Universidad de Valladolid

Escuela de Ingeniería Informática

University of Valladolid

Faculty of Computer Engineering

Máster en Business Intelligence y Big Data en Entornos Seguro/Master Business Intelligence and Big Data in cyber-security environment

Trabajo Fin de Máster / Master Thesis

"Implicaciones laborales de la inteligencia artificial"

"Job Implications of Artificial Intelligence"

Zahraa Khazaal Rashad Mohammed

Supervisor:

Dr.Henar Álvarez Cuesta

2022-2023

Universidad de Valladolid

Escuela de Ingeniería Informática

Certificado de implementación del trabajo de fin de máster titulado "Implicaciones laborales de la inteligencia artificial", presentado por la **Sra. Zahraa Mohammed** *en Ingeniería Informática, en Máster en Business Inteligencia y Big Data en Entornos Seguro, Universidad de Valladolid Bajo supervisión Dr.***Henar Álvarez Cuesta** *Catedrática de Derecho del Trabajo y de la Seguridad Social en Universidad de León.*

Universidad de Valladolid

Faculty of Computer Engineering

Certificate of implementation of the master's thesis entitled "Job Implications of Artificial Intelligence", presented by **Ms. Zahraa Mohammned** *in the faculty of Computer Engineering Master in Business Intelligence and Big Data in cybersecurity Environment, University of Valladolid Under the supervision of* **Dr. Henar Álvarez Cuesta** *Labor Law and Social Security in University of León.*

Dr. Henar Álvarez Cuesta

Acknowledgment

It was a great pleasure to study and learn on this master's with competent professors.

First, I would like to express my sincere gratitude and appreciation to my supervisor, Prof. Dr. Henar Álvarez Cuesta, for her guidance, encouragement, support, trust, and patience with me from the beginning.

I would also like to express my deepest gratitude and appreciation to my professors and colleagues for their in-valuable contributions and encouragement towards completing my studies.

I would like to express my gratitude to my mother for never stopping encouraging and supporting me. And I dedicate it to the soul of my father, may God have mercy on him.

To my beloved husband for never stopped standing by me with his love and kindness and to my beloved children for their endless love. My brothers, my father-in-law, and my dear mother-in-law thank you all for your endless love, kindness, and support throughout my studies.

Dedicated to my beloved Family

“Thank you for always believing in me and never giving up on me”

Table of Contents

List of Figures

List of Tables

Keywords: European Union, regulation, European Commission, General Data Protection Regulation (GDPR).

Abstract

Artificial Intelligence (AI) technology has become increasingly widespread in today's society, yet its potential and development are still in the early stages. Similarly, the establishment of policies and regulatory frameworks to govern AI is still in progress. This thesis work dealt with the use of AI in the workplace, and two main problems were highlighted:

The first problem is related to the nature of decisions made by artificial intelligence and its impact on work. Where bad decisions happen by using algorithmic bias or exploiting the systems and invading the privacy of workers and customers and affecting basic rights and safety. This can draw attention to issues of safety, transparency, accountability, job losses, discrimination biases, and the malevolent uses and poor decision-making.

The second problem is improving working conditions and ensuring that the systems comply with the proposed regulations from the regulation proposed on April 21, 2021, by the European Commission that aims to introduce a common the regulation legal framework for artificial intelligence and General Data Protection Regulation (GDPR) which applied since May 25, 2018, and is regulated by European Union (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016. Also, by Organic Law 3/2018, of December 5. These regulations are ensuring security and safety for the users of these systems. In fact, the formation of good regulations limits errors and malicious practices.

In addition, regulations should be imposed on companies to curb systems of artificial intelligence which has a negative impact on workers before putting these products on the market.

Resumen

La tecnología de Inteligencia Artificial (IA) está muy presente en la sociedad actual, pero aún está en pañales en términos de su potencial y desarrollo. Esto también se aplica al desarrollo de políticas y los marcos regulatorios que las rigen. Esta tesis trató sobre el uso de la IA en el lugar de trabajo y se destacaron dos problemas principales:

El primer problema está relacionado con la naturaleza de las decisiones tomadas por la inteligencia artificial y su impacto en el trabajo, y puede llamar la atención la mala toma de decisiones utilizando sesgos algorítmicos o explotando los sistemas e invadiendo la privacidad de los trabajadores y clientes y afectando los derechos básicos y la seguridad. a cuestiones de seguridad, transparencia, rendición de cuentas, pérdidas de empleo, sesgos de discriminación y usos malintencionados y mala toma de decisiones.

El segundo problema es mejorar las condiciones de trabajo y asegurar que los sistemas cumplan con las regulaciones propuestas a partir del reglamento propuesto el 21 de abril de 2021 por la Comisión Europea que tiene como objetivo introducir un marco legal común para el reglamento de inteligencia artificial y el Reglamento General de Protección de Datos (RGPD) que es de aplicación desde el 25 de mayo de 2018, y está regulado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y también por la Ley Orgánica 3/2018, de 5 de diciembre, y que garantiza seguridad y protección para los usuarios de estos sistemas y la formación de buenas normas limitan el error y las prácticas maliciosas. Además, se debería imponer normativa a las empresas para frenar los sistemas de inteligencia artificial que tiene un impacto negativo en los trabajadores antes de poner estos productos en los mercados

Chapter One

1.1 Introduction

Artificial intelligence (AI) refers to systems or machines that simulate the process of human intelligence to perform tasks accurately, and they can predict the results based on previously defined and collected sets of data. Artificial intelligence manifests itself in several ways [1]; chatbots can provide efficient and accurate answers to users by simulating conversations using AI, creators use AI to analyze the flow of critical information in a fast manner like a large pool of text data to improve scheduling recommendations, and engines running different programs on computers can make automatic recommendations for TV shows based on users' viewing habits by using AI algorithms. AI-powered recruitment solutions have made hiring easier and more routine, increased employee quality by keeping track of their performance, eliminated prejudice, and improved recruiting based on true potential.

AI is more about the ability to accurately analyze data than it is about doing a specific task. While it may conjure visions of advanced, human-like robots dominating the world, its purpose is not to supplant humans. Instead, AI strives to significantly augment human capabilities and contributions, establishing itself as a highly valuable asset for businesses [2].

Today, artificial intelligence is playing a major role in changing the world of work. It automates millions of jobs (technology performs tasks instead of people), which some see as a real threat to workers. In fact, the role of artificial intelligence should not pose a threat to humans, but the development of artificial intelligence leads to managing risk at work and improving some aspects by using it to carry out repetitive and dangerous tasks, which guarantees human safety.

Indeed, artificial intelligence creates jobs and can be used as part of training solutions that can be relied upon to develop employees and improve their skills, which makes them more prepared for future work requirements.

AI systems and technologies are often biased towards skills, which explains how they automate human capabilities such as comparison, prediction, knowledge, and perception. Actually, the effects of AI on labor markets are still unclear, mainly due to the fact that AI technologies in the workplace are still new and not yet widely deployed. While the research evidence on how many jobs have so far been replaced by AI-enabled devices remains inconclusive, future studies will have differing views on fundamental rights, worker safety, and the preservation of their fundamental rights, which must be supported by EU regulations and the European Private Data Protection Act in the European Union by 2018. This is why analyzing the regulation proposal is necessary to apply it properly to the AI systems used in the labor market and their impact on workers [3].

Many experts, in general, agree that AI-driven automation will not lead to widespread job loss but rather a transformation of job roles. As tasks are reassigned between humans and machines, the skill requirements and task profiles for jobs will undergo two distinct changes. The first shift causes a new division of labor in which humans are given unique tasks that are difficult to automate and may be related to decision-making, while machines perform repetitive and dangerous tasks that require constant attention and stamina.

AI has countless benefits that can be achieved through automation, and some of these benefits include increased automation, accuracy in disease diagnosis, and smart decision-making. In terms of increasing automation, AI is able to carry out tasks that were previously complex and costly. This is particularly true in areas such as healthcare, where they are able to diagnose diseases accurately and without the need for human input. In terms of accuracy in diagnosing diseases, AI is able to process large amounts of data more accurately than humans, and this is particularly important in fields such as medicine, where ensuring accuracy is critical to ensuring patient safety. AI also has benefits in decision-making by aiding the process of making decisions under pressure. For example, it can identify hard-to-see patterns, such as correlations between data sets. As AI continues to evolve and gains more widespread adoption, the benefits provided by automation will increase.

In view of the importance of the work of these machines, they must abide by the laws, comply with the regulations, be transparent, and ensure the security of the information owned by these systems to preserve basic rights and avoid any exploitation that harms work, workers, the work environment, and the preservation of basic rights.

This may exacerbate inequality, increase wage discrimination, and create disparities in working conditions among different groups of workers, as well as can potentially perpetuate and amplify existing inequalities in employment. Starting with approaching the concept of artificial intelligence from a purely theoretical point of view and defining a series of criteria and topics that will move freely and resolve potential uncertainties about it. As well, the ethical use of artificial intelligence information to provide the best solutions must be considered to solve the problem of artificial intelligence from algorithmic bias, video surveillance at work, regulating the use of robots, and existing regulations that can be studied and applied in practice to systems used in companies.

One of the benefits of AI in business is that it can revolutionize manufacturing processes across industries. Also, there are many benefits to AI in manufacturing. Here are some of the points from which companies can benefit while applying AI systems:

1. Direct automation: companies can fully automate complex tasks and reduce the need for human labor. This can save companies money and improve efficiency.
2. Quality assurance: AI can help companies to detect production defects more quickly and efficiently. This can improve product quality and save companies time and money.
3. With AI, companies have the flexibility to quickly adapt to market changes and respond to new challenges.
4. Data access: AI can help companies make data more accessible and useful for decision-making. This can improve work efficiency and accuracy.

While there are many benefits to AI in manufacturing, there is still a lot to learn about its potential applications. As with any new technology, it is important for

companies to explore how AI can fit into existing manufacturing processes and strategies.

In this thesis, the work demonstrates how to use artificial intelligence legally to achieve goals and objectives perfectly and tracks the systematic consequences of using it to achieve compliance.

In addition to knowing the challenges that can be found. AI must be used by individuals and business leaders to develop these systems in a positive way without violating rights. One of the most important tasks that must be available in intelligence systems is to correct the availability of data and monitor these systems, in addition to the pressures that workers face when using these systems and how to deal with them and control their compliance with EU regulations for proper use.

Chapter 2 defines the regulation, the type of organization, and the risks and benefits of AI. In addition, this chapter briefly analyzes the nature of the regulations to be used.

Chapter 3 defines data protection regulations and their relationship to intelligence systems and knowing the level of high-risk systems.

Chapter 4 discusses the application of artificial intelligence systems in reality. And the most prominent risks faced at work and the algorithmic bias used in recruitment, in addition to the obligations of users and suppliers about the systems before and after they are put on the market. Also, the chapter conducts a comprehensive evaluation of the regulation the EU Proposed.

Chapter 5 discusses the conclusions of the research work and offers an outline of the immediate areas for future research.

1.2 Objectives

The main objectives of the thesis are to:

1. Study the social and employment consequences of artificial intelligence systems in all fields of work to preserve the basic rights and safety of users of these technologies. Paying attention to the security of employee data and

their rights. Through suggestions in support of legal regulations, monitor their usage, assess if the laws of AI should be regulated, and identify the medium- and long-term difficulties and prospects of AI, to achieve the goal of justice by preserving the rights of workers, protect them from exploitation and better understand their use of these systems. The study also explores the importance of these systems in business development and employment, as well as how to achieve compliance using the European regulatory framework.

2. Highlights the legal regulations that companies must consider in case of using AI for decision-making in hiring employees or plan to do so in the future. The most important areas of law that can be of interest in the context of this research work are data protection and the fundamental rights of workers and users of these systems provided by the following regulations:

    - The General Data Protection Regulation (GDPR) provides an important legal framework in case companies use AI systems to handle data.

    - The proposed artificial intelligence law is important for legal consideration at work to eliminate discriminatory risks that underlie decision-making patterns, preserve the basic rights of workers and users, and highlight the most important requirements that must be met in systems before being applied to the market by suppliers. Also, ensure compliance with regulations for suppliers and users to run these systems smoothly without any issues by adhering to the EU regulatory framework.

Chapter Two

2.1 Definitions of Artificial Intelligence

The concept of artificial intelligence represents the convergence of various scientific disciplines and technologies, aiming to replicate or simulate human-like intelligence in machines. Through advancements in machine learning, deep learning, natural language processing, and other AI techniques, digital devices can now analyze vast amounts of data, recognize patterns, and make informed decisions, ultimately enhancing their ability to assist and augment human activities in numerous domains such as healthcare, finance, transportation, and more [2].

The most important system of it is the algorithms of artificial intelligence. Artificial intelligence algorithms are defined as specific guidelines and formulas that have been programmed for the computer to follow in order to complete the calculations and are a form of cognitive computing. For this reason, experts define artificial intelligence as "systems that display intelligent behavior by analyzing the environment and taking action" (with a certain degree of autonomy) to achieve specific goals.

AI is classified into two types:

- Narrow artificial intelligence focuses on specialized tasks and demonstrates proficiency in performing them. It is designed to excel in a specific area of intelligence but operates within well-defined boundaries. Examples of narrow AI applications include search engines, image recognition software, personal assistants, and autonomous vehicles.

- General artificial intelligence also referred to as strong artificial intelligence, is an advanced form of intelligence capable of solving a wide range of problems. This type of AI aims to exhibit human-like intelligence across various domains. Achieving such intelligence, especially in the form of machines or robots, remains a significant challenge. Building machines with

human-level intelligence would require the development of neural networks as intricate and complex as those found in the human brain [4].

Examples of operations carried out by digital devices are due to the existence of AI detection tests based on mathematical theories [5]. It is necessary to start by identifying the elements that run in AI systems, such as big data and algorithms, and which can be exploited as raw materials. Developers harness AI to streamline manual tasks, detect patterns, and tackle problems efficiently. Training data is employed to establish associations and patterns that enable AI systems to make accurate predictions. This capability is exemplified in smart robots equipped with AI algorithms that can automatically respond to various stimuli based on the knowledge gained from the training data.

In fact, developers need a background in mathematics, coding, algorithmic expertise, and big data analysis. The concept of big data pertains to the collection and analysis of vast volumes of data from diverse sources, which is then subject to automated processing using computer algorithms and advanced data processing technologies. This process involves utilizing stored and transmitted data in a continuous stream to identify patterns and insights. In addition, it is essential to consider various aspects such as privacy, security, and law enforcement when dealing with big data (2225/2016 ini) [6].

Algorithms and big data are essential components of what is called artificial intelligence. Big data and artificial intelligence complement each other. Here, the AI gets better, and the more data provided, the more efficiently the AI systems work. It also helps organizations better understand their customers. On the other hand, big data is simply useless without software to analyze it, so humans cannot do it efficiently. Especially when applied in the world of work, AI and big data complement each other. So, we need a lot of data for AI to be effective. Artificial intelligence operates in the digital realm by utilizing digital devices and specialized software for analysis, algorithm design, and machine learning. A crucial aspect of AI is its ability to absorb substantial amounts of training data. This data is used to identify patterns and associations, enabling the generation of predictions and automated responses. For example, smart robots can provide automated responses based on learned

patterns, while smart devices can identify and describe objects in images by reviewing countless examples. In summary, AI relies on digital tools and vast training data to form associations, make predictions, and perform intelligent tasks [7][8].

We can define artificial intelligence as "a theory for the development of computer systems that are capable of performing tasks that require human intelligence." It is the specific behavior and characteristics of computer programs that mimic human mental capabilities and work patterns [9]. A definition also used by some scholars [10]. However, it can be defined as "intelligent agent design" [11], including various types of intelligence, not just human. The latter approach will be used in our work, where AI is treated, more precisely, as being able to adapt to various previously unknown situations and achieve goals [12].

This definition is consistent with scientific understanding and is widely used in business. We can also identify the problem of setting the goal of organization, which is important for the correct targeting of efforts. And bias and its reproduction, for example, artificial intelligence technology in the recruitment and evaluation processes, where artificial intelligence is used in recruitment for the purpose of predictive analysis, which helps recruit officials better evaluate employee quality and reduce bias. It also helps recruiters scan and analyze resumes in seconds, but they can reproduce biased tendencies based on gender or race. In these cases, AI systems can help reduce the biases that humans may experience, but they can also create new forms of discrimination that can be problematic if there is not a realistic, unified consensus about what AI means [13]. In addition, there is fear. The use of general terms, such as "intelligence," can lead to difficulties of interpretation when those rules are implemented or when they are discussed in court [14]. For example, this thesis will try to use the definition that artificial intelligence is "the design of intelligent agents" [15]. These definitions are flexible and able to adapt to various previously unknown situations. That seems to be the appropriate term to use. In the first place, because it includes different types of intelligence, not just human intelligence. It also considers the flexible, adaptive, educational, and evolutionary nature of AI. It is neither too narrow nor too comprehensive, which distinguishes it from traditional computer systems. According to the current scientific understanding of the subject, even though generic terms such as "objective" and

"traditional computer systems" are still used, they can be effectively applied in a potential organization, as long as there is some degree of coordination of their meanings [16].

In artificial intelligence systems, there are many problems that we may encounter at work. We mention them:

1. Anomaly detection: AI can analyze data to detect deviations from expected patterns or values, alerting users to abnormal events. One example is the utilization of a network of sensors with predefined ranges. Anything outside of these ranges is considered an anomaly.

2. Probability of a future outcome: AI can leverage existing knowledge and probabilities to estimate the chances of a particular event occurring. Furthermore, AI's proficiency in pattern recognition allows it to identify hidden patterns or relationships that humans might not be aware of. This enables AI to provide valuable insights and predictions based on its unique ability to perceive and understand patterns in data [17].

3. Data Bars and Charts: AI's advanced pattern recognition algorithms enable it to analyze visual data more effectively and identify intricate patterns that may not be apparent to human observers. This ability to uncover hidden insights in graphical representations can be valuable for decision-making and data analysis tasks [18].

It's very important to know that the value of big data is related to its quality. If the quality is low, it means that the information is of no value, and this makes it impossible to trust the data when it is analyzed by artificial intelligence and machine learning.

The regulation of AI algorithms and how they are implemented are based on the core principles underlying the proposed regulatory frameworks, and this will help companies across industries launch AI-based initiatives and expand the use of their technologies.

