ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2025, Vol. 37, Nr. 1

# THREATS TO THE PERSONAL RIGHT TO PRIVACY CAUSED BY THE USE OF ARTIFICIAL INTELLIGENCE

**Eglė ŠTAREIKĖ**
*Mykolas Romeris University*
*Maironio str. 27, LT 44211 Kaunas, Lithuania*
*E-mail: egle.stareike@mruni.eu*
*ORCID ID: 0000-0001-7992-991X*

**Paulius GRYBAS**
*Mykolas Romeris University*
*Maironio str. 27, LT 44211 Kaunas, Lithuania*
*E-mail: pauliusgrybass@gmail.com*
*ORCID ID: 0009-0001-6096-5002*

DOI: 10.13165/PSPO-25-37-01-11

***Abstract.*** *This scientific article analyzes how the application of artificial intelligence (AI) technologies affects the protection of the right to privacy in modern society. Given that the capabilities of AI systems are rapidly expanding and becoming increasingly integrated into everyday life, the risks to personal data security and privacy violations are also growing. This scientific article aim is to analyze the threats posed by artificial intelligence technologies in practice to the persons's right to privacy and to evaluate the legal regulation of these threats based on the analyzed cases.*

*The teoretical part of the article examines the concept, development, classification, and key characteristics of artificial intelligence, as well as the evolution of the right to privacy - from its philosophical origins to its current legal regulation. In the empirical part, a case study method was applied, analyzing the examples of the companies Clearview AI and Cambridge Analytica. The investigation of these cases highlighted the threats posed by AI to the right to privacy in practice and allowed for the evaluation of the violations committed and the responses of regulatory institutions.*

*The conducted research confirms that the threat to privacy protection arises not from the AI technology itself but from the way it is applied. It was found that the new Artificial Intelligence Act of the European Union is a significant step in ensuring the protection of personal data. Furthermore, the GDPR also strengthens the right to privacy. However, to achieve effective protection, it is essential to enhance both consumer awareness and the accountability of technology developers.*

***Keywords:*** *artificial intelligence (AI); GDPR; the right to privacy; legal regulation.*

## Introduction

The main changes in the information technology era, in the context of artificial intelligence, began to take shape and unfold around 2010-2012. One of the most prominent examples of this is „AlexNet“, a deep learning model. In the 2012 annual „ImageNet“ competition, „AlexNet“ showed incredible image recognition results (*Pinecone, 2024*), improving its error rate from around 26% to 15.3%. Although this breakthrough in artificial intelligence opened up new possibilities for applying deep learning in various fields, at that time artificial intelligence was not yet widely available for everyday use by every modern person.

However, over the last ten years, with the rapid development of information and artificial intelligence technologies, models such as *GPT-3, BERT, Transformer* have been created, which gave new momentum to artificial intelligence. In recent years, artificial intelligence has begun to have a strong impact on the everyday life of today's society. Today it is used in a wide variety of areas, such as mobile phones with voice-controlled assistants, facial recognition functions, smart home devices, city monitoring systems, healthcare systems, social networks, or finance.

It is often not considered that every day we encounter artificial intelligence solutions that can affect our privacy, which shows the **relevance** of this topic. The **novelty** of the topic can be justified by the previously mentioned facts that artificial intelligence technology has only begun to develop rapidly in recent years, and the possibilities for its use are constantly expanding. Such rapid expansion also creates new threats to a personal right to privacy that previous generations have not yet encountered.

The **issue** of this scientific article is related to the rapidly developing technologies of artificial intelligence, where more and more cases are emerging where these systems violate a person's right to privacy. Despite the growing public and legislative attention to artificial intelligence technology, the question arises - is the existing legal regulation sufficient to protect a person's right to privacy when artificial intelligence technologies are used?

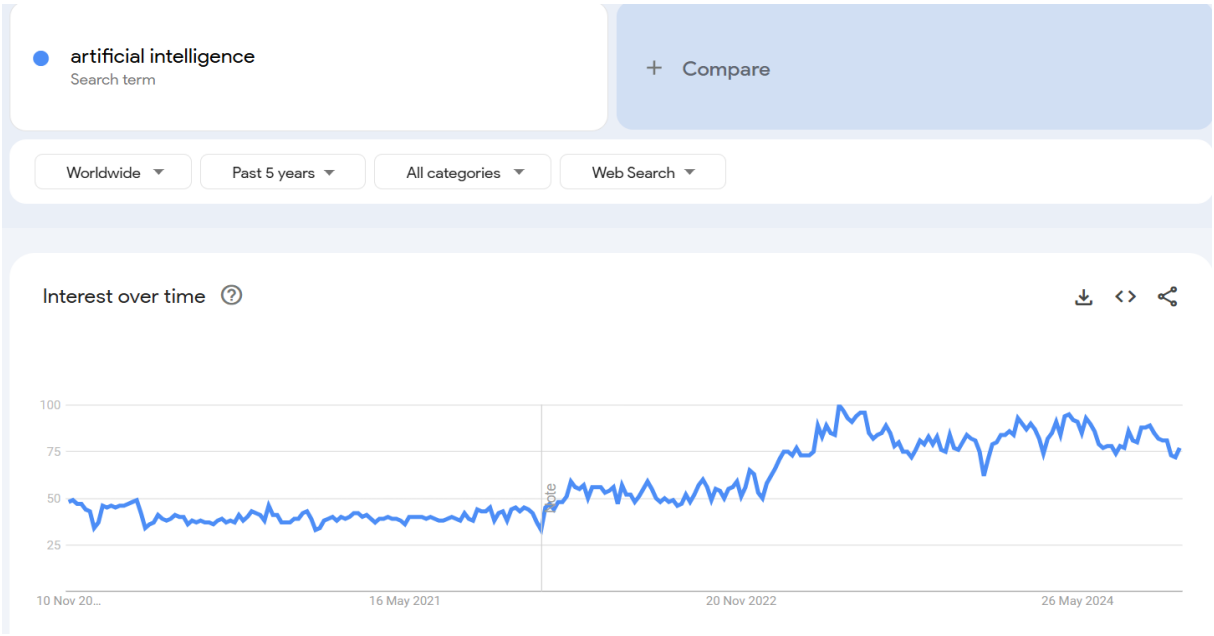
The **aim** of the scientific article is to analyze the threats posed by artificial intelligence technologies in practice to the persons's right to privacy and to evaluate the legal regulation of these threats based on the analyzed cases.

