. In this case, there is an oversight over data controller and also protection of data subject's privacy. This job could be given to Member State supervisory authorities, to European level supervisor or to completely new agency in EU. They could inspect AI systems before they are deployed in the markets and after they are started to be used.

All in all, some authors have noted, that GDPR appears to give strong protection against automated decision making but the protections may prove ineffectual. Therefore, the rules regarding notification and access must be clarified and more guidance must be issued.

3.3. Automated individual decision making

Lastly, we turn to Article 22 of GDPR. This article determines the data subject's right not to be subjected to a decision, which is based solely on automated processing, including profiling, which produces legal effects concerning data subject or similarly affects data subject.

[329] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195, p. 44.
[330] *Id*., p. 45.
[331] *Id*., p. 46.

In this subchapter, we will discuss the scope of this right, problems associated with it and solutions or recommendations how to solve the problems.

Analysis of this article is very important as AI and Big Data technologies gets better and more efficient, already surpassing human counterparts in many regards. Article 29 Working Party concedes, that profiling and automated decision making can be useful for individuals and companies, as it increases efficiency and saves resources[332]. Many legal scholars also note, that indeed in some cases, it might be more beneficial for a data subject if a final decision is based on automated decision making process[333].

Article 22 of GDPR is not an innovative provision, because similar provision already existed in Data Protection Directive[334]. However, this provision was mainly overlooked because of perceived non-significance and lack of potential against algorithm opacity[335]. Furthermore, this rule was rarely applied, and in many Member States was in fact a dead letter[336].

Some Member States have indeed limited Article 12 of Data Protection Directive. For example, a court ruling in Germany limited the rights of Article 12(a) of Data Protection Directive by allowing companies not to disclose information about automated processes because of protection of trade secrets[337]. This is indeed troubling as this right could be dead on arrival, as companies could quickly limit its applicability by using loopholes, such as limited human intervention into automated decision making process or by using courts to protect their trade secrets or intellectual property rights.

All in all, it could be stated, that Article 12 of Data Protection Directive did not dealt with AI systems efficiently and did not address the opacity of AI systems, therefore it is important to determine what the scope of Article 22 of GDPR holds in this regard.

Article 29 Working Party establishes, that the term right in Article 22(1) of GDPR does not mean that Article 22(1) of GDPR applies only when actively invoked by data subject[338]. This means that Article 22(1) of GDPR determines a general prohibition, which makes this provision a passive one and therefore the data subject does not need to invoke it in order for it to apply. What is more, consent requirement in Article 22(2)(a) of GDPR further highlights that Article

---

[332] Article 29 Working Party, *supra* note 165, p. 5.

[333] Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 22.

[334] Article 12(a) of Data Protection Directive.

[335] Lilian Edwards and Michael Veale, *supra* note 176, p. 44.

[336] Tal Z. Zarsky, "Transparent Predictions," *University of Illinois Law Review* 2013(4) (2013): p. 1504, 1517. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/unilllr2013&div=44&start_page=1503&collection=journals&set_as_cursor=0&men_tab=srchresults
Douwe Korff, *supra* note 321.

[337] Article 22 of GDPR.
Please see: Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195, p. 23.

[338] Article 29 Working Party, *supra* note 165, p. 19.

22(1) of GDPR is a prohibition and a passive right. This clarification is welcomed one, as some authors suggested that text of Article 22(1) of GDPR is not very clear[339].

The one major argument for prohibition of automated decision making, including profiling, is that profiling can boost existing stereotypes and social segregation, as data subjects could be denied certain services or this could lead to inaccurate predictions.

However, there are some counter arguments to this position. The regulators should supervise the building of AI and test them, if they are indeed fair and transparent before they hit the markets, rather than prohibiting them in all cases. In this way, AI's benefits would be maximized while protection would be still in place. Furthermore, such an oversight by regulators could allow avoiding biases, discrimination and unfairness more efficiently. However, it is not clear whether the GDPR could be used to create such a mechanism.

All in all, these arguments could be understood as deeper distrust for machines, AI and computerized systems[340] without sufficient evidence, which is not a good way to base the laws upon such a premise.

The first problem which arises when trying to determine what constitutes legal effects or similarly significant effects determined in Article 22(1) of GDPR. In order for an automated decision to have some sort of legal effects it must change or affect legal status of a person, however in some cases data subject does not have any legal right and therefore his status is not changed. For example, being denied an interview or credit by automated decision making process would not constitute as a change to data subjects legal status as he have no right to interview or credit.[341] Article 29 Working Party provides some clarifications to this confusion by stating, that significant effects could be such practices as automatic refusal of an online credit application or e-recruiting practices without any human intervention[342]. Furthermore, they determine that decisions that affect someone's financial circumstances, such as their eligibility to credit or decision, that deny someone an employment opportunity could potentially fall within significance category[343]. Despite this explanation, practically it will be hard for data subject to defend this right. The data subject will have to prove, that, for example, that denying him interview, counts as decision, falls within the category of significant effect and in the end he/she will have to prove, that this processing affects his/her significantly[344].

---

339 For deliberation on this topic, please see: Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195.

340 The GDPR in the Age of Big Data, p. 1017

341 Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *supra* note 195, p. 34.

342 Article 29 Working Party automated decisions, p. 21-22.

343 *Id*.

344 Hajar Malekian, "Profiling under General Data Protection Regulation (GDPR): Stricter Regime?," Linkedin, 2016, https://www.linkedin.com/pulse/profiling-under-general-data-protection-regulation-gdpr-malekian/

Furthermore, Tal Z Zarsky notes, that there are several clashes between Article 22 of GDPR and Big Data developments. First of all, prohibiting automated analysis obviously undermines many of the Big Data benefits, such as efficiency and the development of AI technology. Second of all, even if one exception to the prohibition on automated decision making is met, the specific provisions which call for human response to the machines' decisions are still required and to meet these obligations, Big Data and AI processes must be conducted in a manner that would assure they are interpretable to humans, so they can be explained to the inquiring individual and constantly meeting an interpretability requirement could make those people who design the systems to sacrifice system's precision and efficiency for ability to deliver explanation to humans[345]. Third of all, allowing human interference would further encumber the automated process and slow down the innovative technologies they bring about[346].

This could be indeed the case as the prohibition to the automated decision making processes in itself is stating, that automated decision making systems are to be distrusted, even though their potential to be much more efficient and fairer than humans could be is undeniable.

It is important to remember, that if data controller infringe upon the right of data subjects, the Article 83(5)(b) of GDPR would apply and data controller would be subjected to "*to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*". These fines are significant and quite high. Therefore, the law must be very clear and without any legal uncertainty or possible loopholes.

Furthermore, in the face of potential penalties of this magnitude and considering the complexities of AI system, data controllers may be reluctant to use the technology for automated decision making in certain situations[347]. However, there could be some benefits to this situation, as the data controller would insist to any service providers in a AI supply chain, that contract between them must contain specific provisions including safeguards and compatibility requirements and obligations laid down in the GDPR.

Another problem, which regulators must consider is the effectiveness of Article 22 of GDPR. Many authors called Article 15 of Data Protection Directive rarely enforced, poorly understood and easily circumvented[348]. Article 22 of GDPR did not change significantly,

---

345 Tal Z. Zarsky, *supra* note 47, p. 1017.

346 *Id*.

347 Dimitra Kamarinou, Christopher Millard, and Jatinder Singh, *supra* note 26, p. 16.

348 Izak Mendoza and Lee A. Bygrave, "The Right Not to Be Subject to Automated Decisions Based on Profiling," University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20, 2017, p. 2. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855
Lee Bygrave, *supra* note 171, p. 13-14.

therefore there is a legitimate risk, that Article 22 of GDPR will also become ineffective and just a blank statement.