Machine learning is part of a group of technologies that are grouped under the umbrella of AI. While the terms AI and machine learning are often used interchangeably, it is more accurate to view machine learning as a subset of AI. AI is a broader field encompassing the simulation of intelligent human behavior by machines. Machine learning, on the other hand, focuses on the ability of machines to improve their performance through experience. Its accuracy is achieved by means of algorithms that identify patterns and then use those patterns to create a data model that enables predictions and decision-making within the built-in systems. Through statistical and logical techniques, AI systems can identify, analyze, and predict certain aspects such as behavior and attention, allow information to be extracted from data, and discover new patterns, which will be very important when it comes to providing legal information. A framework for this data and operations within the framework of the employment contract. Automated decision making" means that a user authorizes decision-making, in whole or in part, for an entity through the use of a computer program or service, and that entity will use automatically applied decision-making system models to perform important actions on behalf of the user or to inform the user's decisions when an action is performed Artificial intelligence, machine learning, and deep learning rely on algorithms (not analysts) to find patterns in data and independently make predictions and prescriptions [19], and automated decision making [20][21].

Also, artificial intelligence is defined by the High-Level Group of Artificial Intelligence Systems (AI-HLEG), established by the European Commission to develop the artificial intelligence strategy, as "systems that exhibit intelligent behavior through the ability to analyze the environment and take action independently to achieve the desired goals". The committee applies the term of systems that exhibit intelligent behavior are able to analyze and take measures to achieve specific goals [3][20][22].

Actually, the future of AI and big data holds the promise of enhancing our lives through convenience. Companies that embrace these technologies and prioritize context-driven insights can realize cost savings and achieve a significant return on investment. Recognizing the value of AI and machine learning in utilizing data effectively is a key step for organizations to thrive in this evolving landscape.

So, for data, nothing changes; the collection of data will continue, but with the advancements in AI and big data technologies, the way we analyze and utilize that data will significantly improve. We can expect new and more efficient methods to emerge, enabling us to extract valuable insights and derive meaningful outcomes from the collected data.

It is necessary to evaluate and analyze the impact of artificial intelligence and automation on the future of work and jobs before using them, and this is what the following chapters will try to do. All acquired organization concepts will be applied to answer the main question of this thesis: What is the functional impact of artificial intelligence systems on the future of work and jobs?

2.2 AI Benefits, Security, and Ethical Concerns

Artificial intelligence has captured widespread attention and acceptance among consumers globally. Regular exposure to AI concepts through media and personal experiences fosters confidence and positive impressions, further solidifying the acceptance of AI in society. These interactions contribute to building confidence and trust in AI, especially when it leaves a positive impression [23]. The main principle of AI involves replicating and potentially surpassing human capabilities in perceiving and interacting with the world. This principle has emerged as a key driver of innovation across different domains.

AI's ability to apply different forms of machine learning and recognize patterns in data brings value to businesses in two key ways: providing a comprehensive understanding of data and instilling confidence in predictions for automating complex and routine tasks. These capabilities can empower businesses to make data-driven decisions and enhance operational efficiency [24].

While AI holds promise in addressing societal challenges, others express concerns about the intelligence conferred upon machines. It is important to navigate the development and deployment of AI with careful consideration of ethical and societal implications, ensuring transparency, fairness, and human oversight in the use of AI technologies [23]. Enhanced advances in machine learning can put employees at a disadvantage in carrying out their responsibilities. Most employers will find

machines more efficient, causing them to experience a digital workforce replacement, especially in office assistants, travel agents, teaching positions, etc. [25]. Also, this AI has a range of benefits that can be applied in automated manufacturing, where the technology can speed up production and reduce downtime and costs associated with production. AI can also help improve processes and material utilization, resulting in improved quality and efficiency. Additionally, AI can help identify and prevent potential problems early, resulting in less downtime and higher productivity. In short, AI is transforming industrial manufacturing by providing significant advantages in terms of cost, quality, and efficiency [24]. We cannot forget the ethical concerns raised by the applications of artificial intelligence, for example, in the world of self-driving cars, which raise security and ethical concerns. Cars can be hacked, and when a self-driving car is involved in an accident, the responsibility isn't clear. Self-driving vehicles can also get stuck in a situation where an accident is unavoidable, forcing the programming to make an ethical decision about how to minimize the damage.

Another significant worry pertains to the possible misapplication of AI tools. Hackers have started utilizing advanced "machine learning" techniques to breach secure systems, making security measures more intricate. Additionally, the emergence of deep learning-based video and audio generation tools empowers malicious individuals to create "deep fake" videos. These fabricated videos convincingly depict renowned public figures engaging in actions or uttering statements that never actually occurred. In summary, the misuse of AI tools raises concerns regarding cybersecurity vulnerabilities and the potential for manipulating digital content to deceive and mislead [26][27].

The relationship between artificial intelligence and the law is highly significant due to the increasing prevalence of AI in various aspects of the workplace. This includes areas such as biased algorithms, criminal sentencing, predictive monitoring, and video manipulation. Also, the legal world will be affected by the problems posed by artificial intelligence. Intellectual property rights, competition law, labor law, criminal law and data protection law will be affected, which will have a significant impact on society and the law [28].

2.3 The Legal Concept of Artificial Intelligence Systems

The foundation of AI technology is data, algorithms, and the power of machine learning. Use of our personal data. It is considered one of the most important inputs that companies need through artificial intelligence technologies, but unless legal regulations are put in place, our personal data turns into commodities that will be a tool for profit purposes in the private sector. The possibility of using personal data under the name of monitoring and tracking shall be subject to the supervision of the law. This creates the need for legal regulations that would ensure the protection and confidentiality of such sensitive personal data. Another issue is inequality. The data and algorithms that AI uses were made by humans, but machines can now learn without humans. Legal regulations are needed to prevent data and algorithms from reproducing biases that create inequalities in the work environment. Regulations that would keep the people in the process in such a way as to prevent the emergence of decisions and outcomes that would not benefit society in the parts untouched by human hands in short, legal regulations that will protect human rights must be put in place quickly, considering the new realities revealed by artificial intelligence. Only then will we benefit from technology in a rights-based, fair, and equitable way, and social welfare will increase.

Otherwise, we will witness the emergence of new monopolies and authoritarian powers in this new era and the continuation of the exploitation system today. It is therefore necessary to create new sets of regulations just because a new technology has emerged and has a significant impact on the law. In fact, an example is privacy and data protection laws, which also apply to technologies such as artificial intelligence [29]. Therefore, it became necessary to provide a special and strong legal framework for the use of artificial intelligence. The proposal of the European Union to regulate to ensure the proper functioning of AI and its good use, which is one of the most important priorities of the organizers of this proposal that came out of the European Commission and which is presented as a strong, systematic, and complete regulatory body, Follows the model of the GDPR and a regulation of the European Parliament and the European Council that sets harmonized standards on this matter, artificial intelligence (artificial intelligence law), and SE amending some

legislative acts of the Union in 2021. This will analyze the cross-sectional future regulation of AI in Europe while also briefly reviewing the status of the problem at a business level to contextualize the European regulatory framework. In particular, the main obligations set forth in the European regulation proposal on artificial intelligence will be detailed. Given the intrinsic link between AI and the need to share and process data (whether personal or not), the regulations applicable to personal data will be reviewed from the perspective of privacy (as a fundamental right) [30][31].

Also, in machine learning, algorithms need to be "fed" with huge amounts of data to be able to extract their variables and conclusions, and thus solve the problem faced by the machine. The more data machines analyze, the more power they must make their own decisions. For this reason, the selection of information from which AI systems are fed is critical to ensuring that machine learning and decision-making do not reproduce or exacerbate the biases (racial or sexual) currently prevalent in society. On the other hand, since the machines themselves determine the most efficient processes and decisions and use AI systems, this can lead to unforeseen and not always favorable outcomes for humans. In contrast, the standards that machines follow can be very complex, even for the engineers who were initially programming them, and opaque (not very transparent) to the users who can see them. affected by those decisions. Therefore, the need to regulate or control the development of artificial intelligence is of vital importance so that it cannot affect in a negative way security (physical and psychological) or fundamental rights (in particular, dignity, privacy, and non-discrimination) [32][33]. Currently, there are highly advanced AI projects benefiting humanity developed by public and private entities in areas such as biotechnology research, health, transportation, education, and climate change. On the other hand, the technology can recognize people's emotions and manipulate the human conscience, transporting passengers independently and carrying out features.

Users can predict, with incredible accuracy, the decisions those users will make soon. The implications of using AI systems present a legal, ethical, and social challenge that must be addressed by legislators in a comprehensive manner without affecting the progress of this great tool [20][29].

2.4 Risks and Misconceptions Associated with Artificial Intelligence

Despite the great benefits associated with AI, it is likely to have far-reaching negative connotations, such as the use of systems at work and their impact on workers directly or indirectly. Artificial intelligence indeed presents numerous potential risks, and as the capabilities of AI continue to expand and proliferate, these risks will persist. Some key areas of concern include:

- Lack of traceability: This approach, traceability, allows organizations to track, assess, prioritize, and control AI risks, ensuring that appropriate measures are in place to manage the potential impacts of AI implementations. It is important to have an inventory of the systems and models that utilize AI to enable effective tracking, assessment, prioritization, and control of AI-related risks.

- Introducing programmatic bias in decision-making: this represents a significant risk in AI algorithms, where biases present in the training data can influence decision-making processes. Mitigating this risk requires diverse and representative training datasets, fairness metrics, and ongoing monitoring to address and rectify biases in AI systems. Striving for transparency and accountability in AI algorithms is crucial to ensure unbiased and fair outcomes [34].

- Data sources and violation of personal privacy will become more difficult to protect with the spread of AI, when data leaks or breaches occur, the resulting repercussions can seriously damage a company's reputation and present potential legal breaches with many legislatures now passing regulations restricting how personal data is processed [31].

- Black box algorithms and lack of transparency: the presence of black box algorithms and the lack of transparency in AI systems pose challenges in understanding how predictions and decisions are made. Efforts are underway to enhance explainability and interpretability, promoting transparency in AI algorithms to address concerns around accountability, fairness, biases, and

ethics. As a result, even the creators of these algorithms may struggle to explain precisely how the variables interact to produce the final prediction. This lack of transparency is why some refer to algorithms as "black boxes". [13].

- The capabilities of AI algorithms are uncertain, which raises concerns about legal liability. When AI systems employ fuzzy algorithms and machine learning to enhance decision-making, it becomes challenging to determine who holds legal responsibility for the outcomes. Is it the company developing the AI, the programmer who designed the system, or the system itself? This issue is not hypothetical; in 2018, a self-driving car accident resulted in the death of a pedestrian. The human backup driver was found responsible for not paying attention when the AI system failed. To prevent errors, it is crucial to closely monitor AI systems and ensure proper oversight [35][36].

For all the above issues, we must know: what are the real dangers of artificial intelligence on systems?

The regulations surrounding AI systems adopt a risk-based approach, which is mostly targeting the commercialized or deployed applications of AI. Prohibited uses involve unacceptable risks, while high-risk uses require meeting specific requirements. Low-risk uses typically face fewer regulatory constraints. This approach aims to encourage innovation while safeguarding individuals and promoting responsible AI practices. Uses of AI that harm core values are risky and unacceptable. These are systems that implement subliminal techniques, exploit vulnerabilities, and distort human behavior or are used in computational social recording. The use of AI systems for "real-time" remote identification of people in public places is considered particularly intrusive and is prohibited except in three cases: searching for victims of crime; preventing threats to life and terrorism; and determining the whereabouts of the perpetrators. High-stakes AI systems are at the heart of the list. They are allowed in the market, but they must meet some mandatory requirements [37].

In fact, AI systems can be integrated into products as security components or categorized into different stand-alone product types, such as biometric

identification, critical infrastructure management, vocational education, public services, law enforcement, immigration control, justice administration, and democratic processes. Given the high-risk nature of these applications, it is crucial to implement appropriate measures and requirements to ensure their responsible use and mitigate potential risks [38][39].

2.4.1 BIG Data and Artificial Intelligence in Recruitment

Today, data is no longer just data." Every well-functioning company needs to know where to get that data and how to use it effectively. The term big data is a general term used to describe large amounts of data. Data is produced daily by companies in the internet, telecoms, financial industry, energy industry, healthcare, and transportation. When people talk about big data, they often mean the data hills on the Internet. An automated email comes to your inbox: "A potential employee has been found, the salary and working conditions have already been clarified, and the contract will be signed within a couple of days." Artificial Intelligence has found the perfect employee for your advertised position and has already explained everything without you ever seeing their name or face [40]. AI alone can find a suitable applicant, conduct the interview on its own, draw up contracts, and hire employees. But fully automated recruitment is not allowed, as this leads to bias. This must fall to the human being; that is, this is done through human observation, where this is not possible. This hiring is based solely on evaluating data for AI, which is really more productive and fairer to the company; the problem with AI is the source and the data it refers to. Because if the data collected is actually fake or discriminatory, then the AI will be, and therefore it will be unfair, as AI is constantly evolving based on the data that is collected, and building on this framework is an example of many facial recognition systems that have been trained on white people. They are less likely to identify with black people than others.

A similar problem arises with automatically generated subtitles. With English without accents, subtitles are generated without any problems, but with other languages or English colored with accents, it is difficult for AI to recognize and render them. So, it can happen that some kind of bias system is developed, which, in the worst case, is also reflected in recruitment. For example, if data is collected that

predominantly categorizes men as suitable for certain jobs, the AI will carry out hiring processes based on these assumptions and discriminate against women. If a company's sourcing tool is used exclusively to select potential employees without requiring someone to check the biases they have been taught, there will be more discrimination and unequal opportunity than before, and the work system will be characterized by bias and inequality [41].

2.5 Definition of Regulation

Regulations encompass the identification and organization of activities required to attain goals by dividing them to facilitate their implementation in the necessary time, with the cooperation of multiple employees. It involves dividing tasks based on individual competencies and defining roles to ensure the effective execution of assigned responsibilities [42]. Basically, regulation serves as an administrative process that involves the collection, organization, and coordination of tasks and activities. It includes defining authorities, facilitating coordination between departments, and ensuring efficient and effective achievement of goals. For the regulation of artificial intelligence, the regulation is aimed at ensuring that the systems are safe and respect legislation on fundamental rights as well as the values of the work. Because artificial intelligence is of vital importance for our future, we must manage to strike a delicate balance that will drive innovation and adoption of AI technology across Europe and the world while also retaining all the benefits of AI technology and fully respecting fundamental workers' rights [6][43]. Regulation in the business market refers to the issuance of specific rules, accompanied by some authorized mechanisms to monitor and enforce the rules, i.e., the attempt to provide economic guidance and ethical guidelines for trustworthy artificial intelligence, i.e., imposing economic controls on the behavior of private companies and imposing fines and strict laws for violating behavior that harms basic rights and safety [44][45]. So, you have to know the reasons for regulation in a world where nothing is perfect.

The regulation tool was used to make society work better and to direct the behavior of people and businesses under many conditions that affect society and work. After defining the list, it is important to discuss the reasons behind regulatory

intervention. At the business level, regulation appears when it is assumed that the market is failing to address a particular problem that may cause harm to the public interest [46]. Regulation can be used not only as a means of maximizing economic efficiency but also as a defense for people and the values that society considers relevant when business values are not respected or when they face a high risk. Regulation acts as a tool to direct actions and shape the functioning of various sectors. It provides legal certainty, stability, and incentives to promote smooth operations and development. By setting clear rules and standards, the regulation aims to achieve important societal goals while creating an environment conducive to progress and compliance. Indeed, the goals pursued through regulation can be both timeless and context-dependent. Timeless goals often include improving the lives of individuals and workers, protecting core values, and fostering the overall advancement of humanity. On the other hand, specific goals may vary based on the prevailing social, economic, and cultural conditions of a particular place and time. Thus, when considering the course of regulation, it is necessary to think about humanity in general as well as about the social group in which these decisions will come into effect. Then it is time to examine what makes regulation successful. With this information, it will be possible to assess whether regulations for AI can flourish and evolve [47].

For legal regulation to be effective and efficient, it needs to adhere to several important standards, including:

- Necessity: There must be a reason for organizing it, such as promoting human rights or correcting a market failure, and it must be verified that it is properly complied with.
- Legality: The regulators themselves must have a legal mandate, and the regulations they put in place must have a solid legal basis.
- Targeting: Regulations should be specifically focused on addressing the issue or problem at hand. They should avoid unintended consequences or negatively impacting unrelated areas or entities.

- Proportionality: The measures and requirements outlined in the regulations should be proportional to the intended goal or outcome.
- Legal stability: the organization must be correct and put forward the expected legal obligations to achieve legal certainty;
- Flexibility: to remain appropriate and effective in the face of circumstances and continuous changes.
- Transparency and accountability: the entire organizational work must be owned.

Justifications for decisions made the information and the process as a whole must be fair, comprehensive, clear, simple, and user-friendly, and all parties involved must be informed and consulted in advance. Regulated persons must have sufficient time to comply with the regulation [48].

2.6 Regulation of AI Systems

The European Commission presented a common regulatory and legal framework for artificial intelligence on April 21, 2021. This framework covers various sectors except the military and aims to address the risks of AI while positioning Europe as a global leader in AI governance. It seeks to ensure responsible and trustworthy AI development and deployment while upholding European values and fundamental rights.

The proposed regulatory framework defines artificial intelligence systems as software developed using specific technologies and strategies, such as machine learning. These systems generate information outputs that impact the environments in which they operate, influencing various domains and sectors. The definition helps establish the scope of regulations and guidelines related to AI systems within the framework [49].

The scope of the proposal includes, in addition to users of AI systems located in the EU, providers that place AI systems on the market or enter service in the EU, regardless of their location, providers and users of AI systems located in a third

country, when the output information is used generated by the system in the European Union [43].

Under the proposal, it is important to note that the focus is on regulating specific uses or practices of AI rather than banning entire technologies, such as:

1. Artificial intelligence systems that use subliminal techniques that bypass a person's awareness to fundamentally change their behavior in a way that causes, or is likely to cause, physical or psychological harm to that person or another.

2. Artificial intelligence systems that exploit the vulnerabilities of specific groups based on age or physical and mental disabilities. The aim is to prevent any manipulation or harm that may arise from altering the behavior of individuals belonging to these groups and to promote responsible and inclusive AI practices.

3. Artificial intelligence systems by public authorities for the purpose of assessing or rating the reliability of natural persons.

4. Remote identification systems are "real-time" in publicly available locations for law enforcement purposes, except in certain cases expressly provided.

In terms of permitted uses, a risk-based approach has been developed. In this way, AI systems are classified into high-risk systems, limited or low-risk systems and other systems, with minimal risks it will be mentioned in detail in the next chapter [50].

2.7 Effects of AI

One of the significant impacts of AI is its ability to enhance efficiency and productivity, where AI's ability to automate repetitive and tedious tasks contributes to increased efficiency and productivity within systems. By freeing humans from mundane work, AI allows individuals to focus on more meaningful and important tasks, thereby leveraging their skills and expertise. Additionally, AI systems enhance

operational efficiency by processing large volumes of data and enabling more informed decision-making [51].