The scientific article uses **theoretical research methods** - comparative, which compares the existing legal regulation with the new EU Artificial Intelligence Act. Historical, in order to reveal the course of development of artificial intelligence technologies, to understand how historical developments have affected today's privacy protection issues. The study also used a **qualitative research method** - a case study, based on a study of two specific cases of „Clearview AI“ and „Cambridge Analytica“, in order to understand how the application of artificial intelligence can affect a person's right to privacy, as well as how threats to a person's right to privacy manifest themselves in practice, and in what ways law enforcement entities respond to this.

## Development and main features of artificial intelligence

The fact that the phenomenon of artificial intelligence is inseparable from society today can be substantiated by data from the „Google Trends“ platform. This „Google“ platform allows you to analyze the trends of searches people perform on the „Google“ search engine over a certain period of time. Analyzing the data for the last 5 years, starting in 2019, it can be seen that interest, globally, in searching for information by entering the phrase „artificial intelligence“ into the „Google“ search engine has not been below an index of 25. And since 2022, there has been a strong rise, and since then the index has not fallen below 50, and in recent years it has been between 75 and 100 (*Google trends, 2024*).

ISSN 2029-1701
ISSN 2335-2035 (Online)
Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2025, Vol. 37, Nr. 1




**Picture 1. Statistics for search „artificial intelligence“.**
*Source: "Google trends" data, 2024.*

Such data show that interest in artificial intelligence in today's society is particularly high, and at the same time emphasizes the relevance of this topic and the need to research it and pay attention to public education.

The first steps towards the practical development of artificial intelligence began in the middle of the 20th century. In 1950, Alan Turing published his famous article „Computing Machinery and Intelligence“. This article became a cornerstone, marking the beginning of the science of artificial intelligence. It proposed the famous Turing test as a way to determine whether a machine can be considered intelligent. This test is conducted with the participation of two people and a computer. The principle of the test is based on a game - one person communicates with both another person and a computer via text messages, and the test is passed if the person does not distinguish who they are communicating with at the time, whether another person or a computer (*Turing, 2024*). Alan Turing believed that in 50 years, a computer would be able to play such a game so well that it would achieve a 70 percent winning rate. Today, 74 years later, it can be said that A. Turing was right.

The even more rapid practical development of the science of artificial intelligence gained momentum a few years after his work - with the historic Dartmouth Conference in 1956, which became the first systematic attempt in the scientific world to officially define and establish the science of artificial intelligence as an independent field of research. During the conference, a definition was proposed: Artificial intelligence is the science and engineering of creating intelligent machines (*McCarthy, 2007*). This definition reveals two main directions in the field of AI. The scientific side is research and the development of theories about how machines could imitate intelligence, and the engineering side is the practical creation of systems with intelligence. Although the definition seems quite simple, it has become the basis for many subsequent definitions. The beginnings of computer science and the rapidly growing interest in intelligent machines influenced the conditions for this conference to take place. One of the goals of the conference was to conduct research on artificial intelligence and explore the possibilities of creating systems that could simulate human intelligence using mathematical, logical and engineering methodologies (*McCarthy, 2007*). The aim was also to establish AI science as a

separate discipline, separating it from other scientific fields, and to explore how machines could learn, improve, and solve various problems in a logical manner.

The 1950s–1970s are often referred to as an era of optimism, marked by important AI achievements, such as the creation of „LISP“ in 1958, the first programming language specifically designed for AI, and „ELIZA“ in 1966, the first conversational program capable of simulating human communication. This era of artificial intelligence was characterized by a very strong belief in a breakthrough, but due to high expectations, a decrease in funding, and the failure to implement overly ambitious goals, progress stalled and from 1970 to 1980 there was a so-called „winter“ period in the context of artificial intelligence.

However, with the development of expert systems in the 1980s, artificial intelligence research has gained new momentum. This recovery, combined with technological advances and increasing computer power, opened the door to new concepts that reached their first breakthrough in the 1990s – the beginnings of machine learning (*Tableau, 2025*). After the success of machine learning in the 1990s, artificial intelligence research intensified over time, including in the field of deep learning. Deep learning, using artificial neural networks, has become a key tool for solving complex problems such as speech recognition, image analysis, and text generation. It is a machine learning method that allows computers to learn from large data sets automatically, without direct human intervention. This method uses multi-layer neural networks that analyze data step by step, starting with simpler features such as lines and colors and moving on to more complex structures such as dog shapes or recognizable features (*Lecun, Bengio, Hinton*). Deep learning algorithms, applied to various complex tasks, are creating ever newer and stronger opportunities to use AI in areas such as medical diagnostics, transportation, education, and to facilitate countless other daily human activities in various fields. However, it should be noted that the current rapid development of AI also poses new challenges, ranging from ethical dilemmas to threats to personal privacy.

In his book „The Quest for Artificial Intelligence a history of ideas and achievements“, Nils John Nilsson provided a definition – artificial intelligence is the activity aimed at creating machines that would be intelligent. And intelligence is the quality that allows a subject to act appropriately and anticipate future events in their environment (*Nilsson, 2022*). Simply put, this scientist's definition means the creation of systems that could replace humans in tasks that typically require human intelligence.

Stuart Russell and Peter Norvig emphasize that the essence of AI is the ability to interact with the environment and make decisions focused on achieving specific goals. According to these authors, AI systems should not only learn or imitate human intelligence, but also effectively adapt to changing circumstances (*Russel, Norvig, 2022.)* Such a definition is important in several respects. This definition primarily focuses on the practical aspects of AI applications, that is, decision-making and goal achievement. This definition also emphasizes the system's ability to function effectively on its own in various situations. Definition by S. Russell and P. Norvig remains relevant for modern AI applications. In areas such as autonomous vehicle systems, predictive models, or virtual assistants like „Alexa“ and „Siri“.

In addition to the academic perspective, artificial intelligence is also being intensively studied by technology developers and implementers. The technological approach reveals how AI is perceived in practice - both in the development and implementation of solutions in various fields. This approach allows us to look at AI as a tool that not only solves complex problems, but also transforms everyday life, business, and industry. From the point of view of technology developers and industry representatives, artificial intelligence is an essential tool that allows you to automate processes, increase efficiency, and create innovative solutions in various fields. For example, „Google“ uses AI to improve its search algorithms to provide more accurate and

relevant results to users (*Google AI principles*). „Amazon“ uses AI to generate personalized product recommendations by analyzing consumer behavior and purchase history (*Levine, 2024*). Meanwhile, „Tesla“ is implementing AI technologies for autonomous vehicle control, aiming to create fully autonomous cars. AI is being integrated into various industries such as manufacturing, logistics, finance, and medicine. For example, in medicine, AI is used to analyze diagnostic images, helping to detect signs of disease and suggest appropriate treatments (*Mims, 2024)* Such applications not only increase the efficiency of processes, but also reduce the likelihood of errors, thereby improving the quality and reliability of services.