One solution to aforementioned problem regarding the notion significant would be to clarify and provide further guidance with practical examples. As it stand now the term is very vague and practical examples provided by Article 29 Working Party only touches on hypothetical situations which could fall within this category. Furthermore, the problem in regards to proving the significant effects by data subjects, who has very limited insight into the system, requires more guidance and further development.

Another solution would be for Member States to take action and lead the debate by providing inquiries or by offering future improvements. One example of such an initiative is UK's House of Commons' Science and Technology Committee's inquiry on "algorithms in decision-making,"[349] which gathered expert opinion and developed suggestions in regards to seeking accountability and transparency in algorithmic decision making. This inquiry identified relevant difficulties associated with transparency, mechanisms for supervision and contemplated about how to make decisions explainable. This kind of initiative is a good example on how Member States could lead the debate about the scope, limits and better oversight mechanism in the age of Big Data and AI. Too bad, UK is leaving the EU.

All in all, prohibition of automated decision making is not a welcomed provision, as it directly clashes with AI systems, which are design to improve decision making in various irreplaceable fields such as medicine and finance. The regulators must determine and reevaluate whether Article 22 of GDPR still represent the needs of society or is it just a barrier for a better, more fairer society.

[349] UK House of Commons Science and Technology Committee, "Algorithms in decision-making inquiry launched", February 28, 2017, http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2015/algorithms-in-decision-making-inquiry-launch-16-17/

CONCLUSIONS

This Master Thesis was based on the hypothesis, that GDPR is not a proper regulation for protecting data privacy in the age of AI. The author strongly believes, that the aforementioned hypothesis was confirmed due to the following reasons below.

1. First of all, it is important to mention, that GDPR is not suitable for regulating AI because GDPR in no shape or form address or even mentions the terms AI or even Big Data. This is troubling as AI in the era of Big Data poses new challenges, which were stipulated in third chapter of this Master Thesis. Any good regulation should address the issues associated with this massive technology. This lack of addressing violates the first criteria of good regulation - necessity, as it was very clear from the third chapter of this Master Thesis, that AI systems creates a lot of issues in regards data privacy and is somewhat incompatible with the GDPR, therefore requires provisions dedicated to it. Obviously, the AI technology is wide spread and influential, therefore it needs to be regulated in order to ensure maximum benefits for society and highest possible protection of data privacy. The lack of response from the EU regulators could create a situation, which would correspond to Collingridge dilemma - the industry will be so wide spread, that it would be very hard to regulate. The necessity criteria is also not satisfied by the inclusion of prohibition of automated in individual decision making. This provision was clearly not effective in Data Protection Directive and there is no clear evidence, that the same will not happen to Article 22 of GDPR. Furthermore, the need for such a provision is highly doubtful.

2. Secondly, the GDPR text creates a lot of legal uncertainty for AI industry and AI development. This situation violates another criteria for good regulation - legal certainty. There is a lack of clarity and loopholes surrounding the terms like “solely” and “significant”. Therefore, there is a need to clarify these terms and provide some guidance. Furthermore, the consent clause also rises a lot of uncertainty. The data subject must provide an informed and specific consent for processing, however neither GDPR nor Article 29 Working Party determine how such a consent could be achieved against opacity and unexplainability surrounding AI technology.

3. Thirdly, many rights and obligation determined in the GDPR, go against the development trends of AI technology and in many cases against the nature of AI technology. This potentially could stifle the growth of AI industry and thus would be contrary to the growth criteria necessary for good regulation. AI systems learn by experience and constant updates, thus are hardly

understood even by their developers. What is more, AI systems work best if it has a lot of data to learn from and make efficient decisions. These characteristics of AI are contrary to purpose limitation and data minimization principles. Furthermore, unexplainability of many AI systems is not compatible with transparency principle. However, these clashes are not addressed in the GDPR and only slightly touched by Article 29 Working Party.

4. Fourth of all, the regulators around Europe and around the world still lack the capabilities of regulating AI systems. Any good regulation works only if the regulators who will execute the regulation, knows the intrinsic parts of the technology they are regulating. However, as established in this Master Thesis, the regulators are not ready or able to regulate this industry and majority of knowledge of AI industry is in the hands of several big corporations, which protect this information through intellectual property rights or trade secrets. Furthermore, there is no specific agency or institution in EU, that would deal with the AI technology. Therefore, the capability criteria for good regulation is not met in regards to GDPR. However, this situation could be fixed as regulators need to either hire more people who understand the industry or gain knowledge about the industry by consulting with major companies or with academic world.

5. Fifth of all, as the rules stands now, the AI industry will have to adopt very expensive measures to comply with the GDPR rules or change their infrastructure, or even AI designs. This is not very good for industry, which is developing. The flexibility criteria for good regulation determines, that the regulation must be as such that companies or people could use least expensive and burdensome measures to comply. The GDPR clearly is not in compliance with this criteria.

6. Sixth of all, the effectiveness and durability of GDPR could also be questioned. There is no AI specific regulation, however there are calls for such regulation. Therefore, steps have already been taking in EU to adopt, for example European Civil Law Rules on Robotics, which would have provisions on data privacy, thus some provisions of GDPR could be soon replaced or modified by AI specific regulation.

7. All in all, it could be stated, that GDPR have issues when it comes to regulating privacy in regards to AI technology. However, despite of these issues, the author believes, that with proper solutions these problems could be addressed and possible negative affects would be mitigated or completely vanish.

RECOMMENDATIONS

The author feels, that is necessary for the critique mentioned above and throughout this Master Thesis not to be without any constructive elements. Therefore, the author in the following paragraphs will formulate some possible fixes to the problems of GDPR in the age of intelligent machines.

First of all, new agency dedicated to regulating AI and data privacy must be established. This agency would have several functions in regards to AI technology. To start with, this agency would conduct ex ante testing of AI systems to ensure, that these systems are fair and without flaws before they are deployed in marketplaces. This could be done by developing AI testing AI or by running this soon-to-be-deployed AI through testing software or databases. After this procedure, the agency could have one of two powers: 1) it could deny the deployment of unsatisfactory AI systems to markets until they satisfy the requirements set by this agency or 2) it could provide certifications, meaning that if AI system is good enough it will be certified and thus enjoy limited liability, not certified AI systems would face strict liability. Second function, that this agency could have is testing the AI systems once they are deployed in the markets every certain period of time, for example every 3 years. This testing would be done secretly without companies knowing, that testing is taking place, so as to avoid situation similar with Volkswagen scandal. What is more, this agency would act as hub for sharing knowledge between companies, EU and academic fields to prepare regulators and citizens for development of AI or gain more knowledge about the AI technology. Lastly, this agency would be a supervisor in a sense, that it could look into AI systems, which are protected by intellectual property rights or trade secrets, to determine their compatibility with the rule of law or to check the complaints made by data subjects. Having this agency would ensure much more knowledgeable and more efficient protection of data privacy in EU and could act as example for other countries around the world.

Second of all, the author believes, that another regulation must be adopted for regulating data privacy in the age of AI. This regulation do not have to replace GDPR but it could act as specific regulation, which means, that GDPR would act as general regulation and new regulation would be special regulation in terms of GDPR. Therefore, if the new regulation would set certain rules, these rules would have to be followed despite of GDPR, however if there would be no rules set by new regulation, in that case the general rules in GDPR would apply. This new regulation will have to determine the AI definition (which very hard task to accomplish), decide on the scope of purpose limitation, data minimization and transparency principles, provide data privacy rules in regards to AI, so to ensure fairness, ensure, that there is an independent body,

who can check the complaints of citizens and determine if they are valid and etc. This regulation would take into account the nature of AI technology and how data privacy rules could be set without stifling the growth of AI industry.