While some argue that regulating AI at an early stage may hinder its capabilities, others emphasize the need for proactive measures to address potential risks and ensure responsible development. Finding the right balance between regulation and innovation is a complex task, requiring ongoing monitoring and adaptability to keep regulations effective and relevant in the dynamic AI landscape. So, It is important to establish regulatory frameworks that are agile and can evolve alongside the technology to effectively govern AI while encouraging innovation [52].

For example, AI has made significant contributions to healthcare. It enables better diagnosis and treatment in healthcare by analyzing massive amounts of medical data. In the finance sector, improving investment decisions, fraud detection, and operational efficiency. [53].

According to proponents, AI possesses the capacity to address intricate issues like climate change and diseases in unprecedented ways. However, critics express worries regarding AI's impact on employment, fearing widespread job losses due to automation replacing human workers. This situation could exacerbate poverty and inequality as displaced workers face challenges in finding new opportunities within a competitive labor market. For example, bias in AI algorithms, such as facial recognition technologies, is a legitimate concern. Efforts are being made to address this issue by promoting transparency, accountability, and fairness in AI systems.

Diverse data collection, rigorous testing, and multidisciplinary approaches are important steps to mitigate biases and ensure responsible AI practices. Public awareness and engagement play a vital role in demanding accountability and promoting ethical AI development [54].

The Regulatory Commission emphasizes the importance of transparency, accuracy, and security in AI systems to prevent algorithmic bias. Compliance with regulations and a commitment to transparency and human oversight are essential for achieving justice and ensuring that this form of artificial intelligence as "high risk” is used in a fair and accountable manner [43].

2.8 General Data Protection Regulation (GDPR)

The GDPR is a regulation in the EU that aims to safeguard the privacy and rights of individuals in the EU by establishing clear rules and standards for the processing of personal data and ensuring accountability for organizations handling such data. GDPR contains powerful requirements that combine data protection with security and compliance standards [55].

On May 25, 2018, the EU General Data Protection Regulation came into force, and EU bodies are working on data protection reform across Europe. The world of work now must protect data across the European Union and deal with big data, industry, networks, bots, and artificial intelligence, which means that a new regulation is urgently needed. May 2018 saw the launch of these measures. GDPR has one goal: to standardize data regulation across Europe. This raises a question for companies: What regulations do companies and site operators need to consider when dealing with internal and external data? Who is affected? Companies and data protection officers in general are a good foundation for every consumer and for all those affected by data processing. This is because they are protected by the GDPR. In addition, the GDPR regulations also affect the rights of employees. These rules are relevant for all companies with employees. This therefore means that many companies are doubly affected, as it relates to employee privacy and employment data protection, as well as the privacy of customers, suppliers, and website visitors [56].

Regulations greatly increase the number of these across the continent. Public authorities and all companies whose main activity relates to the processing of personal data are required to appoint a data protection officer at the company level, even if the main activity of the company is not related to data processing; if so, there are at least ten persons constantly involved in the automated processing of data. On premise, a data protection officer must then be appointed [57]. This is likely to be the case for many mid-sized companies. Companies affected by this system must have already taken appropriate measures. Even for the data protection officers already employed by the company, GDPR represented a significant change. This is because their role in the company has changed drastically. If the data protection

officer has worked on data protection compliance previously, he or she will be responsible for monitoring the actions that have been carried out. This has led to an increase in their scope of responsibility and, thus, an increase in their ability to take responsibility. Indeed, the implementation of data protection regulations, such as the GDPR, has had an impact on the workload and responsibilities of data protection officers (DPOs) but has also brought positive aspects. Their expertise is in high demand, and their position within organizations has been strengthened, reflecting the growing recognition of the importance of data protection and privacy in today's digital landscape. Article 39 of the GDPR refers to the duties of the DPOs. Since the implementation of data protection laws, significant changes have occurred, particularly in the areas of online commerce and employee data protection. These laws aim to strike a balance between protecting individuals' rights and facilitating the beneficial uses of artificial intelligence and big data [31][58].

The GDPR includes several key measures that companies, particularly those operating in the field of online commerce, must adhere to. Here are some of the important measures:

1. Data Protection Impact Assessments (DPIAs): Companies must conduct DPIAs for processing activities that are likely to result in high risks to individuals' rights and freedoms. DPIAs help identify and minimize privacy risks by assessing the necessity, proportionality, and safeguards associated with data processing activities.

2. Data Subject Rights: GDPR grants individuals certain rights over their personal data. Companies must ensure that individuals can exercise these rights, such as the right to access their data, the right to rectify inaccuracies, the right to erasure (or "right to be forgotten"), the right to data portability, and the right to object to processing

3. Security and Data Protection Measures: Companies are obligated to implement appropriate technical and organizational measures to ensure the security and protection of personal data. This includes measures such as

encryption, pseudonymization, regular data backups, access controls, and staff training to prevent unauthorized access, loss, or alteration of data

4. Data Protection Officer (DPO): Some companies may be required to appoint a DPO, who is responsible for overseeing data protection activities, providing advice, and acting as a point of contact for individuals and supervisory authorities [31][59].

These are just a few of the key measures outlined in the GDPR. It is important for companies to familiarize themselves with the full requirements of the regulation and ensure compliance to protect individuals' privacy rights and avoid potential penalties for non-compliance.

2.9 The Risks of Artificial Intelligence that Threaten Privacy

AI can be a beneficial force; it is essential to approach its implementation with careful consideration of its implications for human rights. Balancing the potential benefits with ethical considerations is crucial to ensure that AI serves the greater good and avoids negative outcomes. Bridging the huge gap in accountability for how data is collected, stored, shared, and used remains one of the most pressing human issues. Given the rapid and continuous growth of artificial intelligence. The conclusions, predictions, and observations made by AI tools, including the search for explanations about patterns of human behavior, raise serious questions. The biased data sets on which AI systems rely may lead to discriminatory decisions, and already marginalized groups remain more vulnerable to this type of risk. The risk of discrimination associated with AI-driven decisions that may change, limit, or harm human lives is real. "It is therefore absolutely necessary that we systematically assess and monitor the impact of AI systems in order to determine threats to human rights and to mitigate them" [1]. It is also necessary for companies and countries to express more transparency about how they develop and use artificial intelligence because we cannot keep pace with its super-fast pace and must allow its use within certain limits, with limited or no control, and then deal with the inevitable consequences for human rights after the fact.

In summary, the potential of AI to benefit society is undeniable, but it also has the potential to enable widespread human rights violations if left unchecked. Therefore, it is crucial to implement measures that safeguard human rights when using AI. This is necessary to ensure the responsible and ethical use of AI, ultimately benefiting everyone in society. [1][43].

Chapter Three

Legislative Framework Related to Artificial Intelligence and Data Protection

The work in this chapter aims to analyze the legal status of the related issues of artificial intelligence and data protection and their own regulations. The "privacy" of artificial intelligence systems represents the main point in urging jurisprudence, the judiciary, and the legislator to develop rules of responsibility, especially after artificial intelligence systems have become one of the necessities of modern life due to their self-management capabilities and interaction with their external environment [32][60]. Undoubtedly, the technological development in the field of artificial intelligence systems has had its impact on human behavior, which prompts us to analyze the legal problems resulting from these actions, including the extent to which liability and legal provisions can be applied to artificial intelligence and finding out who bears legal responsibility for the actions of the AI [2]. On April 21, 2021, the European Commission submitted a proposal for a European Parliament regulation that sets harmonized rules on AI law. It can be considered a real step in finding legal solutions in the field of artificial intelligence. It will closely affect businesses, organizations, customers, and governments working in the field of AI when regulation comes into force, such as the General Data Protection Regulation (EU) 2016/679 of the European Parliament and Council on April 27, 2016, which became effective in the European Union in May 2018. AI Studies is making the necessary legal arrangements.

To prepare for the social and economic impacts of AI. In fact, the explanatory note on the proposal to regulate artificial intelligence prepared by the European Commission states that it will have many benefits in terms of industry and social activities, and it will also contribute to the European economy. It was indicated that it would provide a competitive advantage in areas such as health, the public sector, finance, and agriculture. In addition, he stated that the social and economic effects of artificial intelligence may have new risks and negative consequences for individuals and society. In the explanatory memorandum, attention was drawn to

the importance of enabling Europeans to benefit from new technologies with artificial intelligence that are developed and operated in accordance with the basic values, rights, and principles of the Union [43][61]. European AI regulation includes harmonized rules and controls around AI, specifying that regulations are evolving rapidly, and so the EU is determined to take a balanced approach to maintaining the Union's technological leadership and ensuring that Europeans respect the Union's core rights and values. We can analyze the proposed European regulatory framework for AI with several points:

First: Its Objectives

1. Ensure the safety and compliance of AI systems that are used in the EU market. This entails making sure that these systems adhere to existing laws, uphold fundamental rights, and align with the values upheld by the EU.
2. Provide a legal framework that offers certainty and clarity to foster investment and encourage innovation in the field of AI.
3. Strengthen governance and enforce existing laws pertaining to fundamental rights and safety requirements in relation to AI systems.
4. foster the development of a unified market for legitimate, safe, and reliable AI applications while preventing fragmentation of the market. The aim is to create a seamless and cohesive market that encourages the adoption and utilization of trustworthy AI applications, promoting innovation and economic growth in the AI sector.

Second: Regulation Titles and Chapters

1. General provisions.
2. Prohibited AI practices.
3. High-risk artificial intelligence systems, the aim is to ensure that high-risk AI systems are subject to specific rules and procedures to minimize potential risks and ensure compliance with regulatory standards. It covers various aspects related to these systems, including their classification, requirements, and obligations for providers and users.
4. Transparency obligations of specific AI systems.
5. Miscellaneous in supporting innovation.

6. Governance, which includes the following chapters: European Artificial Intelligence Council; Competent National Authorities.
7. The European Union database of stand-alone and high-risk artificial intelligence systems.
8. Monitoring and supervising the market and sharing information, which included the following chapters: subsequent market monitoring, exchange of information on accidents and poor performance, and access.
9. Code of conduct.
10. Confidentiality and penalties.
11. Delegation of powers and procedures of the committee.
12. Final Provisions - Accessories.

On February 19, 2020, the European Commission published the White Paper on This document sets out the policy that must be followed to support work in the field of artificial intelligence and to address the risks that may arise from the use of this technology. In this regard, it is emphasized that the legal proposal is a text about drawing up the necessary legal framework for a reliable artificial intelligence [62]. The regulation proposal includes:

- Definition of artificial intelligence system. According to the regulation proposal in Article 3.1, An artificial intelligence system refers to a software program that has been created using specific techniques and methods outlined in Appendix I. This program has the ability to generate output, such as content, predictions, suggestions, or decisions that impact the environments in which people interact. These AI systems are designed with specific purposes defined by humans and serve various functions within those defined contexts.

  Looking at Appendix I, the techniques mentioned in the article are as follows:

  a) Machine learning approaches, it encompasses various approaches and methods, including deep learning, to enable models to learn and make accurate predictions.
  b) Logical and knowledge-based approaches in AI encompass various techniques and tools aimed at representing and utilizing knowledge effectively. These include methods for programming based on logical

induction, maintaining knowledge bases, performing inference and deduction, employing symbolic reasoning, and utilizing expert systems for specialized domain knowledge.

c) The legal proposal defines an artificial intelligence system as incorporating statistical approaches, Bayesian estimation, and research and optimization methods. This definition is comprehensive and reflects a thoughtful approach, taking into account the anticipated advancements in AI technology that will occur incrementally over time [43][63].

- Subjects regulated by the regulation proposal when the by-law proposal is examined, it is seen that the issues regulated by the by-law are specified in the first article are related to the following:
  a) Establishing harmonized rules for the placing on the market, putting into service, and use of artificial intelligence systems within the EU, including
  b) Banning certain AI applications.
  c) High-risk AI systems are subject to specific requirements, and operators of such systems bear certain obligations.
  d) Harmonized transparency rules are implemented to promote uniformity in how artificial intelligence systems are required to disclose information and operate transparently.
  e) Emotion recognition systems and biometric classification and categorization systems are intended to interact with natural persons.
  f) “Market monitoring and surveillance rules for AI systems", looking at the issues regulated by the by-law proposal, it is seen that there is an arrangement on the horizontal axis regarding artificial intelligence systems. The regulation is aimed at those who supply artificial intelligence systems to the market, system operators, and those who monitor the market [2][43].
- The EU proposal on AI oversight contains a risk-based approach. the most serious is an unacceptable risk (prohibited). Accordingly, a distinction is made between AI that presents unacceptable risks, high risks, limited risks, and low risks. Prohibited types of AI are regulated in Title II of the Unacceptably Risky AI Regulations Proposal. Accordingly, the use of these systems is prohibited. This regulation aims to prohibit the use of AI systems that are contrary to the

values of the Union, such as AI systems that violate fundamental rights. Such as those that cause harm to rights and safety by manipulating the use of artificial intelligence technologies and systems in accordance with Article 5(a) of the EU proposal that The use of applications of artificial intelligence systems that cause them to act in a manner likely to harm natural persons Therefore, in paragraph (b) of Article 5, it is prohibited to use applications of artificial intelligence to exploit persons belonging to vulnerable groups, such as children or persons with disabilities, in a way that causes or is likely to cause physical or mental harm to themselves or others. In paragraph (c) of Article 5, public authorities are prohibited from using artificial intelligence for social assessment based on an assessment of the behavior or social characteristics of people. Paragraph (d) of the article prohibits the use of real-time remote biometric recognition systems for law enforcement in public places, with some limited exceptions [43].

3.1 Organization of the topic

The decree focuses on regulating the introduction and utilization of artificial intelligence systems in the market. According to Article 3's legal definition, humans are considered identifiable when they are capable of generating outcomes such as content, predictions, recommendations, or decisions that impact the environment in which they operate. This definition encompasses AI systems that operate independently. In Appendix 1, product-related technologies and concepts includes:

- Machine learning concepts
- Logical and cognitive concepts as well
- Statistical approaches.

The definition in Article 3 only partially satisfies the requirements of a clear and legally secure definition 0[64]. Content creation, predictions, recommendations, or decisions do not describe features specific to artificial intelligence but rather characteristics of software in general. The first supplement limits the scope only marginally. Here too, the terms "logic and knowledge-based concepts" and "statistical approaches" are shown to be very broad. In the end, all types of

algorithmic decision-making and recommendation systems can be classified as artificial intelligence systems [65].

However, it became clear that the definition would be tightened in the ongoing legislative process. It should also be noted that the list of technologies and concepts in Appendix I can be extended by the European Union Commission through delegated legal procedures (Article 73).

3.2 Principles of Data Protection Law

AI technologies heavily rely on personal data, but they also have the potential to influence the privacy of individuals. The collection of data necessary for AI's big data requirements can have implications for privacy, which is a crucial consideration. Chapter 2 of the GDPR establishes a foundation based on well-established privacy principles, including legality, transparency, integrity, and confidentiality. The GDPR establishes a framework that reinforces privacy and security requirements, including transparent data practices, robust security measures, and mechanisms to facilitate the transfer of data across borders while upholding privacy principles [66]. In order these regulations introduce new privacy principles, such as accountability and data minimization, which are consistently emphasized throughout the legislation. Various requirements within the text highlight the importance of these principles in safeguarding privacy and adapting to the data-driven environment, including the following requirements:

1. Data security: This involves implementing strong security measures, both in terms of technological solutions and organizational practices. The aim is to protect data from unauthorized access, minimize the chances of data loss, and prevent unauthorized processing or leakage of sensitive information as GDPR recommended.
2. Expanded rights for individuals: These rights aim to enhance individuals' control and privacy over their personal information in the digital age.
3. Data breach notification: This aims to ensure transparency and enable individuals to take necessary measures to protect their personal data and mitigate potential harms resulting from the breach.

4. These aims to evaluate the performance of existing security measures and identify any areas that require improvement. By conducting these audits and making necessary enhancements, companies can continuously strengthen their security measures and ensure the protection of personal data in compliance with GDPR requirements. [31][66].

With GDPR, europe is emphasizing its strong position on data privacy and security, recognizing the growing reliance on cloud services and the rising occurrence of data breaches. This commitment underscores the importance of protecting personal data in an environment where its vulnerability is prevalent. The regulation itself is large, far-reaching, and very subtle, which makes GDPR compliance intimidating, especially for small businesses.

GDPR defines several legal concepts in detail. Here are some of the most important concepts [67]:

- Personal Data: refers to any information that can be used to directly or indirectly identify an individual. Common examples of personal data include names and email addresses. However, personal data extends beyond these obvious identifiers. It can include location information, race, gender, biometric data, religious beliefs, web cookies, and political opinions..
- Data processing: Any process that takes place on the data, whether it is automatic or manual, Examples given in the text include collecting, saving, editing, creating, storing, using, deleting, etc.
- Data subject: This term typically includes customers or visitors who provide their personal data for various purposes to websites.
- Data controller: is the person or entity that has the authority and responsibility to decide why and how personal data is processed within an organization.
- Data Processor: A third party to process personal data only as instructed by the data controller, maintain confidentiality and security of the data, and assist the data controller in meeting their legal obligations related to data protection [31].

3.2.1 Evaluate the Impact of Data Protection in the Business

Data protection is an important aspect when using AI systems. Legal safeguards limiting the use of AI and deep learning [68] can Regulations of the General Data Protection Regulation apply to the use of artificial intelligence. In the event of data processing in the course of work, it must be done in accordance with the GDPR, and the principles of protection and accountability set out in Article 5. Legality, fairness, and transparency: processing must be lawful, fair, and transparent to the data subjected to it, as well as legal in accordance with Article 6 of the (GDPR). Special consideration is given to AI needs and automated processing processes (Article 22 of the General Data Protection Regulation) [31]. This is important to:

1. Identification of purposes: Data must be processed for the legitimate purposes.
2. Data minimization: Only as much data as possible should be collected and processed for the intended purposes.
3. Accuracy: Personal data must remain accurate and up to date.
4. Storage Limitations: Personally identifiable data should be retained only for as long as necessary for the intended purpose.
5. Integrity and confidentiality: processing must be carried out in a way that ensures appropriate security, integrity, and confidentiality.
6. Accountability: The data controller is responsible for demonstrating compliance with all principles of the GDPR.

The GDPR says that data controllers must be able to demonstrate that they comply with the GDPR. Among the ways to do this:

- Assign data protection responsibilities to the team.
- How the data is collected, how it is used, where it is stored, the employee responsible for it, etc. And maintain detailed documentation.
- Training cadres and implementing technical and organizational security measures.
- Sign data processing agreements with third parties contracted for data processing.