**Classification of artificial intelligence and its threats to the person's right to privacy**

The classification of artificial intelligence allows not only to distinguish its different properties and operating principles, but also to better understand the limits and possibilities of its application. The main classification directions of artificial intelligence can be divided into three types. By level of intelligence, by principle of operation and by scope of application.

According to the level of intelligence, the following types are distinguished:

1. Narrow AI – this type of artificial intelligence is used to perform one specific task. Narrow AI does not have the ability to think; such a machine performs predetermined functions. This is how various phone apps, recognition tools, spam filters, etc. work. For example, „Siri“ or „Google Translate “.

2. General AI – also called general artificial intelligence, today remains only a theoretical concept. General AI should be able to perform any task that a human can perform, using its intelligence, creative thinking, social understanding, and ability to learn and adapt to unseen situations without prior programming (*Joshi, 2002*)

According to the principle of operation (*Santos, Radanliev, 2024*):

1. Reactive machines – such machines operate only based on the data available. They don’t have the ability to remember their past events when making new decisions. One of the most famous examples of such a machine is the chess computer IBM Deep Blue“, which defeated Garry Kasparov in 1990 (*IBM*).

2. Limited memory – this type is able to perform complex classification tasks, recall data, and make predictions. Self-driving cars operate on this principle, but when faced with an unusual task, the machine will not cope, for example, when it sees a new road sign that is not in memory. This is the current state of artificial intelligence.

3. Theories of mind and self-concept – the current goal is to create systems that can understand the thoughts, emotions, and intentions of other people or objects. When such technology is in operation, it would be able to make decisions based on a person's beliefs and emotions. Self-concept theory is a theoretical type of AI, the highest level of development, where a machine could recognize itself and analyze its own actions.

By application area (*The Applications of AI, 2023*):

1. Natural Language Processing (NLP) – is able to understand, analyze, and generate natural human language, such as the ChatGPT language model.

2. Computer vision – performs image analysis and recognition, such as facial recognition systems.

3. Expert systems – programs solve specific problems using a base of rules and existing knowledge, for example, medical diagnostic systems.

4. Robotics is the use of artificial intelligence to control and automate mechanical systems, such as industrial robots and autonomous drones.

The concept of AI, its development, and classifications reveal the complex and ambiguous nature of this technology. Its origins date back to mythological stories and philosophical reflections, and over the decades this technology has become the most relevant field of science and technology. In the context of historical development, from A. Turing to the Dartmouth Conference, AI has emerged as a breakthrough innovation that has a profound impact on various areas of life. Analyzing different definitions reveals the dynamism of the perception of artificial intelligence and its dependence on the perspective - academic, technological, or practical. Scientists such as John McCarthy, Nils John Nilsson, along with Stuart Russell and Peter Norvig, have emphasized the importance of both intelligent imitation and decision-making, and technology developers and industry representatives see artificial intelligence as a tool that is becoming inherent for achieving efficiency and innovative achievements.

The AI classification further expands this concept, revealing levels of intelligence, operating principles, and areas of application. The differences between narrow and general AI help us understand what goals modern AI is capable of achieving today and what tasks can be overcome in the near future. Application areas show how AI is becoming established in everyday activities. A comprehensive explanation of the concept of AI is one of the essential steps in understanding the impact this phenomenon has on modern society. It should be noted that the areas of AI application are important in the context of threats to privacy, therefore the aim is to further reveal the real threats to privacy that may be caused by areas such as facial recognition systems, speech models, or other areas that pose risks. However, before that, it is important to understand the concept of a person's right to privacy.

The right to privacy has traditionally been understood as an individual's right to inviolable personal space, autonomy, and protection from external interference. This principle has evolved from the preservation of physical space to the right to control information about oneself. Modern society, constantly influenced by technological progress, has expanded the understanding of this right, especially in the context of the digital space. AI fundamentally changes the perception of privacy because it is able to collect, analyze, and systematize enormous amounts of data. Digital assistants, bio-metric data recognition systems, and behavioral prediction algorithms are transforming privacy from protecting physical space to ensuring digital autonomy. This requires new legal, ethical and technological measures that can protect the individual in this dynamic technological age. Person's right to privacy today includes not only protection from physical intrusion, but also the ability to control how their data is used in the digital space. The influence of artificial intelligence in this context is particularly important, as this technology can not only automate processes, but also discern patterns of behavior of individuals, predict their actions, or even make decisions based on the collected data.

All of this raises questions about the transparency of data collection and use and the human right to control information. Given these challenges, it is important to understand how the right to privacy is adapting in the era of artificial intelligence, with particular attention to how digital privacy is changing traditional understandings. It is worth noting that when delving deeper into the concept of the right to privacy in the context of AI, a very important "keyword" is discovered - data. In the context of artificial intelligence, personal data is an essential part of the technology's functioning - without it, AI would not be able to learn, analyze, or make decisions. The importance of data in the modern world is undoubtedly one of the fundamental reasons why the right to privacy has transformed and expanded. Digital technologies have enabled a huge flow of data, which includes not only basic information, but also detailed personal profiles, behavioral patterns, bio-metric indicators, geolocation data and much more.

Today, data become an integral part of the right to privacy, as its collection, storage and use are directly related to a person's autonomy and their ability to control information about themselves. Personal data protection expands the concept of the right to privacy, because today ensuring personal privacy includes not only the inviolability of physical space, but also digital data. This raises important questions not only about the right to privacy, but also about how this data is protected from misuse.

A person's right to privacy is a human right with deep roots in a historical and philosophical context, which changes in response to the development of society and technology. From the inviolability of private physical space to digital data management, the concept of privacy has expanded and become comprehensive in the modern world. Artificial intelligence's ability to collect and analyze personal data poses new challenges, so today, digital human privacy is becoming no less important than physical privacy.