Another possible solution for transparency would be oblige companies to create so called explainable AI's. These AI models would be able to generate criteria, which were used for reaching decisions and would provide such explanations in understandable manner. However, this recommendation have it's drawback, which regulators must evaluate. First of all, companies will need to change their infrastructure and AI designs to comply with this obligation, therefore it will be costly. Secondly, many of small AI companies would not be able from purely financial standpoint to implement this recommendation and therefore they would be forced out of the markets.

Lastly, if none of these recommendations would be adopted the regulators should consider changing or scraping the Article 22 of GDPR as it could negatively affect consumers and industry alike. Many of the arguments for this move was already discussed in the Master Thesis, however two of them bear of repeating. First of all, consumers in many industries could pay the price. As the Article 22 allows citizens not to be subjected to automated decision making, the people who choose not to be subjected to such processing would increase price for everybody because there will be a need for human processing and separate infrastructure. This would drive up the prices in such industries as insurance. Secondly, the negative connotations of Article 22 of GDPR proclaims, that automated decision making is some bad practice, which should be avoided. In the opinion of this author, the best solution would be to apply this Article 22 of GDPR only to marketing industry because it is most privacy intrusive and manipulating.

All in all, these are the possible solutions for fixing several issues, that GDPR have in regards to AI. Regulators should evaluate each one of them and determine, which of these would yield the best outcome for protecting privacy in the age of AI.

LIST OF REFERENCES

Legal Acts:

1. "Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data". O.J. L 281/32 (1995). https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046
2. "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg". Council of Europe. European Treaty Series No. 108 (1981). https://rm.coe.int/1680078b37
3. "European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics." 2015/2103 INL (2017). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN
4. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC." O.J.L (119) 46 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
5. "Convention on Road Traffic." United Nations Treaty Series 1042, 1968. https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&lang=en

Guidelines and opinions:

1. Article 29 Working Party. "Annex – health data in apps and devices." February 5, 2015. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf
2. Article 29 Working Party. "Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation." Adopted May 13, 2013. http://ec.europa.eu/justice/article-29/documentation/other-document/index_en.htm

3. Article 29 Working Party. “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.” WP251rev.01, 17/EN, adopted on February 6, 2018.
   http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
4. Article 29 Working Party, “Guidelines on transparency under Regulation 2016/679.” WP260 rev.01, 17/EN, adopted on November 29, 2017.
   http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
5. Article 29 Working Party. “Opinion 03/2013 on purpose limitation.” 00569/13/EN, WP 203. Adopted on April 2, 2013.
   http://ec.europa.eu/justice/article-29/documentation/other-document/index_en.htm
6. “Guide to the Approximation of European Union Environmental Legislation. Annex I. How to interpret environmental legislation.” European Commission. Adopted on August 17, 2015.
   http://ec.europa.eu/environment/archives/guide/annex1.htm
7. “Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data.” Council of Europe. 2017.
   https://rm.coe.int/16806ebe7a

Cases:

1. Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung, Case 215/88, ECLI:EU:C:1989:331.
2. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Case C-293/12, ECLI:EU:C:2013:845.
3. Google Spain v. Agencia Espafiolade Proteccion de Datos (AEPD) and Gonzilez, Case C131/12, ECLI:EU:C:2014:317.
4. Judgment of May 15, 1997 of P Textilwerke Deggendorf GmbH (TWD) v Commission of the European Communities and Federal Republic of Germany, Case C-355/95, ECLI:EU:C:1997:241.

Articles:

1. Andrade, Francisco et al. "Online dispute resolution: an artificial intelligence perspective." *Artificial Intelligence Review* 41(2) (2012): p. 211-240. https://link-springer-com.skaitykla.mruni.eu/content/pdf/10.1007%2Fs10462-011-9305-z.pdf
2. Annany, Mike and Crawford, Kate. "Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." *New Media and Society* 20(3) (2016): p. 1-17. http://journals.sagepub.com/doi/abs/10.1177/1461444816676645
3. Bygrave, Lee. "Automated Profiling, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling." *Computer Law & Security Review* 17 (1) (2001): p. 1-14. http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf
4. Bostrom, Nick. "How long before superintelligence?." *Linguistic and Philosophical Investigations* 5 (2006). https://nickbostrom.com/superintelligence.html
5. Bradford, Anu. "The Brussels Effect." *Northwestern University Law Review* 107(1) (2012): p. 1-68. https://pdfs.semanticscholar.org/2c55/404a1e09859c289644c517020aecd7fe48e4.pdf
6. Burrell, Jenna. "How the machine "thinks": Understanding opacity in machine learning algorithms." *Big Data and Society* 3(1), (2016): p. 1-12. http://bds.sagepub.com/content/spbds/3/1/2053951715622512.full.pdf
7. Calo, Ryan. "Artificial Intelligence Policy: A Primer and Roadmap." *U.C. Davis Law Review* 51(2) (2017): p. 420-421. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/davlr51&div=18&start_page=399&collection=journals&set_as_cursor=0&men_tab=srchresults#.
8. Coraggio, Giulio. "Artificial intelligence and machine learning: what privacy issues with the GDPR?." *The Gaming Tech Law*, 2016. http://www.gamingtechlaw.com/2016/10/privacy-gdpr-artificial-intelligence.html
9. Crawford, Kate. "Can an Algorithm Be Agonistic? Ten Scenes from Life in Calculated Publics." *Science, Technology, & Human Values* 41(1) (2016): p. 77-92. http://journals.sagepub.com/doi/pdf/10.1177/0162243915589635
10. Diakopoulos, Nicholas. "Accountability in Algorithmic Decision Making." *Communications of the ACM* 59(2) (2016): p. 56-62.

https://cacm.acm.org/magazines/2016/2/197421-accountability-in-algorithmic-decision-making/abstract

11. Frey, Carl Benedikt and Osborne, Michael A. "The Future Of Employment: How Susceptible Are Jobs To Computerisation?." *Technological Forecasting and Social Change* 114(C) (2017): p. 1-72. https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf
12. Edwards, Lilian and Veale, Michael. "Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for." *Duke Law and Technology Review* 16 (2017-2018): p. 18-84.
13. Genderen, Robert van den Hoven van. "Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics." *European Data Protection Law Review* 3(3) (2017): p. 338-352. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/edpl3&div=62&start_page=338&collection=journals&set_as_cursor=0&men_tab=srchresults
14. Guihot, Michael, Matthew, Anne F. and Suzor, Nicolas P. "Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence." Vanderbilt Journal of Entertainment and Technology Law 20(2) (2017): p. 385-456. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/vanep20&div=16&start_page=385&collection=journals&set_as_cursor=0&men_tab=srchresults.
15. Gurkaynak, Gonenc, Yilmaz, Ilay and Haksever, Gunes. "Stifling artificial intelligence: Human perils." *Computer Law & Security Review: The International Journal of Technology Law and Practice* 32, 5 (2016): 1-9. https://www.researchgate.net/publication/303782217_Stifling_artificial_intelligence_Human_perils.
16. Hutter, Bridget M. "A Risk Regulation Perspective on Regulatory Excellence." In Gary Coglianese *Achieving Regulatory Excellence,* p. 101-115. Washington, USA: Brookings Institution Press, 2017. https://books.google.co.id/books?id=XdmACwAAQBAJ&pg=PA101&lpg=PA101&dq=Bridget+M.+Hutter,+A+Risk+Regulation+Perspective+on+Regulatory+Excellence,+in+ACHIEVING+REGULATORY+EXCELLENCE+101,+101&source=bl&ots=5EcvhEQJfN&sig=PKCo3nwbgRYxkwOXE04Xq_fxB3g&hl=id&sa=X&ved=0ahUKEwjjtri2yvraAhVKvI8KHS7VCl4Q6AEIJzAA#v=onepage&q=Bridget%20M.%20Hutter%2C%20A%20Risk%20Regulation%20Perspective%20on%20Regulatory%20Excellence%2C%20i

n%20ACHIEVING%20REGULATORY%20EXCELLENCE%20101%2C%20101&f=false Accessed: April 20, 2018