7. The data shall be processed securely by applying "appropriate technical and organizational measures". Technical measures range from requiring employees to use two-factor authentication on accounts where personal data is stored like training employees, adding a data privacy policy to an employee handbook, or restricting access to personal data to only employees in the organization who need it. If there is a data breach, data subjects have 72 hours to report it or be punished. (This notification obligation can be waived if technological security measures such as encryption are used to render the data useless to an attacker.)
8. In (Proposed regulation, Article 17) regulations AI The quality management system will be updated throughout the life of the system. It involves establishing a documented risk management system and organizing data management procedures, including data collection, analysis, tagging, storage, filtering, mining, aggregation, retention, and any other data-related operations that take place prior to market placement, or commissioning of high-level AI systems Risks.
9. Users of high-risk AI systems use the information provided pursuant to Article 13 of the Regulation of AI, which includes harmonized rules to comply with the obligation to conduct an impact assessment on data protection.
10. Permission to process data in Article 6 of the GDPR lists the cases in which the processing of personal data is lawful. It should not even be considered to touch someone's personal data unless it is justified by one of the following: the data subject has given specific and explicit consent to the processing of the data [69].

3.2.2 The Relationship Between Artificial Intelligence Law and GDPR

The particular interest of the legal analysis lies in Article 22 of the GDPR, which specifies that a person should not be subject to a purely automated decision. This GDPR art is the only one specifically geared toward artificial intelligence [31].

GDPR is generally applied equally in all EU member states. It aims to create greater transparency and self-determination regarding personal data. In addition, the

regulation aims to create consumer confidence in digital operations and contribute to the harmonization of previous national data protection laws [70].

GDPR supersedes implementations of the data protection directive to all companies that process the personal data of employees. The definition of data processing remained unchanged during the reform. Accordingly, even delivery services that process customer data are affected by the new obligations. For example, there are more stringent requirements for consent to data processing, documentation requirements, and information requirements. In addition, workers' rights were strengthened, and, for example, the right to "data portability" was introduced. Processors are also covered by new liabilities. All of this requires taking appropriate precautions to comply with the requirements of the GDPR [59]. By supervisory authorities Since companies have to deal with all kinds of When there are disruptions to AI systems at work, it is necessary to prioritize appropriate measures. The focus should be on the following action:

1. Creation of records of processing activities (Article 30 GDPR).
2. Take technical and organizational measures to secure data processing (Article 32 of the GDPR).
3. GDPR-compliant contractual obligations and cooperation with request processing service providers (Article 28 GDPR) Among the most important.

Topics that can be addressed are critical issues such as:

1. Legality of data processing (justification for data processing in Article 6 of the GDPR).in Article 6 of the GDPR (General Data Protection Regulation) outlines the legal basis for processing personal data.
2. Processing of genetic, biometric, or health data (Article 9 GDPR) AI systems process large amounts of personal data, such as biometric data, health data, and location data. Under Article 9 GDPR, AI systems are classified sets out special categories of personal data which are considered particularly sensitive, such as data concerning an individual's racial or ethnic origin, political opinions, religious beliefs, genetic or biometric data, and data concerning an individual's health or sex life or sexual orientation. Processing

of these sensitive categories of data is subject to strict conditions and additional safeguards to protect the rights and freedoms of individuals.

3. Personal data of employees in Article 88 of the GDPR EU establishes the principles for the processing of personal data in an employment context. It provides guidance on how employers should handle personal data, including sensitive data, of their employees and job applicants, and how they should balance their interests in collecting and processing such data against the rights of the individuals concerned.
4. AI and GDPR require cooperation between stakeholders: AI developers, regulatory bodies, and individuals must work together to ensure that AI systems are developed and implemented in accordance with GDPR principles. This requires transparency, collaboration, and active participation from all stakeholders.

Overall, AI law and GDPR are closely intertwined, and AI developers must comply with GDPR requirements to avoid legal repercussions and ensure the protection of individual privacy rights.

3.3 Regulation Proposal Approach

The focus of the proposal for EU regulation of high-risk AI systems. This is what was stated in Part III under this heading for high-risk artificial intelligence systems About applications, products, and in sectors that pose a great risk to health, safety, and basic rights, and the rules for artificial intelligence systems are regulated by Article 43 (conformity assessment, which states in the case of high-risk artificial intelligence systems must Harmonized standards are applied by demonstrating compliance with the reason for the stipulated requirements (and Article 6, Article 7).

The conditions contained in subparagraphs (a) and (b) of Article 6 (1) of the implementing regulations of the proposal

High-risk AI systems are rated High Risk. In accordance with paragraph (1) of Article 6, regardless of whether the AI system is placed on the market or brought into service independently of the products specified in subparagraphs (a) and (b), and both conditions specified in subparagraphs (a) and (b) if they occur, the AI in

question would be considered high risk. They are: a) the AI system is intended to be used as a security component of a product covered by the ITU Harmonization Legislation listed in Annex II, or the AI system itself is such a product, and b) a product with artificial intelligence as the security component or the product itself, which must pass a conformity assessment by a third party in order to be placed on the market or put into service in accordance with the union coordination legislation listed in Appendix II.

In addition, the AI systems defined in Annex III are also high risk as we can see in Proposal for Regulation, Article 62 The proposal to regulate AI will be applied to all AI systems. However, the provisions relating to high-risk AI systems under Title III will only apply to AI systems in two subcategories [43]. The AI systems that make up these categories are expressed in two groups. In the first group, those who are identified in the second appendix are currently.

Products like medical devices are subject to the health and safety compliance legislation of the European Union. This legislation sets forth regulatory requirements and standards to ensure the safety and effectiveness of such products [28]. In the second group, there are stand-alone AI systems utilized in the eight domains outlined in Appendix III. These domains encompass specific areas where artificial intelligence is employed as an independent system. As specified in Annex III of the proposed regulations, the areas covered include: biometric recognition and classification; management and operation of critical infrastructure, training, and vocational training; Employment and management of workers, access to self-employment, access to the enjoyment of basic services and facilities [71]. Article 7 of the proposed system underscores the significance of understanding the purpose, extent, and potential health-related harm associated with the use of an artificial intelligence system. It aims to ensure that the deployment of AI systems is done with careful consideration of these factors and that appropriate measures are taken to mitigate any potential risks to health [43].

The regulation of AI at work aims to create a harmonized and secure market for AI systems in the workplace that aligns with the values and legal framework of the EU, while prioritizing the protection and welfare of individuals. Organizing proposal aims

to create a harmonized framework for AI system regulation in the EU. By applying the regulation across all sectors and adopting a risk-based approach, it ensures effective governance, minimizes risks and promotes the responsible development and use of AI systems within the EU.

The AI Act adopts a risk-based framework that categorizes AI systems into four levels: unacceptable risk, high risk, limited risk, and minimal or no risk. AI systems with the potential for significant harm to individuals would be strictly prohibited, ensuring their safety. The following AI systems would not be allowed to be placed on the market, put into service, or used: So, they are classified by risk, with the Critical Pyramid as mentioned in Figure 1: a risk-based approach where any system deemed to be a clear threat to the EU will be banned based on a social assessment conducted by the AI monitoring committee [43].

1. Unacceptable Risks (Forbidden): Due to the violation of fundamental rights, the use of artificial intelligence that is contrary to the values of the European Union and a very limited number of particularly harmful AI will be prohibited. As an example of those, real-time remote identification systems can be given in public areas used for social assessment by governments, the use of subliminal technologies, and law enforcement, and the systems must comply with additional safeguards such as necessity, proportionality, and prior authorization from a judicial or administrative authority. independent (Articles 5.2, 5.4) of the proposed AI regulation. It must be emphasized that the ban on the use of real-time remote identification systems will explicitly include the use of facial recognition technology in public places. The rationale for banning these AI systems supports core values such as equality, human rights, and safety.

   The regulation sets limitations on the utilization of AI systems and products that go against the values of the European Union (EU) and the basic rights of individuals. It explicitly forbids the application of AI in certain services, which are as follows:

   - Distorting and manipulating human behavior by leveraging the subconscious mind. It specifically targets methods that can potentially cause harm or violate human rights in the process.

- Prohibits the use of systems that may harm individuals based on factors such as age, physical or mental disability, and other characteristics. It specifically addresses the assessment and discrimination of individuals based on their social behavior, race, or gender. The intention is to prevent any adverse effects or discrimination caused by such systems.

2. High Risk: The restrictions on artificial intelligence systems specified in the draft regulations have a negative impact on people's safety or their basic rights, and these systems are considered high-risk. Essentially, the draft regulation does not provide for an absolute ban on high-risk AI systems. However, a few guiding requirements have been proposed for AI systems classified as high-risk. to these requirements, examples can be given of data management, record keeping, transparency, provision of information to users, human monitoring, cybersecurity, and conformity assessment procedures. High-stakes AI systems are subject to mandatory requirements to ensure their responsible and safe deployment. These requirements encompass various aspects including quality of datasets, technical documentation and record-keeping, transparency and provision of information to users, human supervision, robustness, accuracy, and cybersecurity. these mandatory requirements aim to establish a framework that ensures the reliability, transparency, and accountability of high-stakes ai systems. In addition (Articles 8 to 15) aims to regulate conformity assessment, means process involves evaluating the AI system's compliance with the applicable regulations, technical requirements, and performance criteria. This assessment is typically conducted by a designated conformity assessment body or a competent authority. Article 19 aims to ensure that high-risk AI systems are thoroughly evaluated for their compliance and adherence to regulatory requirements. This helps mitigate potential risks, ensures the safety and reliability of the systems, and promotes accountability and transparency in the development and deployment of high-risk AI technologies. AI systems used for recruitment, worker management, and access to self-employment, especially for employee recruitment and selection, should also be considered high-risk for making decisions about the promotion and termination of contracts, assigning tasks, monitoring, or

evaluating people in contractual relationships of a functional nature, as they can significantly affect the future employment prospects and livelihoods of these people. Contractual relationships of a functional nature must include employees and persons providing services through the platforms, as set out in the Commission's 2021 work program [43]. Some examples include:

- Critical infrastructure that could endanger the life and health of citizens, such as transportation Educational or vocational training, which may determine a person's access to education and career path (for example, test dates and student grades)
- Safety components of the product (for example, the application of artificial intelligence in healthcare, such as performing robot-assisted surgeries) Recruitment, employee evaluation, business administration, and approval (e.g., resume editing programs and evaluation of recruitment procedures)
- Basic services for individuals, private and public (such as a credit rating that may deprive a citizen of the opportunity to obtain a loan). Compliance with the law that may interfere with individuals' fundamental rights (for example, assessing the reliability of evidence)
- Also manage immigration, asylum, and border controls, which are extremely important (e.g., validation of travel documents).
- Public and private surveillance systems (e.g., biometric surveillance for law enforcement, facial recognition systems, as well as video cameras for surveillance in public places) [63].

3. Limited Risk: AI systems with some transparency obligations cover situations where the risk of tampering is obvious. For example, when using AI systems such as chatbots, users must be aware that they are interacting with a device. Thus, they will have the opportunity to make a conscious decision to follow through or back out. AI systems are subject to minimal transparency obligations, which are intended to allow people who interact with these systems to make informed decisions. The user then has the right to decide to continue or withdraw from using the application, as in (Article 52). Providers of non-high-risk AI systems are also encouraged to adopt the Code of Conduct

and to voluntarily apply the mandatory requirements for high-risk AI systems as in (Article 69), which states Compliance of AI systems other than high-risk systems, based on specifications and technical solutions that are appropriate means of ensuring compliance with those requirements considering the intended purpose of the systems.

4. Minimum Risk: All other artificial intelligence systems can be developed and used subject to current legislation without additional legal obligations. It was possible to say that most artificial intelligence systems currently used in the EU fall into this category. Most artificial intelligence systems also essentially fall into this category. The Draft Regulation does not interfere in this area, as these artificial intelligence systems represent only a minimal or no risk to the rights or safety of citizens [43][63].

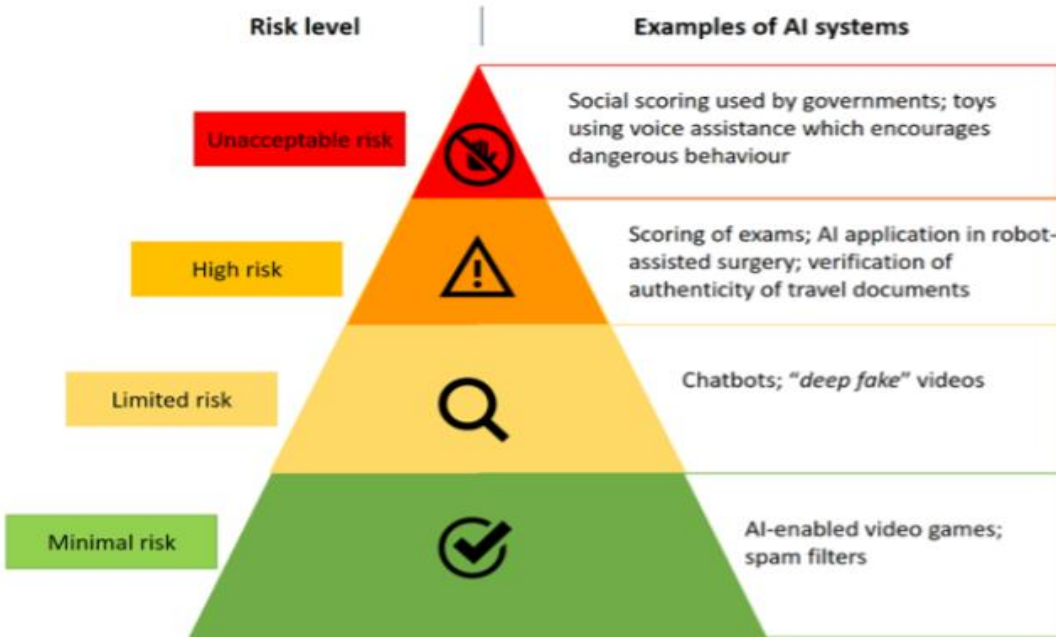

Figure 1: The Criticality Pyramid for AI Systems risk-based approach [63].

3.3.1 High Stakes AI Systems Requirements

Once an AI system is classified as high-risk, it must meet a number of requirements:

1. A risk management system should be established to ensure that risk assessment and control measures are taken throughout the life cycle of the AI system.

2. High requirements on data quality: data used in learning ("machine learning") processes must be relevant, representative, error-free, and complete. Datasets must "appropriately" meet the requirements. We can see this in Article 8 Supplementing Requirements for High-Risk AI Systems, Harmonized Rules for the Introduction, Operation, and Use of AI Systems, Specific Requirements for High-Risk AI Systems for These Standards, Compliance Rules for AI Systems for Interaction with Systems, and Criteria for Determining the Natural Persons Intelligence Systems. Use synthetic and dynamic methods to create image, audio, and video content, market control rules, and monitoring rules. The intended purpose of the High-Risk AI and Risk Management System is indicated in Article 9, which states that the Risk Management System shall be established, and we will use, implement, test, document, and maintain the system in relation to High Risk. The risk management system must have a continuous iterative process that runs throughout the entire risk information cycle, is monitored, and tested, and requires regular systematic updating. To achieve this, we will identify and analyze existing and potential risks, and estimate and assess the risks that may arise when using a high-risk AI system according to its intended purpose and under conditions of misuse; additional assessment of potential risks based on the analysis of data collected from the post-market monitoring system referred to in Article 61, "which provides for post-market monitoring by service providers and a plan for monitoring high-risk post-marketing products, such as artificial intelligence systems.
3. The regulations address the risks of discrimination by AI systems. Unrepresentative datasets can lead to an unconscious distortion of results ("bias"), which is difficult to recognize without careful documentation of the data used. In order to recognize and avoid such bias, the regulation gives providers of artificial intelligence systems an exception to a core area prohibited in the GDPR: they have the option of using personal data for these purposes, which reveals a person's ethnic or sexual origin. Orientation, for example, in Articles 14.4 and 14.3, these measures allow persons in charge of human control to be able, depending on the circumstances:

   The observer must know the capabilities and limitations of a high-risk AI system, properly monitors its operation, and is able to detect and remediate

unexpected malfunctions and behaviors as quickly as possible before harm is inflicted. The controller is aware of the information and output generated by a high-risk AI system ("automation bias"), particularly with those systems that are used to provide information or recommendations for the purpose of helping a natural person make a decision.

1. Comprehensive technical documentation showing that the AI system meets the requirements for high-risk systems, as well as an operating record throughout the life of the AI system.
2. Transparency: Users must be given a set of clearly defined information about the system and the provider.
3. High-risk AI systems must also meet and maintain a "reasonable" level of accuracy, robustness, and cybersecurity.

3.3.2 Compliance with the Requirements of the Regulations

To ensure compliance with the requirements of the regulations, technical documentation must also be created (Article 11). The technical documentation serves as a comprehensive record that provides insights into the design, functionality, and development of the AI system. It should encompass information about the system's architecture, algorithms used, data processing methods, and any relevant parameters or configurations. High-stakes AI systems must also be designed and developed to allow comprehensive logging of processes and events. According to Section 12.1, high-risk AI systems must be designed and developed with event logging capabilities. Logging must "conform to recognized standards. The logging obligation aims to ensure that the performance of an AI system can be traced over its entire lifecycle [37]. For reasons of transparency, traceability of AI decisions, and a commitment to rights and safety. However, if personal data is processed in this process, it may lead to conflicts with data protection regulations. The recording and permanent storage of processes and events is contrary to the normative principle of data protection regulation (GDPR) in Article 5.1(c) Design compliant with data protection will require Data for the commitment of recording later a great deal of effort. As an additional requirement for transparency, Article 13.1 states that high-risk AI systems are designed and developed in such a way that their operation

is sufficiently transparent so that users can appropriately interpret and use the results of the system. Artificial intelligence from fulfilling their obligations under Article 29. The obligation to be transparent aims to ensure that the artificial intelligence system can also be used by the user in a legally compliant manner. In addition, high-risk AI systems must be provided with instructions for use containing accurate, complete, and correct information. and clear information (13.2). In this context, information on the intended purpose is required. In order to minimize risks, AI systems must also be designed and developed in accordance with Article 14.1 so that they can be effectively monitored and controlled by humans. Appropriate intervention mechanisms must be included in AI System for Regulatory Compliance Practice 13.3. Finally, as an additional requirement, Article 15 defines the accuracy, robustness, and cybersecurity of high-risk AI systems. This is to ensure that high-risk AI systems have sufficient resilience in the event of errors, disturbances, or unforeseen situations, but also that in the event of harmful interference, appropriate measures are taken to reduce the risk [63].