**Legal regulation of the right to privacy in the context of artificial intelligence**

The European Union Artificial Intelligence Act (hereinafter referred to as the AIA) officially entered into force on 1 August 2025. Originally proposed by the European Commission in April 2021 and formally adopted by the European Parliament and the Council in December 2023, the AIA represents the world's first comprehensive legislative framework aimed at regulating artificial intelligence technologies. The AIA addresses the potential risks AI systems pose to health, safety, and fundamental rights. It is designed to ensure the safe deployment of AI technologies while safeguarding core European values such as human dignity, privacy, and non-discrimination. The regulation establishes a risk-based approach, where obligations are proportionate to the level of risk that different AI systems may present. (European Commision, 2024; TeisėPro, 2024).

From February 2, 2025, marks an important milestone in the regulation of artificial intelligence in the European Union – the first provisions of the Artificial Intelligence Act have come into force. This means that from this day, certain artificial intelligence systems are completely prohibited, and new obligations arise for developers, providers, and users of AI tools (*TeisėPro, 2025*).

The Artificial Intelligence Act marks one of the first not only theoretical, but also practical attempts to regulate artificial intelligence, outlining clear rules and creating a precedent that may influence other states considering their own AI regulation. The AIA will be fully applicable from August 2, 2026, and with exceptions for certain rules until August 2, 2027. Thus, the article continues by examining the specific threats to the user's privacy rights when using artificial intelligence. The AIA analysis allows us to understand which areas of privacy are protected in the context of AI and where risks arise.

The main goal of the Artificial Intelligence Act is to create a legal framework that would ensure the development of AI technologies that would not violate fundamental human rights and serve the welfare of society. This act not only obliges developers and users of AI systems to comply with certain norms, but also sets clear boundaries in which cases they cannot be crossed. To make those boundaries clear, the AI system is grouped into different levels of risk in the act.

The most stringently assessed systems, the use of which is prohibited, are assigned to the unacceptable risk group. Such systems pose a threat to human rights, freedoms and democratic processes. The AI Act prohibits eight types of practices:

1) harmful artificial intelligence-based manipulation and deception. A real example is „Deepfake“ technology. „Deepfake“ is a combination of the terms „deep learning“ and „fake“.

Deepfake is extremely realistic videos that are digitally manipulated to make the individuals in them appear to be saying or doing things that never happened in reality. The basis of this technology is the use of artificial neural networks, analyzing large data sets, to learn to imitate a person's facial expressions, mannerisms, voice, and intonations. The process involves feeding videos of two people to a deep learning algorithm, which learns to replace one person's face with another (*Westerlund, 2019*). Videos created using this technology can often be seen on various social networks, where speeches by various politicians and public figures are faked.

2) malicious artificial intelligence-based vulnerability exploitation. Such practices can be used by criminals who, perhaps without sufficient literacy, use language models, such as „CHAT GPT“, to create convincing, professional letters, impersonating employees of a bank or other institution and trying to extort certain data or money from a person.

3) social scoring. A real-world example is China's social ranking system, in which citizens are actually divided into "good" and "bad" (*Hou, Fu, 2022*) and gain or lose points depending on their behavior. Higher scores provide opportunities, such as the ability to obtain loans or expedited visas, while lower scores may limit your ability to travel or receive government services.

4) risk assessment or prediction of individual criminal acts. In the United States, the COMPAS - Correctional offender management profiling for alternative sanctions system was used, which assesses the likelihood of prisoners to re-offend. Practice has shown that this system was biased against African Americans, as they were more often seen as posing a higher risk of crime compared to whites (*Strikaitė-Latušinskaja, 2022*).

5) non-targeted collection of internet or security video surveillance material for the purpose of creating or expanding facial recognition databases. We already have real examples in history where such systems were used. Clearview AI collected large amounts of facial photos from various social networks and websites, creating the world's largest facial recognition database, but even before the Artificial Intelligence Act existed, the creation of such a system already violated certain laws, such as the norms set by the GDPR. The main reason for this was that most people were unaware that their faces were being pulled into the system (*European Data Protection Board, 2022*).

6) emotion recognition in workplaces and educational institutions. Thanks to technology and artificial intelligence, devices exist that, for example, measure a student's brain activity and emotional state during lessons, but this raises concerns about personal privacy and psychological stress, so including such systems in the list of prohibited practices seems reasonable and necessary.

7) bio-metric categorization to identify certain protected characteristics. Such systems are designed to group people according to their biological or physical characteristics, in order to determine certain characteristics, race, gender, age, and health status.

8) real-time remote bio-metric identification for law enforcement purposes in public spaces. Such systems can recognize a person in real time by scanning their face, which can help detect wanted individuals, but at the same time, individuals are massively monitored and their identities are determined, even though they are not involved in criminal acts, which violates their privacy.

In addition to unacceptable risk systems, a list of high-risk systems is also distinguished, which will not be banned, but will be strictly regulated. Such systems are related to health, safety, and fundamental human rights. High-risk use cases include:

1) AI security systems responsible for critical infrastructure facilities. For example, the use of AI systems in transport safety systems, the failure of which would be dangerous to human health or life.

2) AI systems in education, for example, an automatic exam grading system, such a system can affect a person's future career and their planned future.

3) AI in medicine, the use of such systems certainly poses a high risk, as their inaccuracy, for example in surgery, can have serious consequences.

4) AI recruitment and job performance systems. One example is the „HireVue“ system, which helps employers save time and analyzes candidates seeking employment based on their facial expressions, speech patterns, and voice, thus filtering out suitable and unsuitable employees for the employer (*Harwell, 2019*).

5) Use of AI in everyday services, for example, AI can biasedly assess a person's creditworthiness, which may determine whether they will be granted a housing loan, the solution of such a system can have a significant impact on a person's life.

6) Use of AI for remote human recognition, identity verification, bio-metric classification, and emotion recognition.

7) Use of systems in law enforcement, for example to analyze evidence in courts.

8) Use in the areas of migration and border control, such as automated systems that analyze migrant data and visa applications.

9) AI solutions in court proceedings, systems that assist judges in drafting decisions, are also considered high-risk systems.

When analyzing these two risk groups, it is clear that unacceptable AI systems are prohibited because they pose a direct threat to human rights, democracy, and public safety. However, high-risk systems are permitted to be used with strict controls. This difference shows that the European Union's AI Act not only aims to prevent threatening systems, but also seeks to create clear regulation that would also allow for innovation while protecting human rights. In addition to these two strongly controlled types of risk, transparent risk systems are also distinguished, such as chat-bots. The main requirement for such systems is to notify the user that they are communicating and interacting with a machine, an artificial intelligence system. The Artificial Intelligence Act does not set any rules for minimal risk systems, such as spam filters and video games.