17. Joh, Elizabeth E. "Policing by numbers: Big Data and the Fourth Amendment." *Washington Law Review* 89(1) (2016): p. 35-68. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/washlr89&div=5&start_page=35&collection=journals&set_as_cursor=0&men_tab=srchresults
18. Kelman, Steven. "Cost benefit analysis: an ethical critique (with replies)." In *Economics of the Environment*, Robert N. Stavins, p. 355-370. New York, USA: W. W. Norton and Company, 1981. https://www.unc.edu/courses/2009spring/plcy/240/001/Kelman.pdf
19. Klimas, Tadas and Vaiciukaite, Jurate. "The Law of Recitals in European Community Legislation." *ILSA Journal of International and Comparative Law* 15(1) (2008): p. 1-33. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604
20. Kroll, Joshua A. et al. "Accountable Algorithms." *University of Pennsylvania Law Review* 165(3) (2017): 633-706. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/pnlr165&div=20&start_page=633&collection=journals&set_as_cursor=0&men_tab=srchresults
21. Lou, Harbing. "AI in Video Games: Toward a More Intelligent Game." *Harvard University Graduate School of Art and Sciences*, August 28, 2017. http://sitn.hms.harvard.edu/flash/2017/ai-video-games-toward-intelligent-game/
22. Mason, Stephen. "Artificial intelligence: oh really? And why judges and lawyers are central to the way we live now – but they do not know it." *Computer and Telecommunications Law Review* 23(8) (2017): 213-225. http://stephenmason.co.uk/wp-content/uploads/2017/12/Pages-from-2017_23_CTLR_issue_8_PrintNEWMASON.pdf
23. Mittelstadt, Brent et al. "The Ethics of Algorithms: Mapping the Debate." *Big Data and Society* 3(2) (2016): p. 1-68. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2909885
24. Mijwel, Maad M. "History of Artificial Intelligence." *University of Baghdad* (2015): p. 1-5. https://www.researchgate.net/publication/322234922_History_of_Artificial_Intelligence
25. Moerel, Lokke and Prins, Corien. "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things." *Wolters Kluwer* (2016): p. 1-98. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123

26. Mumford, Peter. “Best Practices Setting Targets and Detecting Vulnerabilities.“ *Policy Quarterly* 7(3) (2011): p. 36-42. https://ojs.victoria.ac.nz/pq/article/view/4389/3882
27. Parson, Edward A. “Social Control of Technological Risks: The Dilemma of Knowledge and Control in Practice, and Ways to Surmount It.” *UCLA Law Review Discourse* 64 (2016): p. 464-487. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/ucladis64&div=21&start_page=464&collection=journals&set_as_cursor=0&men_tab=srchresults
28. Pichler, Mario, Bodenhofer, Ulrich and Schwinger, Wieland. “Context-awareness and Artificial Intelligence.” *OGAI Journal* 23(1) (2004): p. 4-11. https://www.researchgate.net/publication/200048737_Context-awareness_and_artificial_intelligence
29. Scherer, Matthew U. “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies.” *Harvard Journal of Law and Technology* 29, 2 (2016): p. 353-400. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609777.
30. Smith, Alex. “Big Data, Technology, Evolving Knowledge Skills and Emerging Roles.” Legal Information Management 16(4) (2016): p. 1-6. https://login-westlaw-co-uk.skaitykla.mruni.eu/maf/wluk/app/document?&srguid=i0ad8289e00000163684d8f7dcf50b21a&docguid=I9F77F630D66C11E6B79983EFE7771BC7&hitguid=I9F77F630D66C11E6B79983EFE7771BC7&rank=3&spos=3&epos=3&td=14&crumb-action=append&context=4&resolvein=true
31. Solove, Daniel J. “Privacy Self-Management and the Consent Dilemma.” *Harvard Law Review* 126(7) (2013): p. 1880-1903. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/hlr126&div=87&start_page=1880&collection=journals&set_as_cursor=0&men_tab=srchresults
32. Thon, Bjorn Erik and Nes, Catharina. “Controlling the Algorithms.” *European Data Protection Law Review* 3(1) (2017): 16-19. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/edpl3&div=7&start_page=16&collection=journals&set_as_cursor=0&men_tab=srchresults
33. Wachter, Sandra, Mittelstadt, Brent and Floridi, Luciano. “Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation.” *International Data Privacy Law* 7(2) (2017), p. 1-47. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

34. Warner Jr., David R. “A Neural Network-based Law Machine: the Problem of Legitimacy.” *Law, Computers & Artificial Intelligence* 2(2) (1993): p. 135-148. http://www.law.daval.com/2011/08/n-nets-2/
35. Wang, Pei. “What Do You Mean by “AI”?.” *Frontiers in Artificial Intelligence and Applications* 171(1) (2008): p. 1-12. https://cis.temple.edu/~pwang/Publication/AI_Definitions.pdf
36. Zarsky, Tal Z. “Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society.” *Maine Law Review* 56(1) (2004): p. 13-60. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/maine56&div=7&start_page=13&collection=journals&set_as_cursor=0&men_tab=srchresults
37. Zarsky, Tal Z. “Incompatible: The GDPR in the Age of Big Data.” *Seton Hall Law Review 47* (4) (2017): p. 995-1020. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/shlr47&div=37&start_page=995&collection=journals&set_as_cursor=0&men_tab=srchresults
38. Zarsky, Tal Z. “The Privacy-Innovation Conundrum.” *Lewis and Clark Law Review* 19(1) (2015): p. 115-168. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/lewclr19&div=7&start_page=115&collection=journals&set_as_cursor=0&men_tab=srchresults
39. Zarsky, Tal Z. “Transparency in Data Mining: From Theory to Practice.” In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Toon Calders et al., p. 301-325. Berlin, Germany: Springer, 2013. https://books.google.co.id/books?id=Ricr1ZHnlWcC&pg=PA303&lpg=PA303&dq=Transparency+in+Data+Mining:+From+Theory+to+Practice&source=bl&ots=xgmXtUrxuM&sig=Z5MOEgUKKHbN6g6r31WlNGEnEQA&hl=id&sa=X&ved=0ahUKEwiQurCavoTbAhVJKFAKHTNtBPsQ6AEIRTAE#v=onepage&q=Transparency%20in%20Data%20Mining%3A%20From%20Theory%20to%20Practice&f=false Accessed: April 30, 2018
40. Zarsky, Tal Z. “Transparent Predictions.” *University of Illinois Law Review* 2013(4) (2013): 1503-1570. http://heinonline.org.skaitykla.mruni.eu/HOL/Page?handle=hein.journals/unilllr2013&div=44&start_page=1503&collection=journals&set_as_cursor=0&men_tab=srchresults

Books:

1. Baldwin, Robert, Cave, Martin and Lodge, Martin. *Understanding Regulation– Theory, Strategy, and Practice*. New York, USA: Oxford University Press, 2012. https://books.google.co.id/books?id=x_lcrqoqb9oC&printsec=frontcover&dq=Understanding+Regulation:+Theory,+Strategy,+and+Practice&hl=lt&sa=X&ved=0ahUKEwiNgInEqcjaAhUB6GMKHWvCDyAQ6AEIKDAA#v=onepage&q=Understanding%20Regulation%3A%20Theory%2C%20Strategy%2C%20and%20Practice&f=false Accessed: May 1, 2018.
2. Kurzweil, Ray. *The Singularity Is Near: When Humans Transcend Biology*. New York: Viking, 2005. http://www.grtl.org/Singularity-Is-Near.pdf
3. Kulkarni, Parag. *Reinforcement and Systemic Machine Learning for Decision Making*. New Jersey, USA: John Wiley and Sons, Inc., 2012. https://zodml.org/sites/default/files/Reinforcement_and_Systemic_Machine_Learning_for_Decision_Making.pdf
4. Mayer-Schönberger, Viktor and Cukier, Kenneth. *Big Data - A Revolution That Will Transform How We Live, Work, and Think.* New York, USA: Houghton Mifflin Harcourt Publishing Company, 2013. https://books.google.lt/books?id=HpHcGAkFEjkC&printsec=frontcover&hl=lt&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
5. Nilsson, Nils J. *The Quest for Artificial Intelligence: A History of Ideas and Achievements.* Cambridge, UK: Cambridge University Press, 2010. https://ai.stanford.edu/~nilsson/QAI/qai.pdf
6. Russell, Stuart J., and Norvig, Peter. *Artificial Intelligence: A Modern Approach*. New Jersey: Prestine Hall 2010. https://www.pdfdrive.net/artificial-intelligence-a-modern-approach-3rd-edition-d32618455.html
7. Sterne, Jim. *Artificial Intelligence for Marketing: Practical Applications.* New Jersey, USA: John Wiley and Sons, Inc., 2017. https://books.google.co.id/books?id=cEozDwAAQBAJ&pg=PA234&lpg=PA234&dq=target+pregnant+artificial+intelligence&source=bl&ots=9e0Y_IGaMK&sig=kwm9KkItjTntItiHRgIQU0UiDUU&hl=id&sa=X&ved=0ahUKEwj9ieu-v83aAhXMPY8KHZ01DqMQ6AEIYzAH#v=onepage&q=target%20pregnant%20artificial%20intelligence&f=false Accessed: April 28, 2018.

8. Yudkowsky, Eliezer. *Artificial Intelligence as a Positive and Negative Factor in Global Risk*. New York, USA: Oxford University Press 2008. https://intelligence.org/files/AIPosNegFactor.pdf
9. Wright, David and Kreissl, Reinhard. *Surveillance in Europe.* New York, USA: Routledge, 2015. https://books.google.co.id/books?id=9amQBAAAQBAJ&pg=PA75&lpg=PA75&dq=Data+mining+is+%E2%80%98a+procedure+by+which+large+databases+are+mined+by+means+of+algorithms+for+patterns+of+correlations+between+data%E2%80%99&source=bl&ots=lCVufyexqx&sig=__dQGm7oh0yDbJNWhpkS3PFJkrw&hl=id&sa=X&ved=0ahUKEwipx_utu6zaAhVLuo8KHQtrD8EQ6AEIMjAB#v=onepage&q=Data%20mining%20is%20%E2%80%98a%20procedure%20by%20which%20large%20databases%20are%20mined%20by%20means%20of%20algorithms%20for%20patterns%20of%20correlations%20between%20data%E2%80%99&f=false Accessed: April 30, 2018.

Reports, studies and proposals:

1. "Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." COM(92) 422 final-SYN 297. October 15, 1992. http://aei.pitt.edu/10375/1/10375.pdf
2. "Standardisation in the area of innovation and technological development, notably in the field of text and data mining." European Commission. Report from the Expert Group, 2014. http://ec.europa.eu/research/innovation-union/pdf/TDM-report_from_the_expert_group-042014.pdf
3. Brooks, Rodney et al. "Artificial Intelligence and Life in 2030", One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel. Stanford University, Stanford, CA, September 2016. http://ai100.stanford.edu/2016-report
4. Nevejans, Nathalie. "European Civil Law Rules in Robotics. Study", Directorate-General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs. European Union. 2016. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU%282016%29571379_EN.pdf

5. “Regulatory Performance: Ex Post Evaluation of Regulatory Tools and Institutions.” OECD. Working Party on Regulatory Management and Reform. 60V/PGC/Reg. Paris. 2004.
https://www.oecd.org/gov/regulatory-policy/30401951.pdf
6. Kamarinou, Dimitra, Millard, Christopher and Singh, Jatinder. “Machine Learning with Personal Data.” Queen Mary School of Law Legal Studies Research Paper No. 247/2016, 2016.
https://ssrn.com/abstract=2865811
7. Korff, Douwe. “New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments.” European Commission DG Justice, Freedom and Security Report. 2010.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638949
8. Rieke, Aaron, Robinson, David and Yu, Harlan. “Civil Rights, Big Data and our Algorithmic Future, A September 2014 report on social justice and technology by Robinson + Yu.” Robinson + Yu. 2014.
http://centerformediajustice.org/wp-content/uploads/2014/10/Civil-Rights_Big-Data_Our-Future.pdf
9. Rouvroy, Antoinette. “”Of Data and Men””. Fundamental Rights and Freedoms in a World of Big Data.” Council of Europe, Directorate General of Human Rights and Rule of Law. T-PD-BUR(2015)09REV, 2016.
http://works.bepress.com/antoinette_rouvroy/64/.
10. “Big data, artificial intelligence, machine learning and data protection.” UK Information Commissioner’s Office. 2017.
https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
11. “A comprehensive EU response to the financial crisis: substantial progress towards a strong financial framework for Europe and a banking union for the Eurozone.” European Commission. March 28, 2014.
http://europa.eu/rapid/press-release_MEMO-14-244_en.htm
12. “Draft Explanatory Report on the modernized version of CoE Convention 108.” Council of Europe. 2016.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2
13. “The Future of Financial Services.” World Economic Forum. Final Report. June 2015.

http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

14. "Data Protection Laws of the World". DLA Piper report on Indonesia. 2017. https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf
15. "Preparing For The Future Of Artificial Intelligence." National Science and Technology Council. Executive Office of the President. 2016. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf
16. "The Future is here: Artificial Intelligence and Robotics." Nishith Desai Associates. 2017. http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Artificial_Intelligence_and_Robotics.pdf
17. "The National Artificial Intelligence Research and Development Strategic Plan." National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee. 2016. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf

Newspaper Articles:

1. Auchard, Eric and Ingram, David. "Cambridge Analytica CEO claims influence on U.S. election, Facebook questioned." *The Reuters,* March 20, 2018. https://www.reuters.com/article/us-facebook-cambridge-analytica/cambridge-analytica-ceo-claims-influence-on-u-s-election-facebook-questioned-idUSKBN1GW1SG
2. Beattie, Alan. "Why the whole world feels the 'Brussels effect.'" *The Financial Times*, November 16, 2017. https://www.ft.com/content/7059dbf8-a82a-11e7-ab66-21cc87a2edde
3. Bernard, Tara Siegel et al., "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." The New York Times, September 7, 2017. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html
4. Berreby, David. "Click to agree with what? No one reads terms of service, studies confirm." *The Guardian,* March 3, 2017. https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print
5. Bodkin, Henry. "AI robots sexist, racist, experts warn." *The Telegraph,* August 24, 2017.

https://www.telegraph.co.uk/news/2017/08/24/ai-robots-sexist-racist-experts-warn/