3.3.3 Legal Challenges to High Stakes AI Systems Decisions

The legal decisions found to identify and protect fundamental rights at work, where providers and suppliers of high-risk AI systems should establish a quality management system as described in Proposed Regulations for AI Systems Article 17. According to the proposal of the Rules, the quality management system includes the establishment of a documented risk management system that will be updated throughout the life of the system. According to the proposal of the same regulation, Article 9, it is necessary to establish, document, and maintain the risk management system, including the identification and assessment of risks. The title of the article is "Management System Risks." The risk management system should ensure that risks are eliminated or minimized through appropriate design and development.

And using high-quality datasets. In this regard, the title of Article 10 is "Data and Data Management". High-quality, validated, and tested datasets should be used in training AI systems [43][72].

An important condition for high-risk AI systems is the creation of technical documents showing the extent to which the AI system complies with the proposal of the European Union, as in the title of Article 11 in relation to this issue is “Technical Documents and Documents”. These documents indicate the compliance of the AI system of national authorities or authorized institutions with this regulatory proposal. It should contain the necessary information about the audit (proposed regulation, Article 11.1).

The use of sensitive personal data is permitted to the extent that monitoring is necessary to detect and correct bias (Regulation Proposal Article 10.5). The use of ethnicity data or similarly sensitive data is prohibited in the GDPR, except in cases specified in Article 9 in terms of the GDPR, where there is no exception for EU-wide detection of bias in terms of the GDPR. However, the law of artificial intelligence.

There is an exception to the proposal. This exception can only be used in connection with high-risk AI systems and by the providers and suppliers of such systems. Providers and suppliers of non-hazardous AI systems will not be able to afford this exception. This exception is for those who collect sensitive data and provide high-risk AI systems. It does not constitute a means of guaranteeing its sale to individuals [2].

High-risk AI systems must "keep records," as stated in the title of Article 12 of the proposal. Accordingly, enabling high-risk AI systems to automatically record events and logs while the system is running is "transparency and provision of information to users," as stated in the title of Article 13 of the bylaw proposal. By prioritizing transparency, high-stakes AI systems can effectively serve their intended purpose, empower users, and ensure that the technology is used in a responsible and trustworthy manner. [73].

High-risk AI systems should be subject to "human observation," as stated in the title of Article 14 of the proposal. This type of AI system has mechanisms in place that allow human experts to observe and review their operations, outputs, and decision-making processes. authorized during the period of use of the system. According to the situation and its severity, the authorized persons must fully know the capabilities and limitations of the high-risk AI system and be able to monitor its operation

efficiently within the limits of the plan and the measures that will be taken for this monitoring [20].

It is also necessary for authorized persons to have the authority to disable or mechanically operate an automated system or to interfere with the system (Regulation Proposal, Article 14.4) and in terms of cybersecurity "Article 15.1 of the Regulation proposal specifies that high-risk AI systems must be developed and designed to ensure accuracy durability and cyber security, given the desired end, so the system must work continuously in these areas throughout its life [31][43].

3.4 Legal Obligations of Providers and Users of High-Risk AI Systems

Dealing with natural persons in accordance with Article 52.1 of the legal proposal, which are the transparency obligations of some artificial intelligence systems, aims to ensure that artificial intelligence systems are designed and developed in a way that informs natural persons that they are interacting with an AI system that is clear to use, but this obligation does not apply. On AI systems permitted by law for the purposes of detecting, preventing, investigating, or prosecuting criminal offenses an example of an AI system (such as Chatbot) whose traffic is intended to interact with intelligent programs such as a bot that needs to explain instructions and requirements for the product and its method of use [26].

In accordance with Article 5 of the GDPR, which indicates good faith, transparency, and the lawfulness of data processing when using these systems. That the basic obligations of users there is a definition of the user in Article 3.4 of the Proposal Regulations. Accordingly, user means any natural person, public agency, organization, or company that uses an artificial intelligence system under its authority, except when it is used in the context of a personal, non-professional activity. The term user in public institutions using the artificial intelligence system includes those who use the system for professional purposes in accordance with the proposal of the regulation, and users who use the system for non-professional personal activities not related to work are also considered to be within the scope of the regulation (Article 65.1). here Users are obligated to stop the system in any sudden situation or during suspension if the user believes that the use is dangerous.

Users of high-risk AI systems shall automatically retain records generated by the system to the extent such records are under their control, which will be stored for an appropriate period until the purpose of using the risky AI system is achieved and the applicable regulations under Union law (the proposed regulation, Article 29.5, or pursuant to Article 27 of the RGDP Regulation, which stipulates several statutes are required to perform a data protection impact assessment), For fair results, however, it must be noted that even if the same datasets are used, different results may occur depending on the modeling technique used. It should be noted that while incorporating new datasets into the decision-making processes of AI systems, users are also required to monitor the fairness of the model so that biases do not emerge while processing personal data that reveal ethnicity. ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data relating to health, and data relating to a natural person's sexual activity or sexual orientation are prohibited [6][20].

3.4.1 Rules Regarding the Use of Personal Data

The GDPR governs the use of personal data and establishes rules and guidelines for its processing. One of the fundamental principles of the GDPR is that there must be a lawful basis for processing personal data before it can be collected or used. In principle, it is not processed for any purpose other than that for which it was collected, and it must be processed in a very specific and transparent manner. The rights and obligations of data subjects whose personal data are processed by those responsible for processing under the GDPR can still be associated with individuals; training data can also be classified as "personal data", and data subjects have different rights regarding Using this data for the benefit of the algorithm, the algorithm can make decisions about a particular person. His personal data will then be 'tested' by the algorithm, and the GDPR will be applied. The GDPR states that data subjects must always be informed of such use.

3.5 Transparency Obligations for AI Systems

Transparency obligations are imposed on AI systems with identified risks of tampering, regardless of whether they are classified as high risk. According to Article 52.1, natural persons must be informed that they are dealing with an artificial intelligence system, unless it is clear from the circumstances and context of use. In the future, the use of chatbots will be associated with an obligation to report. There is also a notification obligation for users of emotion recognition software or biometric classification systems (Article 52.2) [74]. In addition, the regulation requires that AI systems that generate or manipulate image, audio, or video content of individuals, objects, places, or events must be flagged. This means that these AI systems must incorporate labels or indicators to indicate that the content has been artificially generated or manipulated. This type of AI system is capable of altering images, videos, or audio recordings so that they are difficult to distinguish from the original content [43][63].

Chapter 4

The Practical Case

The AI regulations place emphasis on excellence and trust. They strive to foster improvements in the work environment, research, and manufacturing sectors while safeguarding the fundamental rights and freedoms of workers engaged in AI systems. Furthermore, these regulations seek to leverage artificial intelligence in various technical, economic, and legal contexts. The focus of this chapter is on understanding how AI affects job-related functions such as recruitment, bias management, and Human Resources (HR's) utilization of AI systems for candidate assessment. Moreover, exploring the implications of identifying and addressing synthetic content, including deepfakes, in different forms of media. Also, analyzed the specific obligations of users and providers of AI systems, where service providers must provide compliance audits that must be performed before AI systems are put into operation or brought to market and organize oversight and enforcement of applications.

4.1 The Impact of Artificial Intelligence Systems on Employment and Work

Human resources in a company's value chain always carry a certain risk due to the unpredictability of human behavior and associated human performance outcomes. This is where AI should start and help make the selection and deployment of employees in the company more efficient and achieve higher performance, higher productivity, higher profitability, and significant time savings in the company. Among other things, artificial intelligence should help reduce erroneous decisions when choosing new employees. Since wrong decisions when hiring new employees lead to defects in the operational area, algorithm-based analysis of internal and external company data aims to support management in personnel decisions for candidates and applicants. It is therefore important to implement a modern and future-oriented recruitment model and to develop functional procedures [75]. In the field of application of artificial intelligence systems, various fields of application

can be distinguished, but they are increasingly used together and closely related. These would be natural language processing, natural image processing, expert systems, and robotics [76]. The first three can already be found in the recruitment process. Natural language processing is characterized by capturing, processing, and responding to natural language. The AI process responsible for processing is referred to as natural language understanding. It is not just about the pure sense of meaning but also about the meaning of the information transmitted. The goal of (Natural language processing) NLP applications is to enable machines to communicate with humans using natural language. For example, today, chatbots are increasingly being used for this purpose [44].

Natural image processing means taking, storing, and manipulating photos and videos. Image recognition and image information processing through automatic pattern recognition are the basic building blocks. The algorithms used are trained using hundreds of thousands of images. For this purpose, conditional relations are used as the basis on which human knowledge is made intelligible to computers. Components of expert systems are the acquisition of knowledge, for example based on big data, the development of solutions to problems, and the ability to communicate solutions to users [45].

Integration of big data and artificial intelligence for processing and evaluating big data sets leads to a change in human resource management and the world of work as a whole and changes the basic principles of corporate management [46].

4.2 The Importance of Artificial Intelligence in Workplace

Decision-making is very important for companies in highly competitive and dynamic market conditions, and the amount of data to be analyzed has increased dramatically. Today, the advent of big data technologies and the increase in computing power have increased the importance of artificial intelligence for businesses [77]. Artificial intelligence has long been associated with computer-adaptive decision-making. Its broad spectrum allows it to perform tasks that would normally require human perception and therefore belong to the technology class. In other words, artificial intelligence is a computer-based system that also solves

man-made problems. Artificial intelligence technologies help companies reduce unwanted delays in making business decisions. To help them reduce conflicts and increase income opportunities [15]. Uncertainty and complexity in decision-making processes make artificial intelligence vague considering the impact of information technologies. We found the opportunity to access a lot of data and use or preserve it in a random way in this work. We will choose employment as a potential field of application of artificial intelligence in work because it contains many tried-and-tested theories and ways in which self-learning algorithms can be based. On the other hand, most hiring processes are now set up digitally, which opens many options for direct contact with AI. AI systems can compare information and data from incoming documents with previously generated historical company data based on machine learning [24]. For example, if social competence is identified as a success category for the position applied for in the analysis, the documents submitted by the applicants are scanned accordingly, and a score is generated. One advantage of this AI method is that the system can analyze incoming applications many times faster, thus speeding up the selection process. Another application of AI in recruitment is related to prioritizing job opportunities. Based on the analysis of company data, the AI can provide information about which jobs are easy to get and which are hard to get at the same time, and then the decision-maker can take appropriate action. The use of AI systems has already been tested in job interviews. In an automated interview, for example, in 2018, there was an interview platform conducted by companies in Korea using AI, and the result was that AI was more efficient than traditional interviews used by non-AI companies in terms of saving cost and time and is likely to be It could be adopted by more companies in the future, but it pointed out the potential for data bias that requires improvement [24].

The use of artificial intelligence in employment and its types depend on whether the use of artificial intelligence supports the employee or the applicant as the following points:

1. Artificial intelligence functions recommendation systems match the candidate's profile and the desired job, and then give the opportunity to the candidate who most closely matches the available job.

2. Matching job requirements with applicant curriculum vitae (CV) recommendation systems. Candidates are supported through knowledge-based search and drives for pre-selection of a potential candidate by automating the search task and providing semantic information about the job
3. The analysis of the CVs of the candidates according to their skills and knowledge through an algorithm to determine the applications for employment.
4. Table 1 explain how AI can support and contact between the candidate and company [78].

Table 1: Recruitment Process [78].

Phase	Application of AI
Job advertisements	Machine learning and language analysis supports recruiters in the formulation of job advertisements, selection, and control online channels.
Job search	AI helps to find the right job for a job seeker considering skills, geographical, and demographic data.
Information/ Communication	Self-learning chatbots that answer frequently asked questions from applicants or propose the right job.
Application	CV parsing to optimally present applicant data. Aplication wizard and digital assistants can take over the task of writing an application for a job for the applicant.
Evaluation and selection	AI analyzes components of the application and evaluates candidates and, thus, predicts the fit of an applicant. Tests and assessments can also be intelligently evaluated.

1. Job Advertisements

This includes all actions through which the employer tries to attract applicants. Improved control of job advertisements and advertising measures for hiring employees are also included, so we can indicate the necessity of the human element. Artificial intelligence can support the placement of advertisements by drawing conclusions about promising keywords and appropriate external channels from the existing data. AI can come in handy here because it can automatically assign a job advertisement to an applicant with the appropriate classification and appropriate categories (entry level, industry, occupation) [79].

2. Job-search Recommendation Systems

This includes all measures and solutions that primarily relate to the applicant with a view to himself. The job search by applicants also offers potential for the use of artificial intelligence in that AI can provide very broad and valid job search results based on the entire professional career, completed training, and acquired qualifications and skills [80]. A link to an Internet profile of a candidate can provide relevant data. With the help of the profile, the artificial intelligence system searches for suitable advertisements on job exchanges. The critical point in the process is how the AI gets the prepared information. A satisfactory result will not be achieved with insufficient data. Relevant training data is therefore of particular importance here. In addition, feedback from the applicants is necessary to evaluate the accuracy of the search results.

3. Application Process

The aim of using AI in the application process is to enable promising matches between employees and employers. The application process is primarily about the possibility of a simple and fast transmission of application data. CV parsers, i.e., processes for automatic data extraction from CVs and other profiles, are to be increasingly equipped with artificial neural network processes and deep learning processes in the next few years to increase

performance. A further simplification would be to fill out even complex application forms with the help of intelligent assistants. As a rule, all the information for the application process is already available somewhere. The assistant serves as a data collector and sends the data in prepared form to the applicant management system. Two competing methods are conceivable here. On the one hand, the classic method of applying with a CV and the subsequent processing of the data using intelligent parsing; or, on the other hand, an approach that does not require the transmission of a CV. The digital personal assistant searches the web for all the data required for the position and transfers this to the applicant management system. The classic prescreening interview could also be taken over by voice assistants soon. Scoring is used to determine the probability that a specific characteristic is present in the potential employee. These would be, for example, punctuality, freedom from errors, performance, remaining in the company, customer friendliness, or contribution to sales. The score is a reliable measure of what qualities an applicant will bring with them. A multi-faceted, timely, and valid technical recording of employee characteristics is made possible [81].

4. Evaluation and Selection Process

Finally, you get to choose the field of application. Here, AI should partly take over by outsourcing administrative activities. Artificial intelligence can be beneficial as it reduces the number of applicants through automated pre-selection. Here, it is entirely possible to apply diversity management rules to prevent social discrimination. How this can be achieved using artificial intelligence is part of the following legal analysis. Further steps in the selection process using AI will be automated assessments, and if sufficient training data exists, tasks and questions can also be grouped using AI. Pre-assessment and virtual interviews can also be conducted during the assessment. One application in this field is HireVue, with which the applicant's tone of voice, gestures, and facial expressions are recognized and analyzed during a video interview. Based on the psychological model, this data is compared with relevant test data, and an algorithm is used to create a score for the applicants [61].

4.2.1 Applications of Artificial Intelligence in Recruitment

Artificial intelligence applications used in recruitment artificial intelligence is the challenge facing human resource professionals in finding suitable candidates, and it is necessary to overcome difficulties and manage the recruitment process more easily. It has been developed to provide the support required to reach a qualified and suitable candidate. It can process large data sets, and candidates can be screened through the platforms. In addition to being cost-effective, fair, and impartial, it also provides more job opportunities for the workforce. Because they add diversity, especially virtual assistants, communication with candidates and applications in managing the candidate database for storage, evaluation, and additional references [15]. As recent advances in learning have led to these AI-based tools, they often use supervised learning to select candidates using algorithms. Supervised machine learning is a sub-category of machine learning and artificial intelligence, and we have to mention the algorithms to classify data or accurately predict outcomes using the seeded datasets for training. In other words, the input tries to predict the output values using the data values [11]. The main task of machine learning is to save the training databases and make the information obtained real. Many ATS programs work with their providers to ensure a smooth recruitment process. It facilitates the use of tracking software in the recruitment process in any organization, reducing the great pressure that falls on the recruiters thanks to the wonderful plugins that you use to facilitate the recruitment process. Most hiring managers want to improve recruitment and social quality with parameters that collect profiles from different sources, such as media, job portals, and networking sites, and they rely on ATS software to automate the process of finding matching prospects. During the hiring process, employers select the best candidates from among many applications.

There are a lot of programs that help and use AI-based solutions. Examples of such software are Textkernel, Watson, Mya, and Olivia. Example Watson helps managers select candidates more efficiently by improving communication. Qualified candidates may be referred directly to HR professionals. These communicate with the candidate and resolve inquiries and recruitment after the application is

submitted. It is also used to reconnect candidates during the process. Also, these companies use chatbot technology in interviews for the recruitment process. Conversational natural language processing and machine learning techniques enable bots to understand and respond to the messages they use. To assess the suitability of job candidates using these techniques by asking candidates realistic questions and following the recruitment process among several applications. It can automatically select the most suitable candidates. Interviews are conducted daily using an internet connection. It can facilitate the recruitment process, as it can be done anywhere and recorded in the meantime. The interviewer can then re-analyze the interview recordings later; thus, this process is a more accurate and effective option. Applications of artificial intelligence at work, especially in human resources. It is necessary to treat it seriously because of the algorithms used and the training and testing samples, so more control and scrutiny must be put into the research process to ensure fair and accurate results. For example, analyzing a video interview via artificial intelligence in recruitment processes, in addition to the main machine learning techniques used, their degrees of efficiency, and the resulting positive and negative results We must focus on some characteristics that may lead to moral damages and legal consequences for candidates and companies because of discrimination in the labor market (such as gender and race). The organization and auditing process should be neutral to the type of analysis conducted in the interviews. Full legal compliance and the most effective management of human resource operations must be ensured [82].

4.2.2 Challenges of Applying Artificial Intelligence in Employment

The application of artificial intelligence in employment faces several obstacles when used in companies:

1. It takes a lot of data to learn how to accurately simulate human intelligence and how to screen resumes like a human employee; it may take several hundred to several thousand resumes for a given job.
2. Human biases in hiring such as bias of a certain age, gender or race can be learned, by the AI even though he has been trained away from this behavior.

3. Resource professionals question the efficiency and importance of AI systems in making their jobs easier and want to make sure the system can perform as well as possible without errors. Most companies have changed their way of hiring and are leaning towards algorithms that produce rankings of candidates according to different features.

