UNIVERSITÀ
DI PAVIA

Dipartimenti di Giurisprudenza, Ingegneria industriale e dell'informazione,
Scienze economiche e aziendali, Scienze politiche e sociali, Studi umanistici

Corso di laurea interdipartimentale in
Comunicazione Digitale

Navigating the Intersections of AI and Data Protection: A Comparative Analysis of the EU and U.S. Approach to Healthcare

Relatore:
Chiar.mo Prof. Alfredo Sassi

Correlatore:
Chiar.mo Prof. Emanuele Tuccari

Tesi di laurea di
Anja Pellizzari
Matricola n. 518819

anno accademico 2023/2024

Table of Contents

Abstract

The 21st century has been characterized by major technological innovations that reshaped our daily lives, habits, and the way we interact. The improvements in computational power and the availability of big data made possible the development of artificial intelligence (AI), which, in recent years, has been incorporated into an increasingly higher number of devices and systems in a wide range of fields. The potential of AI largely relies on the availability of data, which are extracted from individuals' interaction with digital devices, online platforms, and multiple sources that collect our data and utilize them to train algorithms and extract valuable information. However, the dependence on physical persons' data poses ethical, privacy, and safety concerns that governments worldwide are called to address.

With this study, we explore the current main applications of AI and its future potential developments, as well as the concerns emerging from its reliance on data. By doing so, we will explore how the European Union addresses these modern issues through law regulation, and compare it to the United States' approach to these topics. The focus will then shift to the healthcare domain, exploring the EU and US current state and the challenges resulting from their approach to the handling of health data. This study outlines how crucial it is to ensure subjects' privacy and data protection, but also how stringent regulations could potentially lead to stagnant landscapes in terms of technological innovation, highlighting the importance of finding a balance between privacy and progress.

Chapter 1:

Overview of Artificial Intelligence

1.1 Introduction

In recent years, artificial intelligence (AI) has seen rapid growth and a vast application in multiple fields. We can undoubtably affirm that AI technologies have simplified many of our daily tasks. The most resounding example is ChatGPT. This form of machine intelligence is already being used by thousands of individuals for their day-to-day tasks, and has helped simplifying even the most basic actions or decisions. ChatGPT can be used for basically everything that requires some kind of mental effort, such as planning your groceries shopping list, finding information on new destinations, or helping with your homework.

Another recent machine intelligence technology made available to users is Generative AI. This technology is able to transform text input into a completely new image based on a training dataset that is constantly being updated with new information. However, these new technologies present some backlashes as well. AI has been increasingly used to create deep-fake content, such as videos and audio files, posing concerns and ethical issues about its consequences on society and public trust.

For most of us, the potential of these new technologies is mind blowing and has created an unmatched level of excitement. As Joshi (2024)[1] explained, the notion of AI is not completely new to the general public: movies like the Matrix series or Terminator introduced this concept already in the early 2000s. This kind of movie depicts the future of AI in two very different ways. Joshi (2024) states that on one

[1] Ameet Joshi; *Artificial Intelligence and Human Evolution: Contextualizing AI in Human History*; New York; Springer Science; 2024.

hand, we see a bright future in which this technology helps us humans by taking over boring and alienating tasks. On the other hand, he continues, the depicted consequences of AI are not as optimistic: this technology is painted as an evil force that will ultimately become superior to the human race and treat people with hostility by taking control of the world.

As of today, AI remains completely under humans’ control and the risk of it taking over people is nonexistent. In his book, Ameet Joshi (2024) states that:

“

> AI cannot function without humans turning the power switch on and AI cannot reproduce itself. So even if potentially capable of doing more than humans, AI does not have free will as of today”[2].

To better comprehend the outbreak of this technology, it is necessary to know its history, how it started and how it has been evolving in the latest centuries.

1.2 The Evolution of AI

Even if only in recent years the general population has been able to access various forms of artificial intelligence technologies, these can be dated back to the late twentieth century when this concept arose as a completely new term. However, we can find some even earlier and primitive examples of machine intelligence in ancient and modern history.