Currently, the legal system of the Republic of Lithuania does not have a special legal act that would directly regulate the protection of threats to personal privacy rights posed by artificial intelligence. Nevertheless, it is worth noting that state institutions are actively seeking to implement the provisions of the European Artificial Intelligence Act. Therefore, the initiatives and actions of Lithuanian institutions aimed at preparing and implementing the AI Act in the Republic of Lithuania will be further analyzed.

The sources of the Ministry of Economy and Innovation of the Republic of Lithuania provide the following main obligations of the Republic of Lithuania - to publish a list of institutions protecting human rights, to develop rules on permits for the use of a real-time remote bio-metric identification system for law enforcement purposes, to designate national competent authorities, to develop rules on the application of sanctions, to create AI regulatory sandboxes and develop guidelines for their participants, to implement the right to file a complaint with the market surveillance authority, and to develop rules according to which it is possible to access the documents that the AI system supplier must keep, even if it ceases its activities. These key commitments are planned to be implemented by 02-08-2027. While the Republic of Lithuania is fulfilling its obligations, AI system suppliers will also have to fulfill their obligations in parallel (*Ministry of the Economy and Innovation of the Republic of Lithuania, 2025*).

The Republic of Lithuania has already fulfilled certain obligations, for example, a list of institutions protecting human rights has been published. The following institutions are key in protecting human rights in Lithuania when using high-risk AI systems:

1) The Office of the Equal Opportunities Ombudsman – the institution's primary goal is to ensure that private and public persons do not violate the principle of equality of persons and comply with the prohibition of discrimination.

2) Seimas Ombudsman's Office – this institution monitors human rights in Lithuania, also initiates investigations into fundamental human rights problems, and carries out dissemination and public education on human rights issues.

3) The Office of the Ombudsman for the Protection of Children's Rights – the purpose of this office is to improve the legal protection of children, protect the rights of the child and their legitimate interests.

4) The Office of the Inspector of Journalistic Ethics – investigates human rights violations in the media.

These institutions, based on Article 77 of the AI Act, have the right to request access to and receive all documents stored under the AI Act related to the use of high-risk AI systems, and to submit requests to the market surveillance authority to organize a test of the high-risk AI system if the documents received are not sufficient to ensure that the EU legislation on the protection of human rights has not been violated. The institutions on this list also have an obligation to inform the market surveillance authority of any request submitted for access to stored documents, to cooperate with the market surveillance authority and to comply with the confidentiality requirements set out in Article 78 of the AI Act (*Ministry of the Economy and Innovation of the Republic of Lithuania, 2025*).

A common list of national measures was also analyzed; these measures will help the state implement the established requirements, which all member states must implement. The list contains a total of sixteen measures, three of which, considered the most significant, are highlighted below (*Ministry of the Economy and Innovation of the Republic of Lithuania, 2025*):

1) Draft Law on amendments to Articles 1, 2, 11, 13, 14, 17, 21 of the Law of the Republic of Lithuania on Technologies and Innovations No. XIII-1414 and supplementing the law with an annex. The aim of the project is to designate the public institution Innovation Agency as the national competent authority – notifying authority, and to establish that the public institution Innovation Agency would be responsible for the creation of a limited pilot regulatory environment for artificial intelligence and the supervision of the operation of this environment. This measure is highlighted as important because institutional coordination is essential to ensure smooth cooperation between Member States and between national and the EU institutions.

2) Draft Law on amendments to Articles 1, 2, 23 and the Annex to the Law No. X-614 of the Republic of Lithuania on Information Society Services. The aim of the project is to designate the Communications Regulatory Authority of the Republic of Lithuania as the national competent authority – market surveillance authority, and also to entrust it with the functions of a single contact point. As a result of the implementation of this project, the Communications Regulatory Authority of the Republic of Lithuania has become the key entity responsible for technology oversight, transparency, and compliance.

3) Draft Law on the Application and Supervision of Artificial Intelligence. The objectives of the project are to lay down rules on sanctions and other enforcement measures, which may also include warnings and non-pecuniary measures, to be applied for infringements of this regulation by operators, and to take all necessary measures to ensure that they are properly and

effectively implemented. Determine the distribution of functions between institutions performing supervision of AI systems market (national competent authorities and other supervisory authorities). The implementation of this project will ensure sanctions and enforcement mechanisms and a clear division of functions between the institutions performing supervision.

In the context of today, the adoption of the AI Act is of great importance. In particular, the European Union is becoming a leading jurisdiction that has set standards for AI ethics and security that other countries may adopt in the long term. This act also protects citizens' rights in the context of artificial intelligence by establishing clear guidelines for its development and use. Another important aspect is the creation of legal clarity for legal entities, which will help companies develop AI technologies while knowing clear boundaries. In addition, given the rapid development of technologies and changing operating principles, after the entry into force of the AIA, although the act regulates high-risk AI systems in detail, constant monitoring and real-time updates in the event of changes are important in order to avoid the use of legal loopholes. Practical implementation is also an important aspect, a major challenge awaits the European Union countries, which will have to ensure that the AI Act is effectively applied and not circumvented.

For this reason, the pursuit of implementing the European Union Artificial Intelligence Act becomes particularly important, and the implementation of the initiatives and requirements of Lithuanian state institutions in this context becomes a particularly positive indicator. The formation of national legal instruments and institutional structures is an important step in preparing Lithuania for effective regulation of artificial intelligence.

## The impact of the application of artificial intelligence technologies on the protection of the person's right to privacy: analysis of practical cases

In order to comprehensively and thoroughly reveal the impact of artificial intelligence on a person's right to privacy, this paper conducts a qualitative study using the case study method. This method was chosen because quantitative methods, such as surveys or statistical analysis, are not appropriate in the context of this work, as the phenomenon being analyzed is primarily very new and related to complex legal, ethical, and technological areas.

*Case study provides an opportunity to thoroughly analyze and describe a single event or fact in a real context and to describe (explain) the phenomenon under study, especially when the boundaries between the phenomenon and its context are not clear. This is a qualitative research strategy that involves a detailed, in-depth examination of one or more specific cases that illustrate the problem under study. Here, the main focus is on a specific case, which is attempted to be described and explained in as much detail as possible, and to answer the research questions.*

The specific cases chosen – „Clearview AI“ and „Cambridge Analytica“ – are not accidental. They are both directly and widely known to the public and are associated to significant violations of the right to privacy committed using artificial intelligence technologies. The analysis of these two cases allows not only to reveal specific threats to privacy protection arising from the application of artificial intelligence, but also to formulate recommendations and insights that may be useful in developing and improving legal regulation in this area. The selected cases also perfectly illustrate the importance and relevance of the legal and technological aspects analyzed in the theoretical sections in the practical space, therefore, the case analysis in this work will be useful in achieving comprehensive and practically based conclusions.