Large multinational companies have realized the value of many AI systems and video interview companies [35]:

1. Dr. Frida Polly Founder the CEO of Plyometrics, a game-based company that harnesses the power of data and artificial intelligence to select the right employee Dr. Frida Polly trained in neuroscience at Harvard Medical School and completed a postdoctoral fellowship in neuroscience at MIT. "I came up with the idea for plyometrics after realizing how effective resumes can be when applying for a job; you can happen to match the hiring process with the people applying the AI application in question aims to get a much larger pool of applicants for companies and get an idea of which candidates would be more successful in this job." According to Frieda Polly, emphasizing that everyone's goal is to find the right job or the right worker, Polly explains that using artificial intelligence systems wisely benefits everyone. In plyometrics, it uses neuroscience as well as artificial intelligence to predict the right person for the job without bias, matching candidates to jobs and companies where they are most likely to succeed based on their cognitive and emotional attributes. For example, someone recently applied for a new job. He said at the initial stage of the hiring process, the publisher had me play a series of simple games online at home. Games included quickly counting the number of points in two boxes, inflating a balloon without popping it to earn coins, and matching emotions to facial expressions [83]. Then an AI program evaluated my personality. As a result of this evaluation, which no one can interfere with, I either pass or fail the test. But the question is, is it fair for a computer to accept or reject your job application in this way? Honestly, it was a bit stressful when I learned that my application was being evaluated by a computer and not by a human being. It may be far from biased, but it can't be very transparent and equitable. This type of AI software uses the initial

recruitment processes of companies such as McDonald's and JP Morgan Bank. If you pass this test, you can meet with an HR specialist. Pymetrics also says that their system provides greater fairness and that "every algorithm is rigorously tested for bias." Polli states that the program is better than trusting companies with resumes:

"A resume can tell you the hard skills one needs to do the job. "But research and common sense tell us that soft skills also contribute to business success, as do good habits, communication skills Pymetrics also says that their system provides greater fairness and that "every algorithm is rigorously tested for bias". Polli states that the program is better than trusting companies with resumes:

"A resume can tell you the hard skills one needs to do the job. But research and common sense tell us that soft skills also contribute to business success, as do good habits and communication skills" [82].

2. Amazon is one of the companies that uses artificial intelligence. Amazon terminated the use of the artificial intelligence program that it used in hiring in 2018 on the grounds that it was unfair. As online retail giant Amazon abandoned its recruitment system in 2018 because it put female candidates at a disadvantage, there was news that Amazon's artificial intelligence system found male candidates more favorable. The reason for this is that tech industry experience is more common on male resumes. Amazon declined to comment on the matter. Computer models were trained to screen applicants at Amazon. This was done by observing patterns in the resumes of applicants for the job at the company for a period. The results were biased. Most applicants were men, which reflects a bias across the technology industry against women as mentioned in the Figure 2 and Figure 3 [84].

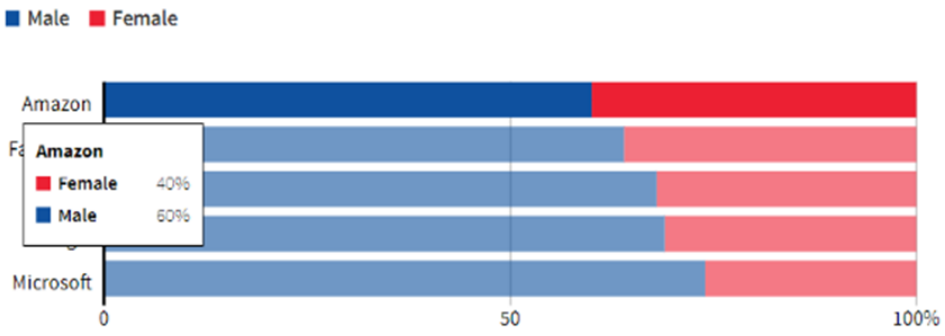

Figure 2: The Gender Breakdown of its Technical Workforce since 2017.(a)[84].

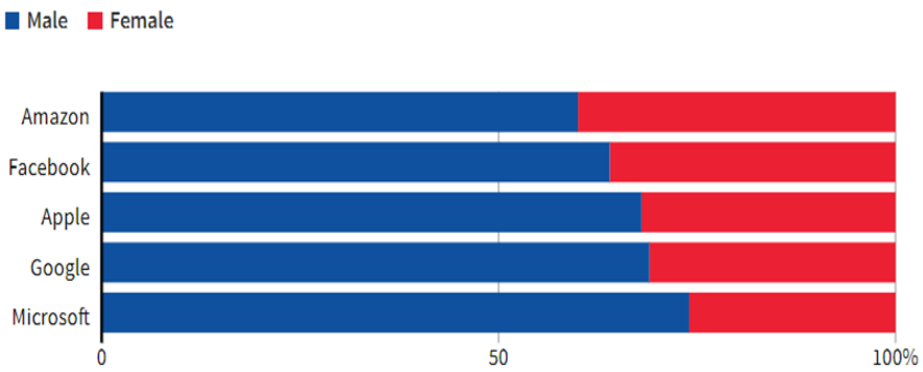

Figure 3: The Gender Breakdown of its Technical Workforce since 2017. (b)[84].

As the example of major US technology companies, including Amazon, shows bias in the selection of employees such as software developers, the number of men far exceeds the number of women, with only 26 percent of women appearing to be female. of men are at Microsoft, 40% are women, and 60% are men at Amazon, the system developed by Amazon to help make hiring decisions is biased against women because the algorithm built its model by learning from previous hiring decisions that favored men. Help automate hiring decisions that have been shown to be sexist. This bias exists because the algorithm builds its model by learning from past hiring decisions that favored men over women [54].

3. We asked Miguel Angel López Hernandez, Director of Human Resources, RRLL, PRL/CHRO and EHS at PcComponentes in Alhama de Murcia, Murcia, Spain, is a Spanish e-commerce technology company specializing in computer, electronic products and home appliances owned by PcComponentes y Multimedia SLU. It currently belongs to the YF Networks group and operates in Spain and Portugal. He told us about his experience with AI systems applied to human resources, which have both positive and negative effects.

Positive effects:

- Efficiency: AI systems can process large amounts of data in a short time, making candidate selection and evaluation processes faster and more efficient.
- Reducing errors: AI can help reduce errors in selection and evaluation processes as systems can more accurately identify patterns and predict outcomes.
- Greater objectivity: AI can help remove human bias in selection and evaluation processes, which can lead to more objectivity and fairness in decision-making. Data analysis: AI systems can analyze huge amounts of data about employees and provide valuable insights into their performance, which can help HR managers make informed decisions.

Negative effects

- Lack of empathy: AI lacks empathy and emotional understanding, which can negatively affect the relationship between employees and the company.
- Discrimination: If AI systems are not designed properly, they can perpetuate prejudice and discrimination against certain groups of people, such as different age groups, gender, race, or ethnicity.
- Data privacy: AI requires large amounts of data to function properly, which can raise data privacy and security concerns.
- Job loss: Automation of some HR processes through AI may lead to some job losses, which may have a negative impact on affected employees.

Miguel sees the reliability of AI systems applied to HR processes as dependent on several factors, including the quality of the data used, the accuracy of the AI model, and the way the system is implemented in the organization. In general, AI systems can be trusted if they are designed and used properly, with ethical and privacy considerations in mind. However, the application of artificial intelligence systems in human resource operations can cause some problems for company employees. some:

- transparency: It can be difficult for people without experience in the field to understand AI models, which can lead to a lack of trust in the decision-making process.
- Bias: If the data used to train AI models contains an inherent bias, the results of HR processes may also be biased, which can negatively affect certain groups of people in the organization.
- Ethical concerns: AI systems can raise ethical concerns about privacy and data security, as well as fairness in decision making.
- Loss of personal relationship: Managing employees through AI systems can reduce the personal relationship between employees and human resource managers, which may affect employee satisfaction and commitment to the organization. Overall, it is important to consider both the potential benefits and issues of AI systems in HR operations and work towards designing and implementing ethical, accurate, and transparent systems that consider the interests of the people in the organization.

We asked him if human supervision is necessary to avoid bias, establish justice in work, and prevent errors. Yes, human oversight is necessary to avoid bias, achieve justice at work, and prevent errors in the use of artificial intelligence in the field of human resources. He also stressed that artificial intelligence itself is not foolproof and can perpetuate bias and discrimination if it is not designed properly. Moreover, AI lacks emotional empathy and understanding, which can negatively affect the relationship between employees and the company.

Therefore, it is important that AI systems in HR operations be supervised by humans, particularly in critical areas such as candidate selection and evaluation, employee recruitment, and career decision-making. Human oversight can help ensure that AI systems are designed and used ethically and fairly and do not perpetuate bias or discrimination against certain groups of people. Additionally, AI systems can produce unexpected or incorrect results if not properly monitored. Human oversight can help detect and correct

errors in the use of AI, ensuring that results are accurate and reliable. In short, human oversight is necessary to ensure that AI systems are used ethically and fairly in HR processes and to prevent errors and biases that can negatively affect employees and the company. Miguel considers that the negative effects of using artificial intelligence in the strategic management of people's functions are as follows:

Negative effects

- Lack of empathy: AI lacks empathy and emotional understanding, which can negatively affect the relationship between employees and the company.
- Discrimination: If AI systems are not designed properly, they can perpetuate prejudice and discrimination against certain groups of people, such as different age groups, genders, races, or ethnicities.
- Data privacy: AI requires large amounts of data to function properly, which can raise data privacy and security concerns.
- Job loss: Automating some HR processes through AI can lead to some job losses, which could have a negative impact on affected employees. For Miguel, as a manager and HR officer, thinks AI systems can be useful in taking over some tasks at work, including hiring new employees and automating other repetitive, low-complexity tasks. AI can help improve efficiency and accuracy in HR processes and free up time for HR managers to focus on more strategic, high-value tasks. However, it is also important to note that AI cannot completely replace human judgment and decision-making. Recruiting new employees is a critical task that requires complex and subjective assessments, and AI may be limited in its ability to assess intangibles such as culture and personal fit. Additionally, AI systems can perpetuate bias if they are trained on biased data or are not adequately designed to mitigate it. It is important to keep in mind that AI is just a tool, and the ultimate responsibility for making decisions rests with humans. In short, we conclude, according to experience, that artificial intelligence systems can be useful in

certain tasks at work, but they must be designed and used with caution and human supervision to ensure that they are used ethically and fairly in human resource operations, and they cannot replace human judgment and decision-making properly. This is where the proposed EU AI Regulations 2021 and GDPR Data Protection Regulations and compliance come into play.

In this regard, it is particularly important that the proposal states that AI systems at work are considered "high risk" due to their potentially tangible effects on the future employability and livelihoods of people when used to: manage persons with whom they have an employment relationship or access to them, as well as in relation to the self-employed, in particular to select persons; make the decision regarding your promotion, termination of contract, or assignment of duties; observe or evaluate persons subject to an employment relationship. In this sense, and apart from concerns about privacy and the protection of personal data, there is a justified fear on the part of the regulator about the potential implications of existing biases in said technologies in relation to discrimination (based on gender, age, disability, religion, race, or sexual orientation). In recruitment, in addition to the implicit biases that may exist with regard to AI for the workplace, it is evident that new methods of selecting employees through algorithms or even determining working conditions (schedules, salaries, promotions, systems in which employees are selected, etc.) intertwine with the basic rights of workers such as data protection and privacy and may even conflict with some basic aspects of the nature of the work relationship with others, such as substituting the employer in the exercise of part of the functions, for example, issuing instructions and orders in the field of its management. According to the European Commission's regulatory proposal, when technologies used in work are considered "high risk", this means the obligation to pass certain controls by the corresponding authorities before they are applied in work and compliance with regulations [63].

4.3 The Purpose of AI Compliance with Regulations

The Commission has identified the main goals that it wants to achieve by establishing a unified framework with the regulation:

- The artificial intelligence systems that will enter the Union market must be safe and respect the fundamental rights, freedoms, and values of the European Union.
- Ensuring legal security that facilitates innovation and investments in the field of artificial intelligence.
- Improving governance and effective enforcement of fundamental rights and security laws already applied to AI systems; To support the formation of a single market for legal, safe, and reliable AI applications and to prevent market fragmentation.

According to Article 1 of the regulation, the main issues emphasized are as follows [43]:

- To establish harmonized rules for placing artificial intelligence systems on the market or operating them within the Federation.
- To block some artificial intelligence systems.
- Provide harmonized transparency rules regarding artificial intelligence systems intended to interact with real people, emotion recognition systems, biometric classification systems, and artificial intelligence systems used to produce or process image, audio, and video content.
- Setting the rules for monitoring and controlling

the market Article 2 of the Regulation regulates the area of application in a manner like the European Union's General Data Protection Regulation. This means that the regulation does not only concern individuals and institutions within the borders of the European Union; it is also binding on the AI system provider or users residing outside the European Union, provided certain conditions are met, according to Article 21 of the regulation [17]:

1. AI providers who provide or deploy an AI system within the Federation, regardless of whether they are established within the Federation.
2. Users located within the federation.
3. Providers or users in third countries of the artificial intelligence system whose outputs are used within the Union.

So, we must know what the obligations of high-risk AI system providers are. Before high-risk AI systems can be placed on the EU market or otherwise operated, service providers must agree to undergo a conformity assessment. This allows them to demonstrate that their system complies with the binding requirements of a trustworthy AI (for example, in relation to data quality, documentation and traceability, transparency, human oversight, accuracy, and durability). Should the system itself or its purpose be significantly changed later, it must undergo reevaluation. For specific AI systems, an independent evaluation body is named to participate in this process. With AI systems, the safety components of products covered by EU sectoral legislation are always considered to have a high risk when used in accordance with this sectoral legislation and must be subject to a third-party conformity assessment. Similarly, a conformity assessment of biometric identification systems is always required by a third party. In addition, providers of high-risk AI systems must ensure quality and implement risk management systems to ensure compliance with new requirements and reduce risks to users and data subjects, even after the product has already been released to the market.

For post-market monitoring, the market surveillance authorities conduct audits and provide service providers with the opportunity to do so to report incidents or serious violations of basic rights that they become aware of [14]. The draft introduces a complex product safety framework that is basically structured around four risk categories, a risk-based approach. It combines a risk-based approach based on a pyramid of importance with a layered enforcement mechanism, as mentioned in the previous chapter. At the member state level, the bank will also have national auditors, like the oversight mechanism of the GDPR. This authority will determine the fine for breaking the rules based on the risks determined by the pyramid. This amount can reach 6% of the global turnover or up to 30 million euros for private institutions according to Article 71 if there are violations:

a) The prohibition of artificial intelligence practices referred to in Article 5 Artificial systems outlaw artificial intelligence with unacceptable risks. that violates basic rights. According to Article 5(a) of the proposal, manipulating people to harm themselves or others or prohibiting the use of intelligence system applications Article 5(b): In the first paragraph, vulnerable groups such as children or persons with physical or mental disabilities for themselves or others are included. Exploitation in a manner that is harmful or likely to cause harm is prohibited Also, high-stakes AI systems Organized under Title III. Under this heading, Applications, Products, and in sectors that pose a significant risk to health, safety, and basic rights.
b) failing to comply with the requirements set forth in Article 10 by the AI system. For example, systems such as face recognition, legal penalties, and social credit are strictly prohibited; systems such as credit management and border control will be subject to approval and inspection processes in the CE certification standard; the ability to explain these algorithms; the representation of the data sets used, such as the use of systems in recruitment; consideration of the rights of applicants in their data; the selection of the appropriate candidate without bias; etc. The artificial intelligence systems used in less dangerous jobs are expected to be AI.
c) Promote low-risk products: The pyramid's foundation refers to tactics that pose little or no danger. This category includes any existing AI system that is not specifically described in the document. According to the Commission, it covers "the vast majority of AI systems currently in use in the EU." Spam filters and AI-powered video games, for example, are not subject to additional regulatory restrictions. Although these AI systems will not be explicitly governed by legislation, Article 69 can influence their development. The Commission thinks that the implementation of soft law systems would encourage the voluntary adoption of values like as transparency, human supervision, and robustness, which are now only applicable to high-risk AI systems. [85].
d) Special Liabilities for Limited-Risk Products: This porous layer covers some non-high-risk techniques. A defining characteristic of AI systems that fall into this category is that they raise certain issues in terms of transparency and

therefore require special disclosure obligations. There are three types of technologies with such specific requirements for transparency: deepfakes, AI systems intended to interact with humans, and AI-powered emotion recognition and biometric classification systems. Article 52 of the proposed regulation would give people living in the EU the right to know if a video they're watching is seriously fake and whether the person they're talking to is a chatbot or a voice assistant. However, there are some exceptions. transparency obligations: it does not apply to AI systems authorized by law to detect, prevent, investigate, or prosecute criminal offenses. It should be noted that emotion recognition systems are exempt from this exception. It is always necessary to provide an explanation of the purposes for which these systems are used [85].

e) How is compliance enforced?

Failure to comply with any of the requirements or obligations set forth in this Regulation other than those set forth in Articles 5 and 10 will result in administrative fines of up to 20,000,000 euros or, if the offender is a company, up to 4% of the total global annual turnover for the previous fiscal year, whichever is greater. In response to a request, providing inaccurate, incomplete, or misleading information to notified bodies and competent national authorities is punishable by administrative fines of up to €1,000,000 or, if the offender is a company, up to 2% of total annual global turnover for the preceding fiscal year, whichever is greater. When determining the amount of an administrative fine in each specific case, all relevant circumstances of the corresponding case will be considered, and the following will be duly considered:

a) The nature, seriousness, duration, and effects of the breach.
b) Whether other market control authorities have already imposed administrative fines on the same operator for the same offense;
c) The size of the operator committing the violation and its market share.

In applying and enforcing regulations, Member States have also played a major role. To this end, each member state should have one or more competent national authorities appointing those who oversee implementation and market surveillance. The basic terms contained in the obligations of the providers of artificial intelligence

systems Prerequisites contained in Chapter 2 of the Proposal for Regulations on Obligations When these judgments are examined, they are generally directed towards the provider of the AI system. According to Article 3.2, the definition of supplier" is "paid or unpaid, in its own name or for the purpose of putting it on the market or providing it with its own brand. The natural person develops or possesses an artificial intelligence system or is identified in the legal code proposal. Cases of any distributor, importer, user, or third party [86].

It is the provider's responsibility to market their high-risk AI systems under their own name or brand. This will be considered a resource within their scope and will showcase if they have made fundamental changes to their high-risk AI systems. It is subject to its responsibility (Article 28 of the proposed regulation). A management system for high-risk AI system providers and suppliers should be established in Article 17 of the Recommended Regulations. The quality management system will be updated throughout the life of the system, which includes the establishment of a documented risk management system. Risks are also identified and evaluated in accordance with Article 9, which is the "Risk Management System." The risk management system will continue to be established, documented, and implemented. The risk management system deals with the appropriate design and development of risks, and they must be eliminated or mitigated. Also, one of the most important obligations is the use of high-risk artificial intelligence systems and the selection of high-quality data sets. As in the title of Article 10, "Real Data Management". The use of sensitive personal data is permitted to the extent necessary to detect and monitor bias as per the recommended regulations, Article 5.10 Data on Race or Similar Sensitivity in the GDPR. The use of data is prohibited, except for the cases specified in Art. There are no exceptions to the GDPR, such as EU-wide bias disclosures. But the AI Law of Motion has an exception. This exclusion is only for high-risk prostheses in relation to intelligence systems and their providers. For high-risk AI system providers, before the introduction of the AI system into the EU market and before it is launched, there is a report that the system complies with the regulation proposal [43][87].