[2] Ameet Joshi; *Artificial Intelligence and Human Evolution: Contextualizing AI in Human History*; New York; Springer Science; 2024; p. 2.

1.2.1 Early Examples

Some people argue that the leap towards a machine that is able to respond and adapt to the changes in its surroundings can be dated back to the ancient Chinese Han Dynasty in 200 BCE when a chariot was built with a figurine that would always point South regardless of where the chariot turned (Joshi, 2024). This example can be accepted as a primitive form of machine intelligence if we stand by the definition of the so-called ‘feedback mechanism’. Joshi (2024) explains it as the basic feedback all the living species use since birth and during all their life when interacting with the environment through their sensory organs, and reacting to it. Another early example is the ancient Greek Antikythera constructed around 100 BCE and used to perform astronomical predictions and calculations (Joshi, 2024). But there are more examples in later history. Leonardo da Vinci is considered as one of the greatest engineers in history and many of his inventions contributed to the development of devices and machines that are still used nowadays. He also played an important role in creating feedback enabled machines, such as a water wheel that could maintain its rotational speed even with variations in the flow of water (Joshi, 2024).

1.2.2 Industrial Revolution

The first widely recognized achievement in creating mechanical feedback machines capable of reacting to their surroundings and adapting to it can be dated back to the Industrial Revolution in the late 18th century (Joshi, 2024). During 1800, Great Britain was the leading country in terms of innovation and production, and it is here where many technological innovations first appeared. One of the most remarkable inventions of this period is the improvement on the steam engine developed by James Watt: Joshi (2024) describes it as “a monumental leap for humankind that took us into a new era of smart machines that had the concept of feedback and self-regulation mechanism built into them" (Joshi, 2024, p.113). This type of engine allowed the vehicle to function by converting the heat energy released from burning coal into mechanical energy for each part of the machine; moreover, Watt introduced a feedback mechanism called 'centrifugal governor' that enabled the engine to automatically regulate its speed and maintain it constant (Joshi, 2024). The centrifugal governor used by Watt basically consisted of a rotating spindle and two weighted arms attached to it that relied on the centrifugal force to adjust to the movement (Joshi, 2024). This governor was crucial as it offered a self-regulating system able to control the engine's speed regardless of the outside conditions (Joshi, 2024). These mechanical sensors implemented by Watt represent the first steps toward the creation of a machine that is able to adjust and adapt to the changes in its surroundings, and constitute the very first steps toward what we call today 'machine intelligence'.

1.2.3 AI in the Past Decade

In their article, Shao et al. (2022)[3] discuss the evolution of AI during the past decade starting off by dividing its development into three stages[4]: Symbol AI or Knowledge-driven approach; Data-driven approach based on deep learning; and Third Generation AI combining the first two stages.

The origin of the discussion about AI can be traced back to the 1940s and 50s when neurological studies first showed that "the brain is a neuronal neural network that emits with or without pulses" (Shao et al., 2022, p. 2). These findings triggered the curiosity of multiple scientists who began to question the possibility of creating an artificial brain that imitates the human one. The gateway to artificial neural networks

[3] Zhou, Shao; Ruoyan, Zhao; Sha, Yuan; Ming; Ding; Yongli, Wang; *Tracing the evolution of AI in the past decade and forecasting the emerging trends*; in "Expert Systems with Applications"; Elsevier; 2022.

[4] Z., Shao; R., Zhao; S., Yuan; M., Ding; Y., Wang; *Tracing the evolution of AI in the past decade and forecasting the emerging trends*; cit., p. 1.

was made possible by neurologist Warren McCulloch and mathematician Walter Pitts who published a book in which they combine algorithms and simulations of human thinking activities (Shao et al., 2022).