The Clearview AI case was chosen because the company used facial recognition technology based on artificial intelligence to illegally collect the bio-metric data of millions of people from public internet sources, social networks, and other platforms. This case reveals the specific risks posed by automated, mass collection and processing of bio-metric data using artificial intelligence.

The Cambridge Analytica case is important because it reveals how artificial intelligence-based profiling and data analysis systems can be used not only for commercial but also for political purposes, manipulating individuals and their privacy. This case also allows us to take a deeper look at the issues of psychological profiling and manipulation of personal data.

**„Clearview AI“ case assessment under the European Union AI Act**

After analyzing the factual circumstances of this case, violations of the right to privacy, and the actions of the institutions of the European Union member states against the „Clearview AI“ company, it is worth noting that, first of all, this case forms a unified position of personal data protection authorities, which indicates that even if a company carries out its technology activities outside the European Union, it must comply with the common European Union legislation, such as the GDPR, if it processes the data of the EU citizens. This case also highlighted other important aspects in the context of the right to privacy, for example, that the protection of bio-metric data and the protection of personal images are distinguished as particularly sensitive areas, therefore, in the event of threats to this data, institutions immediately take action and impose particularly strict sanctions for identified violations, and such threats are not ignored in the European Union.

On January 18, 2020, The New York Times published an article titled „The secretive company that might end privacy as we know it“ that publicly revealed the activities of „Clearview AI“ for the first time. Until then, the company had operated quietly and was reported to have used its services by more than 600 law enforcement agencies, as well as several private companies. The question has been raised whether activities of „Clearview“ violate legal regulation by using facial recognition technology.

On June 10, 2020, the European Data Protection Board (EDPB) issued a preliminary assessment expressing serious doubts about the legality of such a service in the context of the EU law. *"In its response to MEPs on the „Clearview AI“ tool, the EDPB also shared its concerns about certain developments in facial recognition technology." The EDPB recalls that, under the Law Enforcement Directive (EU) 2016/680, law enforcement authorities may process bio-metric data for the purpose of uniquely identifying a natural person only in accordance with the strict conditions of Articles 8 and 10 of the Directive. The EDPB has doubts as to whether any Union or Member State law provides a legal basis for using a service such as the one offered by „Clearview AI“. Therefore, as it stands and without prejudice to any future or pending investigation, the lawfulness of such use by the EU law enforcement authorities cannot be ascertained. Without prejudice to further analysis on the basis of additional elements provided, the EDPB is therefore of the opinion that the use of a service such as „Clearview AI“ by law enforcement authorities in the European Union would, as it stands, likely not to be consistent with the EU data protection regime.*

It should be noted that this case was assessed by the institutions based on the GDPR norms, since at the time the European Union Artificial Intelligence Act had not yet entered into force, therefore this study also aimed to assess how the activities of the „ClearView AI“ company in this case would be assessed based on the provisions of the newly entered European

Union Artificial Intelligence Act, how the activities of this company would be assessed, and what the differences would be when applying the AI Act compared to the GDPR.

Under the Artificial Intelligence Act, „Clearview AI“ is believed to have violated at least one clearly stated prohibition. Certain AI systems are prohibited altogether if they pose unacceptable risks. For example, Article 5(e) of the EU AI Act, “making available on the market, putting into service for this specific purpose or using AI systems that create or extend facial recognition databases by non-targetedly collecting facial images from the internet or from security video surveillance systems (CCTV) footage”

„Clearview AI“ automatically collected facial images for its system from publicly available online sources, including social networks, news portals, and public videos. In this way, these images were used to create a bio-metric database, which was later offered commercially to law enforcement agencies. It is believed that such practices directly correspond to prohibited activities under the cited Article 5 of the DI Act, since the data was collected inappropriately, without consent, from the public internet space. Given the scope of the regulation set out in Article 1 of the Artificial Intelligence Act, it is clear that the activities of „Clearview AI“ would have fallen within the scope of the Regulation. According to Article 1(a), (c) of the AI Act, the AI Act applies to both suppliers and installers, regardless of whether they are established in the European Union or in a third country, if their AI systems are used in the Union or have an impact on the Union residents. Although Clearview AI is based in the United States, the company collected and processed bio-metric data and facial images of citizens of the European Union countries and offered its technology for use by law enforcement authorities in several EU member states, including Sweden, Italy, France, and Austria. Such actions clearly comply with the provisions of the AI Act.

Given that in practice the authorities have applied the strictest penalties based on the provisions of the GDPR, and that the AI Act would include this company's technology in the scope of prohibited systems, it is reasonable to assume that in such a situation the AI Act would also impose severe penalties as provided for in Article 99 of the Act - „Non-compliance with the prohibitions on AI-related practices referred to in Article 5 shall be subject to administrative fines of up to EUR 35,000,000 or, in the case of an undertaking, up to 7% of its global annual turnover in the preceding financial year, whichever is higher.“

The „Clearview AI“ case has exposed the threats that artificial intelligence-based bio-metric systems can pose to a person's right to privacy. The company's illegal practice of collecting facial images, ignoring the rights of data subjects, and transferring data to third countries without safeguards and contracts - all of this has shown how modern technologies can be used to violate human rights principles. The European Union member states, through their data protection authorities, reacted unanimously, imposing large financial sanctions and adopting decisions on data removal and cessation of activities. Analyzing this case under the European Union Artificial Intelligence Act, it is clear that such a system falls into the category of prohibited AI systems, therefore the sanctions could be even stricter than under the GDPR.

This case becomes significant not only in legal practice, but also in creating clearer standards for regulating artificial intelligence, in order to prevent the misuse of personal data in the future. The work continues with another famous case analysis, „Cambridge Analytica“, which, although based on different technology, also involves the use of data without explicit consent and reveals a different way of using artificial intelligence tools - to manipulate the obtained personal data in order to influence their political choices.