4.3.1 High-risk AI System Requirements for Sellers or Importers Analysis of Proposed Regulations

1. The providers must ensure that high-risk AI systems meet the following requirements:
   - They must Develop high-stakes AI systems that use techniques that include training models with data from training, validation, and testing datasets.
   - Training, validation, and test datasets must be relevant, representative, error-free, and complete. We can see it in [10.1, 10.3]
   - be sufficiently transparent to allow users to appropriately interpret high-risk results. High-risk AI systems must be designed and developed in such a way as to ensure that they operate with a sufficient level of transparency for users to correctly interpret and use their output information. and we can see it. [Art.13.1]
   - be sufficiently accurate, robust, and secure in relation to their intended purpose. [Art. 15.1]
   - Automatic registration of processes and events during operation [Art. 12.1]
   - It can be supervised by people to supervise the operation of the high-risk AI system. It stops High-risk AI systems will be designed and developed in such a way that natural persons can actively monitor them during the period they are in use, fully understand the capabilities and limitations of the high-risk AI system, and properly monitor its operation so that they can detect and resolve indications of anomalies, operational problems, and unexpected behaviors in time. As soon as possible, and this is in [Art. 14.1, 14.4].
2. Providers of high-risk AI systems before introducing an AI system into the EU market, the system must comply with the proposed regulations, applicants are required to undertake a conformity assessment (Article 16 (e, a) of the proposed regulation) and 19.1 service providers or suppliers use This evaluation is an internal evaluation in most cases. They will announce themselves after verification. no changes This statement must also be

updated when it is made. Tele biometric identification and public infrastructure networks every five years or less will be evaluated by a designated third party.

- For artificial intelligence systems that are used for remote identification, the provider and the provider of such systems are required to carry out a conformity assessment [Article 43.1]. In the case of an artificial intelligence system that is a security product or a component of a product derived from existing products, in accordance with the rules of the EU Health and Safety Harmonization, it is subject to conformity assessment by a third party, and the conformity assessment is carried out by these third parties [Art. 43.3]. This is because applications, products, and sectors pose a significant risk to health, safety, and basic rights. The rules related to artificial intelligence systems are regulated (Art 43, Art 43.6-43.7).
- For other artificial intelligence systems, the conformity assessment is carried out by the provider itself [Art. 43.2]. To ensure the supposed compliance with the requirements of high-risk AI systems as in [Art. 40].
- Suppliers must place the EU Declaration of Conformity in accordance with Article 48 and the CE Mark in accordance with Article 49 [30].

3. Before bringing a high-risk AI system to market, service providers must establish a risk management system that identifies risks throughout its life cycle [Art. 9.1].
    - Risks are determined through testing and a post-market monitoring system [Art. 9.4 and Articles 61.1, 61.2].
    - If necessary, risk management measures should be taken so that system risks are 'acceptable' [Art. 9.4].
4. The provider's must create and maintain updated technical documents that prove this. Its systems meet the requirements of high-risk AI systems [Art. 11.1 and Article 18].
5. Providers are required to provide instructions for user, which contain information on the property, The capabilities and performance limitations of their systems include [Art. 13.2, 13.3].

6. Service providers must establish a quality management system that ensures compliance with AI regulations [Art. 17.1].
7. Service providers must report serious accidents or malfunctions to the supervisory authority [Art. 3.44 and Article 62.1].
    - Serious accidents are accidents that can lead to the death of a person or serious harm to his health; serious damage to property or the environment; or severe and irreversible disruption of critical infrastructure.
    - Malfunctions are accidents that violate EU law protecting fundamental rights. Represent. In the case of artificial intelligence systems meant to interact with natural people, service providers must be sure to inform the people who interact with the AI system if this is not the case [Art. 52 .1].
8. In artificial intelligence systems for emotion recognition or biometric profiling, these are systems that identify people by categories such as age, gender, ethnic origin, sexual orientation, or political orientation.
    - Users are required to inform the registered persons about the operation of the system to avoid ethical problems.
    - The natural persons who are exposed to the operation of the system must be informed. According to the law, biometrics of artificial intelligence systems are permitted and used to detect, prevent, and investigate crimes.
9. Users of artificial intelligence "deep fakes" manipulated systems that manipulate image, audio, or video content so that it is real and appears to be real, must report that the content has been manipulated. [Art. 52.3].
    - Codes of practice must be established by service providers of artificial intelligence systems [Art. 69].
10. Market surveillance authorities have unfettered access, even from a distance. Training, validation, and testing datasets used by service providers [Art. 64.1] When an AI system meets the requirements of the Regulation but still poses a health risk to the safety of persons or other aspects of public interest, the market watchdog shall require the provider of AI systems to take appropriate measures to eliminate the potential risk or withdraw the AI system from the market according to [Art. 67.1] [30].

11. To ensure legal certainty of AI innovation support measures in Article 53 of the Regulations proposal referring to controlled sandboxes for AI sandboxes set up by the competent authorities of one or more Member States or the European Data Protection Supervisor must provide a controlled environment that facilitates the development, testing, and validation of innovative AI systems during a limited period before they are put on the market or put into service under a defined planning, and validation of innovative AI systems during a limited period before they are put on the market or put into service under a defined plan. This shall be done under the direct supervision and direction of the competent authorities to ensure compliance with the requirements set forth in these regulations, and, where applicable, before the launch or operation of artificial intelligence systems, they shall be developed and tested under direct supervision in a controlled environment and evaluated before they are put on the market or placed in service. Regulations can be supervised. The aim of these sandboxes is to ensure legal certainty for those involved in innovation and regulation, to ensure compliance with the proposal, and to supervise relevant national authorities to maximize the impacts of AI and the risks that may arise from understanding it. Sandbox is a sandbox environment. In this sandbox, software developers put the software they are working on. They can test it without affecting the application, system, or platform. Mirror potential programs or applications from all user data on the network with unlimited access to system resources. [As a result, we have found this bylaw in the bylaw proposal to be appropriate [43].

The impact of the regulation on the labor market and basic rights can be summarized as follows: The regulation ranks products that use all or part of AI software according to the risk of a negative impact on fundamental rights such as human dignity, freedom, equality, democracy, the right to non-discrimination, data protection, and health and safety. The greater the possibility of exposing the product to these rights at risk, the greater the severity of the measures taken to remove or mitigate the negative impact on the basic rights, to the extent of banning those products that are completely inconsistent with these rights, and

this is the responsibility of the supplier or service provider. The following Table 2 shows the solutions by product classification.

Table 2: The Impact of Regulation on the Labor Market, Basic Rights and Solutions by Product Classification [43].

Risks for fundamental rights	Types of products classified according to risk	Solutions
(Article 5) The use of intelligence system applications is prohibited. Article 5(b): In the first paragraph, vulnerable groups such as children or people with disabilities are included. physically or mentally to themselves or others Exploit in a way that is harmful or likely to cause harm. The use of artificial intelligence applications is prohibited. Article 5(c): social behavior or the behavior of people by public authorities It is based on artificial intelligence based on the evaluation of characteristics. Social recording AI apps are banned. of the article 5 To implement the law in public places in Paragraph (d). The use of remote, real-time biometric recognition systems is limited. Prohibited, except that exceptions apply.	products capable of - Causing or being able to cause physical or psychological harm or exploit and carry out extortion by manipulating human behavior to circumvent the free will of users of artificial intelligence systems related to exploitative practices. - It is possible to impose a so-called "social assessment" by or on behalf of public authorities if they are treated in a harmful way due to the entry of irrelevant data that may lead to harm.	The use of these products is prohibited and called prohibited systems

the product (Article 5)	- Remote "real-time" biometric identification systems in publicly accessible spaces used by law enforcement agencies fall into this category. - Real-time biometric recognition systems for law enforcement purposes Its use is prohibited in some cases. With facial recognition software.	This type of product, generally and almost exceptionally prohibited and under the control of the authority.
(art.6) Pursuant to paragraph (1) of Article 6, artificial intelligence is independent of the products specified in subparagraphs (a) and (b) of Art. Whether it is put on the market or put into service Both of the conditions set forth in subparagraphs (a) and (b), regardless of The AI system in question is high-risk. It will be. These are: a) the Consortium Coordination for the AI system listed in Appendix II; use of a product covered by legislation as a safety factor intended, or the AI system itself is such a product; b) put it on the market in accordance with the harmonization legislation of the Union included in Appendix	Products - already subject to the European legislation referred to in Annex II of the Regulation and to the conformity assessment by third parties in view of the placing on the market or putting into service of products according to the same legislation as in Appendix II; Identification and classification of natural persons by biometric sentiment and biometrics in the Bill of Rights; management and operation of critical infrastructure; vocational education and training; employment and management of workers; access to and use of essential private services and public services and benefits; and law enforcement	To mitigate the high risks, the following conditions must be met as stipulated by the regulation before these products are put on the market: - A risk management system must be provided to assess and combat risks. - Provide and manage high quality data. Because the higher the quality of the data, the lower the risk to fundamental rights and the avoidance of discriminatory errors. - Provide the necessary information to assess the system's compliance with the requirements and carry out the assessment of this conformity with the officials. - the possibility of tracking results by keeping documents through log files to ensure transparency in relations with users, their reporting duties and human oversight to control and reduce risks;

II; or from a third party to assess compliance with the assignment. An AI product or system with a security component that must pass Situations in which the intelligence system itself is the product		- Obliges suppliers, distributors, and users, as stipulated in Article 16-Article 29, to comply with the conditions to ensure robustness, safety, and accuracy in managing artificial intelligence so that the results are not subject to errors or defects.
(art. 52) According to Article 52.3 of the bill; They create or process the content of images, audio, or video to present people, things, and places, such as other entities or events	Products that touch natural persons Products that create or manipulate images or audio Manipulated systems that impersonate video content that closely resembles people at work or video used in job interviews could be falsely shown to someone as authentic or truthful.	- People should be informed that there is artificial intelligence of this type. They interact with them. - Natural persons must be informed that their video or audio content has been artificially created or manipulated.

4.3.2 Obligations of Users of High-risk AI Systems

One of the most important obligations imposed by the regulation is to ensure the use of artificial intelligence systems in conjunction with the risk management system. The risk management system to be developed must be able to eliminate or reduce risks, implement technical measures, provide information, and test existing practices. In addition, the regulation imposes comprehensive obligations regarding high-risk AI systems as well as [88]:

1. Data management.
2. Store and keep records of technical information.
3. Transparency and provision of information.
4. Human supervision.
5. Accuracy, robustness, and cyber security the definition of "user is specified in Article 3(4) of the Proposed Regulations.

In this way, users should not use the AI system during a personal, non-professional activity. Any fact you use is under its own power, except where it is used. "a legal person, public institution, organization, or other body." User expression in the text of the article using the artificial intelligence system Natural persons, legal persons, and visible public institutions using the artificial intelligence system for professional purposes. In accordance with the legal proposal, users are considered users of the domain. Here, using the AI system in the personal non-professional activities of high-risk AI users must use the system as specified (Article 29.1) of the proposed regulation. Measures relating to human control specified by the vendor or supplier shall be applied (Regulation Proposal 29.2). Users should also ensure that the data uploaded to the system is relevant to the intended use of the system. (Proposed Regulation, Article 29.3).

Other obligations to users (health, safety, or fundamental rights) unforeseen situations or dangers related to liberties (Proposed Regulation, Article 65.1) to monitor the operation of the system Users can use the system in any emergency. Discontinue use if it is thought to be dangerous. subject to suspension. In addition, users are aware of this position of the provider, and the provider must be notified

(System Proposal, Article 29.4). The technology identifies high-risk AI users. They have control over automatically created records. Synthetic records that pose a significant danger. Users should train the system using validated data. The restrictions apply whether or whether economic operators, such as suppliers, data controllers, or processors, are based in the EU in Article 2 of the IA Regulation and Article 3 of the GDPR). This answer effectively implies adopting standards that include not just access to EU markets but also access to customers and users in a globalized system of marketing intangible products and services that have no borders and are not necessarily local to an area. The results are likely to be obtained. However, for the same dataset, different outcomes depend on the modeling technique used. Also test models. It must be indicated. New datasets for AI systems to prevent biases from arising when incorporated into decision-making processes. It should be noted that users should also follow the fairness model. Is the AI model fair and unbiased toward all customer segments? Deal with transparency and interpretability and test the AI model appropriately to ensure that it provides the required safety and performance [89].

4.3.3 Legal Obligations for Personal Data

In the recruiting process, artificial intelligence algorithms frequently process personal data, putting people's rights and freedoms at risk. Therefore, data protection is an important regulatory criterion for the development and use of artificial intelligence systems in which personal data is processed. The areas subject to data protection law analysis when using artificial intelligence are transparency, purpose restriction, legality, data minimization, information requirements, implementation of data protection impact assessment, and prohibition of automated decisions. The processing of personal data always means the infringement of the fundamental rights of data subjects, which is why the interests of protecting data subjects require legal obligations to act. Article 6 Paragraph 1 GDPR defines prohibition with permission reservation, according to which data processing is legal only if it is legalized with the consent of the data subject. So, data processing using deep learning can be legally based on consent, fulfillment of a contract, and legitimate interests. The legal validity of the exceptional fact of

consent is set out in Article 7 of the GDPR. It should be possible to give consent unequivocally after sufficient information has been provided, and voluntariness requires real choice for those affected. In addition, the consent must be related to one or more specific purposes. In terms of AI, voluntariness should be questioned if lock-in effects prevent an opt-out option. Article 22 of the GDPR requires special AI features in relation to consent, in that consent must be expressly granted for automated decision-making. Contract execution as a license is regulated in Art. 22. 2 GDPR and is mainly used for time-consuming operations.

There is a European project called GDPR: Management of Workplace Data Processing through Industrial Relations, under the supervision of the Italian Trade Union Confederation. GDPR aims to promote collective bargaining and social dialogue efforts in the field of workplace data handling, as well as the adoption of collaborative solutions. Protecting workers' rights is one of the most important things to consider in the context of long-term digital transformation. The main outcome of the project will be the organization and delivery of customized training modules designed for manufacturing trade unionists and workers' representatives. The processing of personal data is one of the issues that will have, and will have in the near future, a very significant impact on the balance of bargaining power between workers and employers. New technologies, based on the use of artificial intelligence, algorithms, and in big data make it possible to collect and process a larger number of worker data in a relatively simple and inexpensive way than was possible thanks to the previous generation, undoubtedly beyond human capabilities. This, together with the ability of these tools to develop probabilistic models of workers' future behavior and make decisions independently based on the processed data, can have devastating effects on traditional managerial privileges associated with the employment relationship, such as the recruitment process, work organization, performance monitoring, and the exercise of disciplinary authority. What if your boss was an algorithm? Economic incentives, legal challenges, and the rise of artificial intelligence at work It should be noted that systems that analyze people, a data-driven approach to human resource management, can have a significant impact not only on individual labor relations but also on workers perceived as a group, in part because of the technical characteristics of this type of

algorithmic tool. In view of this, it seems that a "collective" approach to organizing data processing during an employment relationship is also necessary on the part of the workers themselves. Strong involvement of trade union organizations on this topic would also be fully consistent with the "human participation" approach. Diletta Porcheddu is a PhD candidate in Learning and Innovation in Social and Work Contexts (University of Siena/Adapt) with an ADAPT Advanced Apprenticeship track. GDPR is just a legal obligation to comply with, not an object or instrument of contract. The GDPR project's next rounds of study will focus on determining whether trade unions continue to take a 'defensive' attitude to the problem of workers' data processing or have adopted more 'participatory' methods. This also takes into account new legislative provisions on automated decision-making or monitoring systems, such as Legislative Decree No. 104/2022 (implementing EU Directive 2019/1152 on transparent and predictable working conditions in the EU), which grants workers and their representatives' access to information about data-driven technologies. [90].

Chapter 5

5.1 Conclusions

1. The expanding role of AI in different areas of organizations, including human resource management, opens up significant opportunities for research endeavors. This work aimed to explore the legal implications of deploying AI systems for hiring decisions in corporate environments. It specifically focused on the feasibility of implementing a legal framework for companies to follow. Furthermore, the study examined prominent instances, such as Amazon, and scrutinized the legal requirements applicable to importers, AI system providers, and users, considering their potential legal impacts. Proposing the European Union's Regulation on Artificial Intelligence Systems to create a legislative regulation is a vital step for safety, basic rights protection, supervision, and consumer protection, and we believe the risk-based approach used in proposing the AI Act was good. As AI technology brings both advantages and concerns. To achieve fairness and address potential risks, it is vital to have appropriate rules and penalties in place to regulate AI usage. These measures help maintain a just and responsible AI ecosystem.

2. According to applicable laws and regulations, providers and users will be required to feed their systems appropriate information so they can ensure compliance with the law. Thus, the required control aspect will be satisfied to a large extent. For the HR field, for example, bias means that important characteristics such as race, religion, disability, sexual orientation, etc. should not play a role in the application process and evaluation.

3. General Data Protection Regulation (GDPR) are used to maintain integrity, protect fundamental rights, and monitor and protect consumer and personal data. Depending on the risk-based approach when proposing artificial intelligence, the problem of discriminatory algorithms should be discussed, as the data protection regulations consider in Art. 22 of the GDPR, because of the effects of artificial intelligence on data subjects. The acceptability of the

decision-making process is regulated, not the acceptability of the data processing itself, because automated decisions have an impact on personality traits and lead to significant legal effects or disabilities for those affected. Automated decision-making processes must adhere to extensive information requirements. This is essential to guarantee that data processing activities are conducted in a manner that complies with data protection standards.

4. To guarantee that data processing activities align with data protection requirements, it is necessary to adopt both technical and organizational measures throughout the development and utilization of AI systems. These measures help safeguard personal data and maintain compliance with data protection standards.

5. It is vital to adhere to data protection principles, including purpose limitation and transparency when using AI systems. The original purpose of data processing should be maintained throughout algorithm programming and subsequent tasks. If new purposes arise, they should be defined and remain compatible with the original purpose. This principle extends to the use of personal data for training AI systems as well.

6. In systems like emotion recognition or biometric profiling, it is crucial to inform employees who are subject to these systems that their data may be processed, including the generation of videos or photos using technologies like Deep Fake. This information should be provided to the individuals involved, and their consent should be obtained for such processing.