An important contribution to artificial intelligence arrived in 1950 from the British mathematician and computer scientist Alan Turing, who is still considered as one of the pivotal figures in this field and a pioneer in machine learning. In this year, Turing publishes his article 'Computing Machinery and Intelligence' where he first introduces his famous Turing Test through which it was possible to determine if a machine could be considered intelligent based on a series of questions and answers with another party, but with no interaction between the two (Shao et al., 2022). After the test, if the other party was able to determine whether he was interacting with a human or a machine, then the computer could be considered as to be able to think (Shao et al., 2022, p.2).

The official birth of AI is generally considered to be in 1956 when this term was formally used for the first time by John McCarthy during a seminar dealing with the use of machines to simulate human intelligence at Darthmouth College, which is widely accepted as marking the birth of AI (Shao et al., 2022). In the following years, the development of AI continued with milestones such as the system 'Student' by Daniel Bonrow in 1964 that could understand natural language input, and 'Eliza', the first computer program by Joseph Weizenbaum that could communicate with humans, representing the starting point for modern chatbots (Shao et al., 2022).

However, after this first wave of enthusiasm and climax for AI, during the 70s its development encountered the first technical difficulties. In their article, Shao et al. (2022) explain that:

“

> The limited memory and processing speed of computers were not enough to solve any practical AI problems. This period is usually called "the first AI winter" and it lasted until the end of the decade. No one could make a huge database back then, and the research progress came to a standstill"[5].

Moreover, computer developers experienced a shortage of government funds which led to an increasing disinterest in AI (Sharma and Garg, 2021)[6].

The second wave of AI begins in the 1980s but has its most important developments in the 1990s. The first one is the introduction of the semantic web in 1998 by Tim Berners-Lee that aimed to make the data on the internet more understandable to computers by implementing a semantic-based knowledge network that would extend the meaning of human requests which, up to that moment, was only limited to keywords (Shao et al., 2022). Later on, Edward Feigenbaum introduced a system that imitates the decision-making process of human experts: the Dendral expert system (Shao et al., 2022). Another crucial development based on knowledge and experience in AI history is the chess program Deep Blue by IBM. This program was designed to process up to 200 million possible moves in only one second, and also establish the best next move looking 20 moves ahead (Shao et al., 2022); with this sophisticated system based on a simulation of human intelligence behavior, Deep Blue was able to defeat the world champion of chess, Garry Kasparov, in 1997 representing a milestone in AI and computational computing.

The arrival of deep learning marked the beginning of the third wave of AI characterized by the increasing incorporation of AI-related topics and technologies into people's lives, and the arrival of open platforms like OpenAI (Shao et al., 2022).

[5] Z., Shao; R., Zhao; S., Yuan; M., Ding; Y., Wang; *Tracing the evolution of AI in the past decade and forecasting the emerging trends*; cit., p. 3.

[6] Lavanya, Sharma; Pradeep Kumar, Garg; *Artificial Intelligence: Technologies, Applications, and Challenges*; 1st Edition; New York; Chapman and Hall/CRC; 2021.

This new wave brought tremendous progress in society as people are gradually incorporating AI into their lives, and companies into their systems. A popular example of AI starting to make appearance into people's houses is the introduction of the vacuum cleaner AI Roomba in 2002 (Sharma and Garg, 2021).

The reason behind the success of deep learning in many areas of AI can be attributed to three main driving factors: data availability, computing powers, and algorithm design (Shao et al., 2022). Deep learning can use a large amount of data, and this is what makes it stand out from traditional machine learning. These data are then used to improve its performance and accuracy.

1.3 Definitions of AI

Ever since researchers and innovators started discussing the implementation of artificial intelligence, its main goal was to be at the service of people and facilitate their daily tasks, especially the most repetitive and boring ones. For these reasons, experts have been trying to develop a machine able to simulate the actions and thinking process of human beings. These attempts gave rise to artificial intelligence as we know it today, whose aim is to think, work and behave like a real person. In his book about AI (Sharma and Garg, 2021), Pradeep Garg illustrates the definition of artificial intelligence given by McCarthy stating that it is:

"

> A science and a set of computational techniques that are inspired by the way in which human beings use their nervous system and their body to feel, learn, reason, and act"[7].