6. Borowiec, Steven. “AlphaGo beats Lee Sedol in third consecutive Go game.” *The Guardian*, March 12, 2016. https://www.theguardian.com/technology/2016/mar/12/alphago-beats-lee-sedol-in-third-consecutive-go-game.
7. Bradley, Tony. “Facebook AI Creates Its Own Language In Creepy Preview Of Our Potential Future.” *The Forbes*, July 31, 2017. https://www.forbes.com/sites/tonybradley/2017/07/31/facebook-ai-creates-its-own-language-in-creepy-preview-of-our-potential-future/#b892b97292c0
8. Ciolli, Joe. “2 Berkeley grads are using AI to make stock-buying decisions — and it could change investing forever”. *The Business Insider*, November 28, 2017. http://www.businessinsider.com/ai-powered-etf-aieq-stock-market-machine-learning-investments-2017-11
9. Chaykowski, Kathleen. “Facebook News Feed Change Prioritizes Posts From Friends Users Care About.” *The Forbes*, June 29, 2016. https://www.forbes.com/sites/kathleenchaykowski/2016/06/29/facebook-tweaks-news-feed-algorithm-to-prioritize-posts-from-friends-you-care-about/#585f2378da2e
10. Clark, Liat. “Google’s Artificial Brain Learns to Find Cat Videos.” The *Wired*, June 26, 2012. https://www.wired.com/2012/06/google-x-neural-network/
11. Cooper, Helene. “Obama signs overhaul of Financial System.“ *The New York Times*, July 21, 2010. https://www.nytimes.com/2010/07/22/business/22regulate.html
12. Crawford, Kate. “Artificial Intelligence's White Guy Problem.” *The New York Times*, June 25, 2016. https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html
13. Davies, Alex. “Waymo has Taken the Human out its Self-Driving Cars.” *The Wired*, July 11, 2017. https://www.wired.com/story/waymo-google-arizona-phoenix-driverless-self-driving-cars/
14. Fonzone, Christopher and Heinzelman, Kate. “Should the government regulate artificial intelligence? It already is.” *The Hill*, February 26, 2018. http://thehill.com/opinion/technology/375606-should-the-government-regulate-artificial-intelligence-it-already-is

15. Gabbatt, Adam. “IBM computer Watson wins Jeopardy clash.” *The Guardian*, February 17, 2017. https://www.theguardian.com/technology/2011/feb/17/ibm-computer-watson-wins-jeopardy
16. Garcia, Denise. “Battle Bots: How the World Should Prepare Itself for Robotic Warfare.” *Foreign Affairs*, June 5, 2015. https://www.foreignaffairs.com/articles/2015-06-05/battle-bots
17. Griffin, Andrew. “Robot Judges Could Soon be Helping with Court Cases.” *The Independent,* October 24, 2016. https://www.independent.co.uk/life-style/gadgets-and-tech/news/ai-judge-robot-european-court-of-human-rights-law-verdicts-artificial-intelligence-a7377351.html
18. Helft, Miguel. “Google Uses Searches to Track Flu’s Spread.” *The New York Times*, November 11, 2008. http://www.nytimes.com/2008/11/12/technology/internet/12flu.html
19. Hotten, Russell. “Volkswagen: The scandal explained.” *The BBC*, December 10, 2015. http://www.bbc.com/news/business-34324772
20. Jang, Erin. “What Companies Are Winning the Race for Artificial Intelligence?.” *Forbes*, February 24, 2017. https://www.forbes.com/sites/quora/2017/02/24/whatcompanies-are-winning-the-race-for-artificial-intelligence/#2af852e6fcd.
21. Jim, Paul J. “The First Ever Fund Managed by a Robot Is Here. So Far It's Beating the Market”. *The Time*, October 25, 2017. http://time.com/money/4993744/robot-mutual-fund-beating-stock-market/
22. Kaleagasi, Bartu. “A New AI Can Write Music as Well as a Human Composer.” *The Futurism,* March 9, 2017. https://futurism.com/a-new-ai-can-write-music-as-well-as-a-human-composer/
23. Kentish, Benjamin. “Richard Branson calls for universal basic income because robots are taking people's jobs.” *The Independent*, October 10, 2017. https://www.independent.co.uk/news/business/news/richard-branson-universal-basic-income-robots-taking-jobs-automation-threat-a7993006.html
24. Keohane, Joe. “What News-Writing Bots Mean for the Future of Journalism.” *The Wired*, February 16, 2017. https://www.wired.com/2017/02/robots-wrote-this-story/
25. Kleinman, Alexis. “How Netflix Gets Its Movie Suggestions So Right.” *The Huffington Post*, July 08, 2013.

http://www.huffingtonpost.com/2013/08/07/netflix-movie-suggestions_n_3720218.html

26. Lyengar, Vinod. "Why AI Consolidation Will Create the Worst Monopoly in US History." *Techcrunch*, August 25, 2016. https://techcrunch.com/2016/08/24/why-aiconsolidation-will-create-the-worst-monopoly-in-us-history
27. Lohr, Steve. "How Big Data Became So Big." *The New York Times*, August 11, 2012. http://www.nytimes.com/2012/08/12/business/how-big-data-became-so-big-unboxed.html?smid=pl-share
28. Markoff, John. "Computer Wins on "Jeopardy!": Trivial, It's Not." *The New York Times*, February 16, 2011. https://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html
29. Mozur, Paul. "Google's AlphaGo Defeats Chinese Go Master in Win for A.I." *The New York Times*, May 23, 2017. https://www.nytimes.com/2017/05/23/business/google-deepmind-alphago-go-champion-defeat.html
30. Newcomb, Alyssa. "Massive Equifax Data Breach Could Affect Half of the U.S. Population." *The NBC News*, September 8, 2017. https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686
31. Newcomer, Eric and Webb, Alex. "Uber Self-Driving Truck Packed With Budweiser Makes First Delivery in Colorado." *Bloomberg*, October 25, 2016. https://www.bloomberg.com/news/articles/2016-10-25/uber-self-driving-truck-packed-with-budweiser-makes-first-delivery-in-colorado
32. NG, Alfred. "IBM's Watson gives proper diagnosis for Japanese leukemia patient after doctors were stumped for months." *The New York Daily News*, August 07, 2016. http://www.nydailynews.com/news/world/ibm-watson-proper-diagnosis-doctors-stumped-article-1.2741857.
33. Paradis, Norman A. "The Golden State Killer case shows how swiftly we're losing genetic privacy." *Vox*, May 5, 2018. https://www.vox.com/the-big-idea/2018/5/3/17313796/genetic-privacy-killer-golden-state-serial-killer-genealogy-genome
34. Perper, Rosie. "Cambridge Analytica's parent company claimed it invented the tough guy image that got Rodrigo Duterte elected." *The Business Insider*, April 6, 2018. http://www.businessinsider.sg/cambridge-analytica-duterte-tough-guy-image-for-presidential-election-2018-4/?r=US&IR=T

35. Pimental, Albert. “Big Data: The Hidden Opportunity.” *Forbes*, May 1, 2012. http://www.forbes.com/sites/ciocentral/2012/05/01/big-data-the-hidden-opportunity/
36. Popper, Nathaniel. “The Robots Are Coming for Wall Street.” *The New York Times*, February 25, 2016. https://www.nytimes.com/2016/02/28/magazine/the-robots-are-coming-for-wall-street.html?_r=0
37. Schatsky, David, Muraskin, Craig and Gurumurthy, Ragu. “Demystifying artificial intelligence. What business leaders need to know about cognitive technologies.” Deloitte University Press. 2014. https://www2.deloitte.com/content/dam/insights/us/articles/what-is-cognitive-technology/DUP_1030-Cognitive-Technologies_MASTER.pdf.
38. Sulleyman, Aatif. “AI will be better than human workers at all tasks in 45 years, says Oxford University report.” *The Independent*, June 1, 2017. https://www.independent.co.uk/life-style/gadgets-and-tech/news/ai-jobs-stealing-outperform-human-workers-all-tasks-oxford-university-report-a7767856.html
39. Waldman, Peter, Chapman, Lizette, and Robertson, Jordan. “Palantir Knows Everything About You.” *Bloomberg*, April 19, 2018. https://www.bloomberg.com/features/2018-palantir-peter-thiel/
40. Weller, Chris. “The world's first artificially intelligent lawyer was just hired at a law firm.” *The Business Insider*, May 16, 2016. http://www.businessinsider.com/the-worlds-first-artificially-intelligent-lawyer-gets-hired-2016-5/?IR=T
41. Zoldi, Scott. “GDPR: time to explain your AI.” *The Financier Worldwide*, August, 2017. https://www.financierworldwide.com/gdpr-time-to-explain-your-ai/#.WvgGjIiFPBU
42. “Coming to an Office Near You.” *The Economist*, January 18, 2014. https://www.economist.com/news/leaders/21594298-effect-todays-technology-tomorrows-jobs-will-be-immenseand-no-country-ready
43. “Eugene the Turing test-beating 'human computer' – in 'his' own words.” *The Guardian*, June 9, 2014. https://www.theguardian.com/technology/2014/jun/09/eugene-person-human-computer-robot-chat-turing-test
44. “Google’s “superhuman” DeepMind AI claims chess crown.” *The BBC news*, December 6, 2017. http://www.bbc.com/news/technology-42251535.
45. “Equifax under pressure after data breach update.” *The BBC*, February 12, 2018.