7. As the field of artificial intelligence continues to evolve, the future of European AI law will necessitate close cooperation between computer science and legal disciplines. This collaboration is essential for developing comprehensive legal standards that address societal risks associated with AI and promote the widespread access and responsible use of AI systems. Indeed, adopting an interdisciplinary approach can greatly benefit corporate practices, and there is a need for synergies between IT and legal enforcement within organizations. Regarding self-regulation by actors outside the political

realm, corporations have the opportunity to make valuable contributions through the establishment of codes of conduct. These codes can serve as guiding principles and ethical frameworks that help govern the responsible use of artificial intelligence within the organization. Legal uncertainty cannot only be avoided for companies; legal protection for individuals can be ensured by orienting themselves towards comprehensive and specific legal standards.

5.2 Future Work and Recommendations

Below are some recommendations that companies should consider when utilizing AI systems:

1. Legal doubts and possible solutions for companies that want to use AI, the problem is that the risks of automated decisions are far from being fully known, and the scope of the need for regulation and the possibilities of legislation are currently insufficient. Many legal questions have not yet been sufficiently clarified. Regulatory measures are still to be taken when AI systems are used to bring more transparency and accountability through algorithms, comply with transparency obligations, and ensure legal certainty for businesses regarding the establishment and use of AI methods.

2. Ensure equal treatment in the company. Anyone using a company's AI systems must ensure that the underlying data quality is high and system-related discrimination is prevented. Like in HR, managers must realize that decision-making processes based on data or systems are not objective and fair in and of themselves. Standard specifications must be observed. Data, systems, and results must be regularly checked for distinction. To avoid distortions in the data sets, it is necessary to ensure that the training data is balanced.

3. Before using an AI solution, the legal admissibility and necessary limitations of AI must be clarified. The appointment of a systems administrator and an administrator for data protection regulations in relation to artificial

intelligence systems contributes. Thus, potential risks to individuals can be identified and mitigated at an early stage.

References

1. Ali, A. H., Abdullah, I. D., Aswad, A. R., Abdeldayem, M. M., & Aldulaimi, S. H. (2022). Human Rights and Artificial Intelligence: Evaluation of Legal Challenges and Potential Risk. *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2022*. https://doi.org/10.1109/ICETSIS55481.2022.9888888
2. Veale, M., & Zuiderveen, B. F. (2021). Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach. *Computer Law Review International*, *22*(4). https://doi.org/10.9785/cri-2021-220402
3. Buiten, M. C. (2019). Towards Intelligent Regulation of Artificial Intelligence. *European Journal of Risk Regulation*, *10*(1). https://doi.org/10.1017/err.2019.8
4. Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The New EU Cybersecurity Framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Review*, *35*(6). https://doi.org/10.1016/j.clsr.2019.06.007
5. Richard, B., Juan, J. C., & Javier, L. G. (2022, February 18). *State of Artificial Intelligence in Spain*. https://www.computing.es/analytics/estado-de-la-inteligencia-artificial-en-espana/
6. European Commission. (2018b). High-Level Expert Group on Artificial Intelligence. European Commission Digital Single Market Policy: https://ec.europa.eu/digital-singlemarket/en/high-level-expert-group-artificial-intelligence
7. Francisco, M. (2023). Artificial Intelligence for Environmental Security: National, International, Human and Ecological Perspectives. In *Current Opinion in Environmental Sustainability* (Vol. 61). https://doi.org/10.1016/j.cosust.2022.101250
8. Jamie, B., Heang, K. K., Clogher, R., & McBride, K. (2019). Hello, World: Artificial Intelligence and its use in the Public Sector. *OECD Observatory of Public Sector Innovation (OPSI)*, *36*.

9. Smuha, N. A. (2019). The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence. *Computer Law Review International*, *20*(4). https://doi.org/10.9785/cri-2019-200402
10. The Oxford English Dictionary, (n.d.). 'Artificial Intelligence' https://en.oxforddictionaries.com/definition/artificial_intelligence
11. Michael Negnevitsky. (2019). *Artificial Intelligence: A Guide to Intelligent Systems* (3rd Edition).
12. Moor, J. (2006). The Dartmouth College Artificial Intelligence Conference: The next fifty years. *AI Magazine*, *27*(4).
13. Wischmeyer, T. (2019). Artificial Intelligence and Transparency: Opening the Black Box. In *Regulating Artificial Intelligence*. https://doi.org/10.1007/978-3-030-32361-5_4
14. Stahl, B. C., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence: Protecting Fundamental Rights and Ethical Values. *Computer Law and Security Review*, *45*. https://doi.org/10.1016/j.clsr.2022.105661
15. Ortega, J., Profesor, & Martínez, J. (2020). *Inteligencia artificial*. https://www.researchgate.net/publication/346550856_Inteligencia_artificial
16. Mitrou, L. (2019). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3386914
17. Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., Maddikunta, P. K. R., Fang, F., & Pathirana, P. N. (2022). A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions. In *Future Generation Computer Systems* (Vol. 131). https://doi.org/10.1016/j.future.2022.01.017
18. Hupont, I., Micheli, M., Delipetrev, B., Gómez, E., & Soler Garrido, J. (2022). Documenting High-Risk AI: An European Regulatory Perspective. *TechRxiv*. https://doi.org/10.36227/techrxiv.20291046.v1
19. Ghillani, D. (2022). Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. *American Journal of Artificial Intelligence*, *x, No. x*. DOI: 10.22541/au.166379475.54266021/v1

20. European Commission. (2018a). Communication Artificial Intelligence for Europe https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF
21. Torens, C., Durak, U., & Dauer, J. (2022). Guidelines and Regulatory Framework for Machine Learning in Aviation. *AIAA Science and Technology Forum and Exposition, AIAA SciTech Forum 2022*. https://doi.org/10.2514/6.2022-1132
22. Sotala, K., & Yampolskiy, R. V. (2015). Responses to Catastrophic AGI Risk: A Survey. In *Physica Scripta* (Vol. 90, Issue 1). https://doi.org/10.1088/0031-8949/90/1/018001
23. Webb, M. (2019). The Impact of Artificial Intelligence on the Labor Market. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3482150
24. Sally, P. (2012). *ICM/WHO Global Standards for Midwifery Regulation*. Slideserve.Com.
25. Popenici, S. A. D., & Kerr, S. (2017). Exploring the Impact of Artificial Intelligence on Teaching and Learning in Higher Education. *Research and Practice in Technology Enhanced Learning*, *12*(1). https://doi.org/10.1186/s41039-017-0062-8
26. Aoki, N. (2020). An Experimental Study of Public Trust in AI Chatbots in the Public Sector. *Government Information Quarterly*, *37*(4). https://doi.org/10.1016/j.giq.2020.101490
27. Mania, K. (2022). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. In *Trauma, Violence, and Abuse*. https://doi.org/10.1177/15248380221143772
28. Justo-Hanani, R. (2022). The Politics of Artificial Intelligence Regulation and Governance Reform in the European Union. *Policy Sciences*, *55*(1). https://doi.org/10.1007/s11077-022-09452-8
29. Verheij, B. (2020). Artificial Intelligence as Law: Presidential Address to the Seventeenth International Conference on Artificial Intelligence and Law. In *Artificial Intelligence and Law* (Vol. 28, Issue 2). https://doi.org/10.1007/s10506-020-09266-0
30. Proposal for a Regulation of the European Parliament and of the Council. (2021). *Laying Down Harmonised Rules on Artificial Intelligence (Artificial*

Intelligence Act) and Amending Certain Union Legislative Acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

31. Regulations (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. (n.d.). *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) (Text With EEA Relevance)*. Retrieved June 14, 2023, from https://eur-lex.europa.eu/eli/reg/2016/679/oj
32. Ebers, M., Hoch, V. R. S., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. (2021). The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J*, *4*(4). https://doi.org/10.3390/j4040043
33. Stahl, B. C., Andreou, A., Brey, P., Hatzakis, T., Kirichenko, A., Macnish, K., Laulhé Shaelou, S., Patel, A., Ryan, M., & Wright, D. (2021). Artificial Intelligence for Human Flourishing – Beyond Principles for Machine Learning. *Journal of Business Research*, *124*. https://doi.org/10.1016/j.jbusres.2020.11.030
34. Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of Artificial Intelligence: A Risk and Guideline-Based Integrative Framework. *Government Information Quarterly*, *39*(4). https://doi.org/10.1016/j.giq.2022.101685
35. Hovy, E., Navigli, R., & Ponzetto, S. P. (2013). Collaboratively Built Semi-Structured Content and Artificial Intelligence: The Story so Far. *Artificial Intelligence*, *194*. https://doi.org/10.1016/j.artint.2012.10.002
36. Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (2013). Machine Learning: An Artificial Intelligence Approach. *Springer Science & Business Media, Berlin.*
37. Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2022). Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation. *Minds and Machines*, *32*(2). https://doi.org/10.1007/s11023-021-09577-4
38. Modgil, S., & Prakken, H. (2013). A General Account of Argumentation with Preferences. *Artificial Intelligence*, *195*. https://doi.org/10.1016/j.artint.2012.10.008
39. M. Tem Jones. (2008). *Artificial Intelligence: A Systems Approach*. Jones & Bartlett Learning, Infinity Science Press LLC.

40. Varshney, D. (2020). Digital Transformation and Creation of an Agile Workforce: Exploring Company Initiatives and Employee Attitudes. In *Contemporary Global Issues in Human Resource Management*. https://doi.org/10.1108/978-1-80043-392-220201009
41. Geetha, R., & Bhanu Sree Reddy, D. (2018). Recruitment Through Artificial Intelligence: A Conceptual Study. *International Journal of Mechanical Engineering and Technology*, *9*(7).
42. Koop, C., & Lodge, M. (2017). What is regulation? An Interdisciplinary Concept Analysis. *Regulation and Governance*, *11*(1). https://doi.org/10.1111/rego.12094
43. LEY DE INTELIGENCIA ARTIFICIA (2021, April,21). *Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL)* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN
44. Nayef, A.-R. (2015, August 12). *The Moral Code: How To Teach Robots Right and Wrong*. https://www.foreignaffairs.com/moral-code
45. Gael Churchill G. (2014). *European Union Regulations | European Encyclopedia of Law: Outline of the Community (European Union) Legislation about Regulations*. https://europeanlaw.lawlegal.eu/regulations/
46. Woll C. (2022, February 13). *"Regulation" Encyclopedia Britannica* . Https://Www.Britannica.Com/Topic/Regulation.
47. Djoneva B. (2018, October 16). *Human Rights and Technology: Impossible Union or Permanent Contradiction?* https://www.esglobal.org/derechos-humanos-y-tecnologia-union-imposible-o-contradiccion-permanente/
48. Neffa, J. C. (2006). Evolución Conceptual de la Teoría de la Regulación. In *Teorías sociales y estudios del trabajo: nuevos enfoques*.
49. Oren, E. (2018, December). Point: Should AI Technology Be Regulated?: Yes, and Here's How. *Communications of the ACM*, 30–32. https://cacm.acm.org/magazines/2018/12/232893-point-should-ai-technology-be-regulated/abstract

50. Ulnicane, I. (2022). Artificial Intelligence in the European Union: Policy, Ethics and Regulation. In *The Routledge Handbook of European Integrations*. https://doi.org/10.4324/9780429262081-19
51. Allen, T. C. (2019). Regulating Artificial Intelligence for a Successful Pathology Future. In *Archives of Pathology and Laboratory Medicine* (Vol. 143, Issue 10). https://doi.org/10.5858/arpa.2019-0229-ED
52. McKinsey Global Institute. (2019). *Artificial Intelligence in the United Kingdom: Prospects and Challenges*. https://www.mckinsey.com/featured-insights/artificial-intelligence/artificial-intelligence-in-the-united-kingdom-prospects-and-challenges
53. Schönberger, D. (2019). Artificial Intelligence in Healthcare: A Critical Analysis of the Legal and Ethical Implications. *International Journal of Law and Information Technology*, *27*(2). https://doi.org/10.1093/ijlit/eaz004
54. Coeckelbergh, M. (2019). Ethics of Artificial Intelligence: Some Ethical Issues and Regulatory Challenges. *Technology and Regulation*. https://doi.org/10.26116/techreg.2019.003
55. Sánchez, C. M. (2022). *Los Riesgos de la Inteligencia Artificial para el Principio del Igualdad y no Discriminación: Planteo de la Problemática y Algunas Aclaraciones Conceptuales Necesarias Bajo el Prisma del Sistema Interamericano de Derechos Humanos.* https://www.researchgate.net/publication/361510404
56. Taylor, C. R. (2019). Editorial: Artificial Intelligence, Customized Communications, Privacy, and the General Data Protection Regulation (GDPR). In *International Journal of Advertising* (Vol. 38, Issue 5). https://doi.org/10.1080/02650487.2019.1618032
57. Regulation General Data Protection. (2018). *General Data Protection Regulation (GDPR)* . Intersoft Consulting.
58. Miguel, R. (2019). *Spain's New Data Protection Law: More than Just GDPR Implementation*. https://iapp.org/news/a/spains-new-data-protection-law-more-than-just-gdpr-implementation
59. Houser, K., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3212210

60. Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., Hirschberg, J., Kalyanakrishnan, S., Kamar, E., Kraus, S., Leyton-Brown, K., Parkes, D., Press, W., Saxenian, A., Shah, J., Tambe, M., & Teller, A. (2016). Artificial Intelligence and Life in 2030 One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel. In *Stanford University*.
61. Núñez, Z., & Carmen, M. (2021). Los Nuevos Avances en la Regulación Europea de la Responsabilidad Civil por los Daños Ocasionados en el ámbito del Transporte con Inteligencia Artificial. *Revista Española de Derecho Europeo*, *78–79*. https://doi.org/10.37417/rede/num78-79_2021_636
62. European Commission. (2020). *White Paper on Artificial Intelligence A European Approach to Excellence and Trust*. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.
63. Dimitar Lilkov (2021). EU Artificial Intelligence Act: The European Approach to AI. A Risky Endeavour https://www.aipolicyconsulting.com/the-eu-s-new-rules-on-ai

64. Almeida, D., Shmarko, K., & Lomas, E. (2022). The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks. *AI and Ethics*, *2*(3). https://doi.org/10.1007/s43681-021-00077-w
65. Talib, M. A., Majzoub, S., Nasir, Q., & Jamal, D. (2021). A Systematic Literature Review on Hardware Implementation of Artificial Intelligence Algorithms. *The Journal of Supercomputing*, *77*(2), 1897–1938.
66. An, N., & Wang, X. (2021). Legal Protection of Artificial Intelligence Data and Algorithms from the Perspective of Internet of Things Resource Sharing. *Wireless Communications and Mobile Computing*, *2021*. https://doi.org/10.1155/2021/8601425
67. Hoofnagle, C. J., Sloot, B. van der, & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and What it Means. *Information and Communications Technology Law*, *28*(1). https://doi.org/10.1080/13600834.2019.1573501
68. Früh, A. ;, & Haux, D. (2022). Foundations of Artificial Intelligence and Machine Learning. *(Weizenbaum Series, 29). Berlin: Weizenbaum Institute for the*

Networked Society - The German Internet Institute. https://doi.org/10.34669/WI.WS/29

69. Eur-Lex Europe. (2018, May 25). *The general data protection regulation applies in all Member States*. Access to European Union Law. https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html
70. Wolff, J., & Atallah, N. (2021). Early GDPR Penalties: Analysis of Implementation and Fines through May 2020. *Journal of Information Policy*, *11*. https://doi.org/10.5325/JINFOPOLI.11.2021.0063
71. Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, *35*(4).
72. Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*. https://doi.org/10.6028/NIST.SP.1270
73. Sarrión, J. (2022). Smart Technologies and Fundamental Rights in the EU Multilevel System. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4130107
74. Varošanec, I. (2022). On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI. *International Review of Law, Computers and Technology*, *36*(2). https://doi.org/10.1080/13600869.2022.2060471
75. Kim, J. Y., & Heo, W. G. (2022). Artificial Intelligence Video Interviewing for Employment: Perspectives from Applicants, Companies, Developer and Academicians. *Information Technology and People*, *35*(3). https://doi.org/10.1108/ITP-04-2019-0173
76. Jarrahi, M. H. (2018). Artificial Intelligence and the Future of Work: Human-AI Symbiosis in Organizational Decision Making. *Business Horizons*, *61*(4). https://doi.org/10.1016/j.bushor.2018.03.007
77. Legg, S., & Hutter, M. (2007). Universal Intelligence: A Definition of Machine Intelligence. *Minds and Machines*, *17*(4). https://doi.org/10.1007/s11023-007-9079-x

78. Chatzipanagiotis, M., & Leloudas, G. (2020). Automated Vehicles and Third-Party Liability: A European Perspective. *SSRN Electronic Journal*, *2020*, 109–199. https://doi.org/10.2139/ssrn.3519381
79. Latimer, P., & Maume, P. (2015). Promoting Information in the Marketplace for Financial Services: Financial Market Regulation and International Standards. In *Promoting Information in the Marketplace for Financial Services: Financial Market Regulation and International Standards*. https://doi.org/10.1007/978-3-319-09459-5
80. Tarkowski, A., & Keller, P. (2021). Digital Public Space – A Missing Policy Frame for Shaping Europe's Digital Future. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3936353
81. Sartor, G., & Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *European Union*.
82. Peter Dizikes. (2016, June 23). *Driverless cars: Who gets protected?* MIT. https://news.mit.edu/2016/driverless-cars-safety-issues-0623
83. Taylor, M. (2016, October 7). *Self-Driving Mercedes-Benzes Will Prioritize Occupant Safety over Pedestrians*. https://www.caranddriver.com/news/a15344706/self-driving-mercedes-will-prioritize-occupant-safety-over-pedestrians/
84. Jeffrey, D. (2018, October 11). *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women.* Rutters . https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G
85. Gaumond E. (2021, June 4). *Artificial Intelligence Act: What Is the European Approach for AI?* Law Fare Blog. https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai.
86. Sousa, A. H. (2023). Non-Contractual Liability Applicable to Artificial Intelligence: Towards a Corrective Reading of the European Intervention. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4351910
87. European Commission Policy and Legislation. (2018, April 25). *Shaping Europe's Digital Future: Elements of the European Data Economy Strategy 2018*. https://digital-strategy.ec.europa.eu/en/library/elements-european-data-economy-strategy-2018

88. Tom, D. (2021, October 18). *Effective AI Risk Mitigation Relies on Identification and Prioritisation*. Digital Nation. https://www.digitalnationaus.com.au/news/effective-ai-risk-mitigation-relies-on-identification-and-prioritisation-571414
89. Kevin, B., Rachel, D., Liz, G., & Alex, S. (2021). Getting to Know - and Manage Your Biggest AI Risks. *Mckinsey and Company* https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it
90. Porcheddu, D. (2023). The Role of Trade Unions in the Processing of Workers' Data: Insights from A European Unionco-Funded Project. *englishbulletin.adapt.it.* The role of trade unions in the processing of workers' data: insights from a European Union co-funded project | English Bullettin (adapt.it)