[7] L., Sharma; P. K., Garg; *Artificial Intelligence: Technologies, Applications, and Challenges*; cit., p. 3.

AI is artificial because it’s human created, and intelligent because it has the ability to learn from experience, find analogies, elaborate datasets, solve and comprehend different kinds of problems, and adapt to new surroundings (Sharma and Garg, 2021). The availability of large amounts of data is crucial for AI to be able to operate properly. This is because, unlike human beings who can process and learn smaller amounts of data, AI systems need larger datasets to discover relationships and find analogies. AI speeds up the process of getting information from the data while also using minimum effort. John McCarthy, the father of AI, defines it as “a branch of computer science by which we create intelligent machines which can think like human, act like human, and able to make decisions like human” (McCarthy, 2019, pp. 2-3)[8].

The emergence of AI technologies into people’s everyday lives sparkled both interest and concern. Most people are still not aware of the real potential AI holds to improve the quality of our experience in multiple fields, from healthcare to education, from entertainment to banking and so on. The comparison between human intelligence and the potential of AI raised some questions among people about what the risk of future improvements in this technology could look like. First, it is important to specify that AI is still completely controlled by humans and cannot turn itself on or off. Moreover, it is not able to reproduce itself so, even if its potential can be greater than that of any person, it still cannot be seen as independent and as having free will (Joshi, 2024). These two conditions are the reason why there is still no reason to fear AI; however, if this technology was to acquire these capabilities, it could potentially become harmful and turn itself against humans.

[8] McCarthy, John; *Artificial Intelligence Tutorial – It’s your time to innovate the future*, Dataflair Team, 27 November 2019 (Available from: https://data-flair.training/blogs/artificial-intelligence-ai-tutorial/).

1.4 Market Potential of AI

The aim of AI is to simulate human intelligence by creating machines that can think like humans. AI is currently being utilized in multiple and very different fields. Its potential to supplement human abilities can be seen as a valuable partnership between technology and humans to ensure better performances in terms of accuracy, speed and reliability. In their book, Sharma and Garg (2021, pp.6-7) list some of the opportunities that the human-AI partnership can offer. Among these, it provides further support for humans' abilities allowing better understanding and perception; it can bridge the language and economic barriers; it can build intelligent systems capable of providing interactive communication between AI systems and humans.

In the past few years, more and more industries have started relying on AI to enhance their performance by implementing this type of technology into their systems. AI is currently being used in the automobile industry, in military planning, airport security and entertainment just to mention a few. The following are some of the areas that are projected to benefit the most from the application of AI (Sharma and Garg, 2020, pp.14-15):

1.4.1 Healthcare

The partnership between AI and doctors is expected to drastically reduce the percentage of errors, providing patients with faster recovery and early discovery of medical conditions. Thanks to technologies such as object recognition and image classification, the machine will be able to detect details that are not visible with the naked eye, helping with more accurate and faster diagnosis. AI is not going to replace humans in their job, but it will complement their abilities for a better outcome. An example is the progressive use of robots assisting surgeons in the operating room. In the 'Artificial intelligence in healthcare' study by the European Parliament (2022, p.5) it is explained that “AI has progressively been introduced into virtually all areas of medicine, from primary care to rare diseases, emergency medicine, biomedical research and public health”[9]. The study also explains how AI can be used in healthcare management as well to increase efficiency and quality.