**Assessment of the „Cambrigde Analytica“ case under the European Union AI Act.**

„Cambridge Analytica“, a company founded in the United Kingdom, has presented itself as an advanced data analytics company that helps reach specific groups of individuals based on their behavior, opinions, and habits. They said they use a lot of information about people's ages, interests, political views, and even psychological traits to create highly targeted marketing messages. The company also used sophisticated data analysis and prediction techniques to identify groups of people who behave similarly and deliver tailored content to them. This information was collected from different sources, sometimes even without people's consent, and decisions were made on its basis in political campaigns and advertising. In simple terms, this system worked like this: if a person liked certain posts on social media, watched a specific type of video, browsed certain pages, or shared certain content, all of this activity was analyzed to create a psychological portrait of the person. Based on this portrait, political messages or advertising were applied to the person while they were browsing the internet, which was intended to influence their opinions or behavior.

In summary, the most important features of this company's activities can be distinguished: it was a private data analysis company, it helped political parties and businesses reach target groups of people, data was collected from various public and not always transparent sources, people were assessed, their personality, values, and behavior were analyzed, and the created content was adapted to specific groups and shown to them through various digital and social channels.

When assessing the activities of CA in accordance with the provisions of the AI Act, there is no doubt whether the data analysis system they used, based on profiling and automated decision-making, did not violate the restrictions or prohibitions set out in the AI Act. For example, Article 5(a) of the AI Act prohibits – „using an AI system that uses methods that affect the subconscious mind of a person, of which the person is unaware, or that purposefully uses methods of manipulation or deception, with the aim of substantially changing the behavior of a person or group of persons, or by substantially changing that behavior, significantly weakening their ability to make a reasoned decision, thereby forcing them to make a decision that they would not have made otherwise…“. Considering that CA used advertisements that were purposefully shown to specific people, based on their psychological profile, it can be argued that this could be seen as an attempt to exploit a person’s psychological vulnerability.

Viewed through the prism of Article 5(c) of the European Union Artificial Intelligence Act, it can be argued that activities of „Cambridge Analytica“ theoretically met certain characteristics of prohibited practices. Article 5(c) of the EU AI Act – „making available on the market, putting into service or using AI systems to assess or classify natural persons or groups of persons for a given period of time on the basis of their social behavior or known, inferred or foreseeable personal or personality traits, where the social ranking results in one or both of the following: i) harmful or unfavorable treatment of certain natural persons or groups of persons in social contexts that are not related to the contexts in which the data were originally generated or collected; ii) harmful or unfavorable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behavior or its dangerousness.“ In simple terms, it can be assumed that the essence of this prohibition is to protect people from being unfairly assessed on the basis of their behavior, especially when that behavior has nothing to do with the situation in which it is subsequently used. For example, if a person on „Facebook“ „likes“ patriotic posts or articles about security, it doesn't mean they need to be shown political ads from one party or biased information about immigration. Or if a person is interested in health and alternative medicine online, they should not automatically be classified as those who

distrust science and be constantly exposed to misinformation. This protects people from getting the wrong impression based solely on their clicks or browsing habits. „Cambridge Analytica“ collected and analyzed data provided by users on social networks, created psychological profiles, and used them for political purposes - aiming to influence people's opinions and behavior in elections.

Taking into account these provisions, it can be assumed that if the activities of the CA were assessed under the new AI Act, there would be reasonable grounds to apply the prohibitions specified in Article 5. This would mean the possibility of imposing correspondingly severe fines, as provided for in Article 99 of the AI Act - up to 35 million euros or 7% of global annual turnover, and the company's systems would be considered in the group of prohibited practices.

## Conclusions

After analyzing the concept, development, and main characteristics of artificial intelligence, it can be stated that it is a rapidly developing and multi-layered technology, the definition of which depends on the approach - scientific, practical, or technological. Although there is no single definition, most sources agree that AI is the ability to automate tasks that require human intelligence. Its classification by operating principle, level of intelligence, and scope of application helps to better understand which technologies are considered AI and in what areas they are used. Historical development shows how AI has moved from ideas to practical application, and today's possibilities also raise new questions about its impact on humans and their rights.

Modern society and the development of AI technologies have led to the fact that the concept of privacy is no longer understood only as the inviolability of the body or home - today it is increasingly associated with the right to control information about oneself in the digital space. AI's ability to automatically collect, analyze, and predict based on personal data poses serious threats to informational autonomy. Therefore, protection against unauthorized use of data becomes an essential part of privacy. This transformation of the law shows that in the era of AI, privacy must be understood as the right to control data, not just as the inviolability of physical space.

The current legal regulation of the person's right to privacy in the Republic of Lithuania in the context of artificial intelligence is primarily based on the General Data Protection Regulation applied by the European Union, which ensures the basic principles of data protection and is directly applicable in the Member States. The latest and most significant step in this area is the adoption of the Artificial Intelligence Act, which becomes the world's first legal act that systematically regulates the use of AI and seeks to ensure human rights, including the right to privacy, against the backdrop of technological development. There are currently no national legal acts directly regulating the interaction of AI and privacy in Lithuania. However, both Lithuania and all the EU Member States are actively preparing for the full implementation of the Artificial Intelligence Act, developing national measures and forming a network of responsible institutions, aiming to ensure the practical application of this legal act.

The practical impact of the application of artificial intelligence technologies on the protection of a person's right to privacy, as analyzed in the cases of „Clearview AI“ and „Cambridge Analytica“, reveals that the main threats arise not from the technology itself, but from how and for what purposes it is used. Both cases examined demonstrated systematic privacy violations – from the illegal collection of bio-metric data without consent to the creation and manipulation of a person's psychological profile for political purposes. The European

Union's Artificial Intelligence Act would theoretically have allowed such practices to be designated as prohibited – both due to the inappropriate collection of bio-metric data and profiling methods. This shows that the new regulation has great potential to more effectively protect the person's right to privacy in the context of AI by clearly identifying risky or illegal systems. At the same time, the study revealed an important insight: technical progress alone is not enough; strengthening transparency, information, and personal control over data is necessary.