http://www.bbc.com/news/technology-43033202

Online Courses:

1. Bentham, Jeremy. *Principles of Morals and Legislation* (1780), excerpt. Harvard University course on Justice. https://courses.edx.org/courses/course-v1:HarvardX+ER22.1x+2T2017/courseware/C_03/c6828de7461a416381457d1eced938dc/1?activate_block_id=block-v1%3AHarvardX%2BER22.1x%2B2T2017%2Btype%40vertical%2Bblock%40b0048dfca2ce4c0cbd3a5a976c771318
2. McGuire, Brian et al. "The History of Artificial Intelligence." History of Computing course at the University of Washington-Seattle, University of California-San Diego, and University of California-Berkeley. Washington. 2006. https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf
3. Sandel, Michael. „Justice: What's The Right Thing To Do? Episode 02: "PUTTING A PRICE TAG ON LIFE." Harvard University course on Justice. Uploaded in 2009. https://www.youtube.com/watch?v=0O2Rq4HJBxw

Additional Sources:

1. Altavilla, Dave. "NVIDIA CEO And Elon Musk On Autonomous Cars: Could Human Drivers Eventually Be Outlawed?." *HotHardware*, March 18, 2015. https://hothardware.com/news/nvidia-ceo-and-elon-musk-on-autonomous-cars-could-human-drivers-eventually-be-outlawed
2. Bardram, Jakob E. "Applications of Context-Aware Computing in Hospital Work – Examples and Design Principles." Proceedings of the 2004 ACM symposium on Applied computing. http://delivery.acm.org/10.1145/970000/968215/p1574-bardram.pdf?ip=152.118.150.218&id=968215&acc=ACTIVE%20SERVICE&key=580EBA767A7E72A7%2E2F107ED8A98F1C18%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1525842634_0c60a98dba3f5f3c02e768050f29011e.
3. Bradford, Anu. "The Brussels Effect: The Rise of a Regulatory Superstate in Europe." Columbia Law School. 2013. http://www.law.columbia.edu/media_inquiries/news_events/2013/january2013/brussels-effect

4. Bryk, William. “Artificial Superintelligence: The Coming Revolution.” Harvard Science Review. 2015. https://harvardsciencereview.com/2015/12/04/artificial-superintelligence-the-coming-revolution-2/.
5. Budiman, Abby and Manevich, Dorothy. “Few see EU as world’s top economic power despite its relative might.” Pew Research Center. 2017. http://www.pewresearch.org/fact-tank/2017/08/09/few-see-eu-as-worlds-top-economic-power-despite-its-relative-might/
6. Clark, Jen. “Is Watson the best medicine? The impact of big data analysis on healthcare.” *IBM,* January 3, 2017. https://www.ibm.com/blogs/internet-of-things/iot-and-healthcare/
7. Copeland, Jack. “What is Artificial Intelligence?.” Reference Articles on Turing. 2000. http://www.alanturing.net/turing_archive/pages/reference%20articles/what%20is%20ai.html.
8. Joint written evidence submitted by the Association for the Advancement of Artificial Intelligence and the UK Computing Research Committee for robotics and artificial intelligence inquiry by Science and Technology Committee of UK House of Commons http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/robotics-and-artificial-intelligence/written/32533.html
9. Corea, Francesco. “A Brief History of Artificial Intelligence.” *KD Nuggets,* April 2017. https://www.kdnuggets.com/2017/04/brief-history-artificial-intelligence.html
10. Herbich, Ralf. “Session with Ralf Herbrich Director of Machine Learning and Managing Director of Amazon Development, Germany.” Quora. 2016. https://www.quora.com/profile/Ralf-Herbrich/session/106/.
11. Malekian, Hajar. “Profiling under General Data Protection Regulation (GDPR): Stricter Regime?.” Linkedin. 2016. https://www.linkedin.com/pulse/profiling-under-general-data-protection-regulation-gdpr-malekian/
12. Marr, Bernard. “Why only one of the 5 Vs of big data really matters.” IBM Big Data and Analytic Hub. 2015. http://www.ibmbigdatahub.com/blog/why-only-one-5-vs-big-data-really-matters
13. McCarthy, John. “What is Artificial Intelligence.” Stanford University. 2007. http://www-formal.stanford.edu/jmc/whatisai/node1.html.

14. Mendoza, Izak and Bygrave, Lee A. “The Right Not to Be Subject to Automated Decisions Based on Profiling.” University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20. 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855
15. Sandvig, Christian. “Seeing the Sort: The Aesthetic and Industrial Defence of “the Algorithm”.” Journal of the New Media Caucus. 2015. http://median.newmediacaucus.org/art-infrastructures-information/seeing-the-sort-the-aesthetic-and-industrial-defense-of-the-algorithm/
16. Schatsky, David, Muraskin, Craig and Gurumurthy, Ragu. “Demystifying artificial intelligence.” Deloitte Insights. 2014. http://dupress.com/articles/what-is-cognitive-technology/
17. Thomadakis, Stavros B. „What Makes Good Regulation.“ Paper presented in IFAC Council Seminar. Mexico City. November 2007. http://www.ifac.org/system/files/downloads/30th_anniversary_Thomadakis_Pres_Nov_07.pdf
18. “10 facts on patient safety.” World Health Organization. Updated March 2018. http://www.who.int/features/factfiles/patient_safety/en/
19. “Algorithms in decision-making inquiry launched.” UK House of Commons Science and Technology Committee. February 28, 2017. http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2015/algorithms-in-decision-making-inquiry-launch-16-17/
20. “Asilomar AI Principles.” Asilomar Conference. 2017. https://futureoflife.org/ai-principles/
21. “A Six Minutes Intro to AI.” Snips. Accessed 2018 April 15. https://snips.ai/content/intro-to-ai/#what-is-ai.
22. “Data Protection Eurobarometer.” European Commission. June 2015. https://perma.cc/3XLK-VKA6
23. “Deep Learning for Healthcare”. Nvidia. Accessed 2018 April 28. https://www.nvidia.com/en-us/deep-learning-ai/industries/healthcare/
24. “GDPR Handbook: Unlocking the EU General Data Protection Regulation.” White and Case. Chapter 6: Data Protection Principles. 2017. http://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-dataprotection

25. “Natural Language Processing, what it is and why it matters.” SAS. Accessed 2018 April 20. https://www.sas.com/en_us/insights/analytics/what-is-natural-language-processing-nlp.html
26. “Patient safety. Data and statistics.” World Health Organization. http://www.euro.who.int/en/health-topics/Health-systems/patient-safety/data-and-statistics

ABSTRACT

The Master Thesis analyse artificial intelligence technology and its compatibility with the General Data Protection Regulation. This analysis is performed by evaluating relevant to artificial intelligence articles of General Data Protection Regulation in order to determine whtether they effectively regulate artificial intelligence and whether they could potentially stifle the growth of artificial intelligence industry. The evaluation of relevant articles is based on the criteria for determining what kind of regulation could be considered as a good regulation.