1.4.2 Education

AI can be used in this field to assist students by adapting the learning experience and content to each one of them and their specific needs; it can also assist teachers with automatic examination grading systems. Some of the benefits of the implementation of AI in education include personalization based on the student’s needs; tutoring through customized support; feedback on course quality to help educators make improvements accordingly; meaningful feedback to students[10]. Even in education, AI is not meant or projected to replace human beings, but its aim will be to assist them and make them save time to dedicate to other tasks that AI cannot help with. With the emergence of AI, new technologies have become available to the majority of the population. An example worth mentioning is ChatGPT by OpenAI: this is an AI powered chatbot that allows the user to complete tasks in a conversational way. The user will simply write his or her request, and ChatGPT will answer providing help even with the composition of emails, codes or essays, or just with coming up with a title for your paper or a catchy quote for your social media post.

[9] EPRS-European Parliamentary Research Service, *Artificial intelligence in healthcare: Applications, risks, and ethical and societal impacts*, in “European Parliament”, June 2022 (https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf Accessed on 20/06/2024).

[10] University of San Diego, *43 examples of Artificial Intelligence in Education*, in “Artificial Intelligence” (https://onlinedegrees.sandiego.edu/artificial-intelligence-education/ Accessed on 21/06/2024).

1.4.3 Transportation and Travel

AI is already being used in this industry to estimate flight delays, make travel arrangements, and find the best routes or prices for hotels and plane tickets. Some of its latest applications in transportation include the enhancement of safety measures and urban mobility by analyzing traffic flows, and an early detection of anomalies in it (Lungu, 2024)[11]. Important advancements have been made in the field of self-driving vehicles which are able to drive themselves and recognize obstacles, detect pedestrians, adjust their speed, and make up for any possible distractions of the driver.

1.4.4 Retail

Some large industries in retail have started experimenting with new ways to make the customer experience more engaging and personalized for their clients. One of the most popular examples are Amazon's purchase recommendation systems that suggest complementary items to add to the cart based on the purchasing history and research and what other customers purchased. Another example from Amazon of AI applied to retail is the new Amazon Go. Amazon Go is a new kind of grocery store with no checkout line or scanning item procedure. What makes this store different than others, according to Amazon website, is that:

"

> It is powered by Amazon's Just Walk out shopping which lets you skip a traditional checkout when you pay with your Amazon app (or through a payment method that's already tied to your account)"[12].

[11] Mihai Adrian, Lungu; *Smart Urban Mobility: The Role of AI in Alleviating Traffic Congestion*, in "Sciendo", 2024, DOI: 10.2478/picbe-2024-0118

[12] Amazon, *Amazon Go* (https://www.amazon.com/b?ie=UTF8&node=16008589011 Accessed on 20/06/2024).

The Amazon Go web page explains that when an item is taken off the shelf, a series of sensors register this movement and automatically add the item to your virtual cart; the same process happens when anything is put back on the shelf.

Another important example of AI in retail are smart mirrors. A smart mirror is an interactive device that, with the use of AI, offers the user an engaging and innovative experience when shopping. The possibilities of use for this kind of device are multiple: it can display digital information such as date and weather, news and calendar reminders, but also assist customers when shopping by filtering offers for personalized products and virtual try-on options[13]. Smart mirrors can fulfill various roles including advertising, entertainment and health-related services such as body temperature measurement and examination of skin conditions[14]. AI in retail can look like chatbots for customer assistance, interactive devices to enhance the user experience, recommendation engines and trend predictions, but also robots helping with human tasks.

1.5 Challenges of AI

As we already mentioned, the implementation of AI and its large-scale usage is not always as smooth. AI is a human machine system that can only function with inputs given by humans; for this reason, the quality of its performance depends on the quality and quantity of data available in the datasets these technologies and algorithms are trained on (Sharma and Garg, 2021).

AI can bring challenges also in the workplace. In 2024, Deloitte published a report called ‘AI can cut costs, but at what cost to the workforce experience?’ (Dunlop et al.,

[13] Kamil Puk, *How Smart Mirrors are Transforming In-Store Experiences*, in “Netguru”, February 27th 2024 (https://www.netguru.com/blog/smart-mirrors-in-retail Accessed on June 21/06/2024).
[14] Ibid.