## References

1. Cambridge Analytica. Available at: https://web.archive.org/web/20160216023554/https://cambridgeanalytica.org/services (Accessed: 16 April 2025).
2. European Commision, 2024. *AI Act enters into force.* Available at: https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en (Accessed: 1 August 2024).
3. European Data Protection Board. 2020. Europos duomenų apsaugos valdybos (EDAV) trisdešimt pirmoji plenarinė sesija. Darbo grupės dėl mobiliosios programėlės „TikTok“ sudarymas, atsakymas EP nariams dėl „Clearview AI“ priemonės naudojimo teisėsaugos institucijose, atsakymas ENISA patariamajai. Available at: April 11, 2025 https://www.edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_lt (Accessed: 18 March 2025).
4. European Data Protection Board. 2022. Facial recognition: Italian SA fines Clearview AI EUR 20 million. Available at: https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en (Accessed: 18 March 2025).
5. Google AI principles. *Our approach to building beneficial AI.* Available at: https://ai.google/static/documents/EN-AI-Principles.pdf (Accessed: 15 May 2025).
6. Google trends, 2024. Available at: https://trends.google.com/trends/explore?date=today%205-y&q=artificial%20intelligenc&hl=en-GB (Accessed: 15 November 2024).
7. Harwell, D. 2019. A face-scanning algorithm increasingly decides whether you deserve the job. *The Washington post*. Available at: https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/ (Accessed: 28 April 2025).
8. Hill, K., 2022. *The Secretive Company That Might End Privacy as We Know It, Ethics of Data and Analytics*, Auerbach Publications. Available at: https://www.taylorfrancis.com/books/edit/10.1201/9781003278290/ethics-data analytics-kirsten-martin?refId=0c5e2440-1219-47a1-9ab6-7d08f91f9854&context=ubx (Accessed: 18 March 2025).
9. Hou, R., Fu, D. 2022. Sorting citizens: Governing via China's social credit system. *Governance* 1-20.Available at: https://www.researchgate.net/profile/Rui-Hou2/publication/365862623_Sorting_citizens_Governing_via_China%27s_social_credit_system/links/6464f64a702026631653fff0/Sorting-citizens-Governing-via-Chinas-social-credit-system.pdf (Accessed: 28 November 2024).
10. IBM. *History „Deep blue*“. Available at: https://www.ibm.com/history/deep-blue (Accessed: 18 March 2025).

11. Joshi, N., 2002. 7 Types of artificial intelligence, *Forbes*. Available at: https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/?sh=45e12add233e (Accessed: 28 November 2024).
12. Lecun, Y., Bengio, Y., Hinton, G. *Deep learning.* Available at: https://hal.science/hal-04206682/document (Accessed: 26 May 2025).
13. Levine, I. 2024. *How Amazon is using generative AI to improve product recommendations and descriptions*, Available at: https://www.aboutamazon.com/news/retail/amazon-generative-ai-product-search-results-and-descriptions (Accessed: 15 May 2025).
14. Ministry of the Economy and Innovation of the Republic of Lithuania, 2025. Bendras nacionalinių priemonių sąrašas. Available at: https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/nacionaliniu-priemoniu-sarasas/ (Accessed: 28 April 2025).
15. Ministry of the Economy and Innovation of the Republic of Lithuania, 2025. Laiko juosta - DI akto įsigaliojimas ir pagrindiniai įsipareigojimai. Available at: https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/laiko-juosta/ (Accessed: 28 April 2025).
16. Ministry of the Economy and Innovation of the Republic of Lithuania, 2025. Žmogaus teises ginančių institucijų sąrašas. Available at: https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/zmogaus-teises-ginancios-istaigos/ (Accessed: 28 April 2025).
17. McCarthy, J. 2007. *What Is Artificial Intelligence?*. Available at: https://www-formal.stanford.edu/jmc/whatisai.pdf (Accessed: 15 May 2025).
18. Mims, Ch. 2024. A Powerful AI Breakthrough Is About to Transform the World, *The Wall Street Journal*. Available at: https://www.wsj.com/tech/ai/a-powerful-ai-breakthrough-is-about-to-transform-the-world-095b81ea? (Accessed: 28 November 2024).
19. Mokslo medis. *Tyrimų metodai ir metodikos*. Available at: https://mokslomedis.lt/atvejo-studija/ (Accessed: 28 April 2025).
20. Nilsson, N. J. 2009. *The quest for artificial intelligence a history of ideas and achievements*, Cambridge University Press. Available at: https://ai.stanford.edu/~nilsson/QAI/qai.pdf (Accessed: 16 April 2025).
21. P*inecone. AlexNet and ImageNet: The Birth of Deep Learning*, 2024. Available at: https://www.pinecone.io/learn/series/image-search/imagenet/ (Accessed: 15 November 2024).
22. Russel, S. Norvig, P., 2022. *Artificial intelligence a modern approach*, Pearson Education Limited. Available at: https://dl.ebooksworld.ir/books/Artificial.Intelligence.A.Modern.Approach.4th.Edition.Peter.Norvig.%20Stuart.Russell.Pearson.9780134610993.EBooksWorld.ir.pdf (Accessed: 16 April 2025).
23. Santos, O., Radanliev, R. 2024. *Beyond the Algorithm: AI, Security, Privacy, and Ethics.* Addison-Wesley Available at: https://www.google.lt/books/edition/Beyond_the_Algorithm/QHriEAAAQBAJ?hl=lt&gbpv=0 (Accessed: 18 November 2024).
24. Strikaitė-Latušinskaja, G. 2022. Automatizuoti administraciniai nurodymai Lietuvoje, *Teisė*, Vol. 125, pp. 145–160, Vilnius University Press. Available at:

https://www.zurnalai.vu.lt/teise/article/download/30836/29758? (Accessed: 18 March 2025).

25. Tableau. com. *What is the history of artificial intelligence?* Available at: https://www.tableau.com/data-insights/ai/history (Accessed: 26 May 2025).
26. TeisėPro, 2024. *Įsigaliojo DI aktas: kokie reikalavimai bus pradėti taikyti artimiausiu metu.* Available at: https://www.teise.pro/index.php/2024/08/06/isigaliojo-di-aktas-kokie-reikalavimai-bus-pradeti-taikyti-artimiausiu-metu/ (Accessed: 18 March 2025).
27. TeisėPro, 2025. *ES dirbtinio intelekto aktas: pirmosios nuostatos jau taikomos.* Available at: https://www.teise.pro/index.php/2025/02/06/es-dirbtinio-intelekto-aktas-pirmosios-nuostatos-jau-taikomos/ (Accessed: 18 March 2025).
28. The Applications of AI in Natural Language Processing, Computer Vision, and Speech Recognition, 2023. Available at: https://www.futureskillsprime.in/blogs/applications-ai-natural-language-processing-computer-vision-and-speech-recognition/ (Accessed: 18 March 2025).
29. Turing, A. M. 2024. *Mind a quarterly review of psychology and philosophy*, Outlook Verlag, VOL. LIX. NO. 236, p. 433-460. Available at: https://www.eliassi.org/turing-mind-1950.pdf (Accessed: 15 May 2025).
30. Westerlund, M. 2019. *The Emergence of Deepfake Technology: A Review*, Technology Inovation Management, Vol 9 (11). Available at: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf (Accessed: 15 May 2025).