The evaluation of the articles shows, that many articles do not properly take into account or even address the nature artificial intelligence technology and its impact to data privacy. Therefore it is concluded, that General Data Protection Regulation is not properly equip to handle challenges posed by artificial intelligence technology and thus there is a need for new artificial intelligence specific regulation.

Keywords: General Data Protection Regulation, artificial intelligence, data privacy, good regulation.

Magistriniame darbe analizuojamas dirbtinio intelekto suderimamumas su Bendruoju duomenų apsaugos reglamentu. Ši analizė atliekama įvertinant kiekvieną aktualų dirbtinio intelekto technologijai Bendrojo duomenų apsaugos reglamento straipsnį, siekiant nustatyti ar atskiras staipsnis efektyviai reglamentuoja dirbtinį intelektą ir ar atskiras straipsnis netrukdo dirbtinio intelekto industrijos augimui. Toks vertinimas yra paremtas kriterijais, skirtais įvertinti ar bet kokio pobūdžio reglamentas yra geras reglamentas.

Įvertinimo rezultatai rodo, kad daug straipsnių netinkamai reglamentuoja ar net neįvertina dirbtinio intelekto technologijos ir jos įtakos duomenų apsaugai. Remdamasis šiais rezultatais autorius daro išvadą, kad Bendrasis duomenų apsaugos reglamentas nėra tinkamas reglamentas įveikti dirbtinio intelekto technologijos keliamus iššūkius, todėl autorius rekomenduoja sukurti naują reglamentą, skirtą reglamentuoti dirbtinį intelektinį.

Ranktažodžiai: Bendrasis duomenų apsaugos reglamentas, dirbtinis intelektas, duomenų apsauga, tinkamas reglamentas.

SUMMARY

The purpose of this Master Thesis is to evaluate compatibility between artificial intelligence technology and General Data Protection Regulation in order to determine whether General Data Protection Regulation is a proper and effective regulation in the age of intelligent machines.

The Master Thesis consists of three chapters. The first chapter attempts to define the artificial intelligence and its components, the so called artificial intelligence symphony. It is concluded, that there is no universal definition for artificial intelligence, let alone a proper working definition for legal research. Furthermore, the first chapter also analyses the historical developments of artificial intelligence technology and current legal documents, which are regulating or designed to include regulation of AI. The analysis of legal documents shows, that there are no artificial intelligence specific laws in all major countries around the world and artificial intelligence is mostly regulated by general laws.

The second chapter tries to examine how to effectively regulate data privacy in the age of artificial intelligence. This examination is done by identifying the criteria for determining what could be considered as a good regulation in general and analysing the possible challenges that regulators would possibly face when regulating artificial intelligence. The author concludes, that the nature of artificial intelligence and its industry's growth must be taken into account in order to avoid any negative effects regulation might have on this technology and its growth.

The third chapter is designed to analyse the most comprehensive data protection regulation in the world – General Data Protection Regulation – and whether it will effectively regulate the artificial intelligence technology and its industry in Europe. The author takes every relevant article of GDPR and tries to determine possible challenges or problems, that could arise when dealing with artificial intelligence technology, and tries to provide possible solutions or recommendation on how to solve them.

All in all, the Master Thesis determines that General Data Protection Regulation is not the proper data protection regulation to deal with artificial intelligence and thus there is a need for artificial intelligence specific regulation in Europe.

SANTRAUKA

Šio magistrinio darbo tikslas yra nustatyti dirbtinio intelekto technologijos suderinamumą su Bendruoju duomenų apsaugos reglamentu, siekiant nustatyti ar Bendrasis duomenų apsaugos reglamentas yra tinkamas ir efektyvus reglamentas protingų mašinų amžiuje.

Magistrinis darbas yra padalintas į tris dalis. Pirmojoje dalyje bandoma apibrėžti kas yra dirbtinis intelektas ir nustatyti jo komponentus, vadinamąją dirbtinio intelekto simfoniją. Autorius daro išvadą, kad nėra nei universalios, nei tinkamos darbinės dirbtinio intlekto sąvokos. Taip pat, pirmojoje dalyje analizuojama dirbtinio intelekto technologijos istorija ir šiuo metu egzistuojantys teisiniai dokumentai, kurie yra skirti reglamentuoti dirbtinio intelekto technologiją ar kurių reglamentavimo apimtis apima dirbtinio intelekto technologiją. Ši analizė rodo, kad didžiosios pasaulio valstybės neturi reglamentų, skirtų išimtinai reglamentuoti dirbtinį intelektą, todėl dirbtinis intelektas yra reguliuojamas per bendrojo pobūdžio įstatymus.

Antrojoje dalyje nagrinėjama, kaip efektyviai regulamentuoti duomenų apsaugą dirbtinio intelekto eroje. Šis nagrinėjamas atliekamas identifikuojant kriterijus, skirtus įvertinti ar bet kokio pobūdžio reglamentas gali būti laikomas geru reglamentu, ir analizuojant galimus iššūkius, su kuriais reguliuotojai susidurs bandydami reglamentuoti dirbtinį intelektą. Autorius daro išvadą, kad dirbtinio intelekto technologijos pobūdis ir dirbtinio intelekto industrijos augimas turi būti tinkamai įvertinti reglamentuojant dirbtinį intelektą, siekiant išvengti neigiamų pasekmių šiai technologijai ir jos vystymuisi.

Trečioji dalis yra skirta analizuoti patį išsamiausią duomenų apsaugo reglamentą pasaulyje – Bendrąjį duomenų apsaugos reglamentą - ir nustatyti ar šis reglamentas tinkamai reglamentuos dirbtinio intelekto technologiją ir industriją Europoje. Autorius įvertina kiekvieną su dirbtinio intelekto technologija susijusi Bendrojo duomenų apsaugos reglamento straipsnį ir stengiasi nustatyti galimus iššūkius ar problemas, kurios galėtų kilti reglamentuojant šią technologiją, bei autorius pateikia galimus sprendimus ar rekomendacijas, kaip įveikti minėtas problemas ir iššūkius.

Apibendrinant, daroma išvada, kad Bendrasis duomenų apsaugos reglamentas nėra tinkamas duomenų apsaugos reglamentas reglamentuoti dirbtinio intelekto technologiją ir todėl yra reikalinga sukurti naują reglamentą, skirtą išskirtinai reglamentuoti dirbtinio intelekto technologiją Europoje.

Annex No. 4
Form approved on 20 November 2012 by the decision No. 1SN-10
of the Senate of Mykolas Romeris University

HONESTY DECLARATION
16/05/2018
Vilnius

I, ARNAS AIDUKAS, student of
(name, surname)

Mykolas Romeris University (hereinafter referred to University),
LAW FACULTY, INSTITUTE OF INTERNATIONAL AND EUROPEAN UNION LAW
(Faculty /Institute, Programme title) INTERNATIONAL LAW PROGRAMME

confirm that the Bachelor / Master thesis titled

" DATA PRIVACY AND ARTIFICIAL INTELLIGENCE: IS THE GENERAL DATA PROTECTION REGULATION THE RIGHT REGULATION IN THE AGE OF INTELLIGENT MACHINES

1. Is carried out independently and honestly;
2. Was not presented and defended in another educational institution in Lithuania or abroad;
3. Was written in respect of the academic integrity and after becoming acquainted with methodological guidelines for thesis preparation.

I am informed of the fact that student can be expelled from the University for the breach of the fair competition principle, plagiarism, corresponding to the breach of the academic ethics.

(signature)

ARNAS AIDUKAS
(name, surname)