2024)[15]. As the report shows, in November 2023 “only 10% of leaders indicated that they currently use AI often to make decisions, and 74% of leaders anticipate using AI often for decision-making within the next five years” (Dunlop et al., 2024, p. 1). The developments of AI have increased its capabilities in terms of decision-making, problem solving and processing; however, the importance of the human workforce is not to be underestimated. The fear of losing job places to these new technologies is one of the reasons for the concerns around AI. In a world in which price reduction is the priority for companies, the time and money saving aspect brought by AI capabilities is a threat for those working in creative industries and production compartments (Dunlop et al., 2024). The uncertainty around one’s job has an impact over his or her motivation and overall satisfaction, which ultimately impacts on the percentage of turnover (Dunlop et al., 2024). Many are afraid of being replaced by AI-enabled machines in their jobs; there is a possibility that this will happen for certain types of jobs, but humans will still be needed to oversee and manage the work of the machine, for maintenance and development which will ultimately create new job positions (Dunlop et al., 2024).

Another tension challenging the implementation of AI is the concern regarding data privacy and security. As we already mentioned before, AI systems are trained on large datasets of data that might be sensitive and personal. This exposes individuals and businesses to the risk of data theft, data breach, and also negative impacts on human rights; the data being collected can be about both individuals and groups, and they usually regard marketing trends, searching history, and their location (Sharma and Garg, 2020, p.233). This type of data can be collected automatically by devices or with technologies that require this type of input data to function, such as visual recognition; the data is then processed and shared for specific purposes. When the

[15] Amelia, Dunlop; Charlie, Woodward; Saie, Ganoo; *AI Can Cut Costs: But at What Cost to the Workforce Experience?* Netherlands; Deloitte Digital; Natter; 2024.

data collected is being used for commercial purposes, the threat for privacy is relatively low, but other types of uses can have more serious consequences. The potential power of AI also poses risks of unethical use and amplified biases (Dunlop et al., 2024). For these reasons, many governments have already taken action to regulate the usage of data and the practices of data collection. A noteworthy example is the General Data Protection Regulation (GDPR) implemented by the European Union to ensure the full protection of citizens' personal data.

1.5.1 Advantages and Disadvantages of AI

Despite the great benefits brought into society by AI technologies, they also come with some disadvantages. In their book, Sharma and Garg (2021) discuss both the advantages and disadvantages of AI as follows below.

The advantages of AI are higher in number compared to the disadvantages, and, according to Sharma and Garg (2021) they include:

1. Accuracy: AI-based machines drastically reduce human errors by pattern and trend recognition. When data is captured automatically and not manually into the system, the possibility of manual error is eliminated resulting in high accuracy.
2. Speed: AI systems can make predictions, analysis and decisions faster than any human being. This factor significantly reduces working times and speeds up the process. Moreover, these machines can work continuously without any break for long periods of time.
3. Better decision-making: the decision-making process can often be affected by the feelings and emotions of the people involved in the decision; this can also include personal biases and prejudices resulting in an unfair decision. AI-enabled machines eliminate all these factors and ensure the most optimal decision and solution in all cases.

4. Reliability: the elimination of any kind of personal bias and the high accuracy of AI guarantee high and unchanging reliability of these systems.
5. Multitasking: AI systems are able to handle several tasks simultaneously, and to optimize the use of resources. The same degree of focus is given to every single task indistinctly, even when processing large amounts of data.
6. Working in risky areas: “AI-equipped machines are very useful in actions that are hazardous to humans, such as defusing a bomb, exploring the nuclear sites, cleaning up a toxic spill” (Sharma and Garg, 2021, p.13).

The disadvantages of AI mentioned by Sharma and Garg (2021) include:

1. Costs: the costs for AI systems can be very high for both the hardware and the software. They also require frequent maintenance and updates which can be very costly. In some cases, even the processing of data can require large expenses.
2. No creativity/originality: this disadvantage applies particularly to Generative AI, a subset of AI which is utilized to create new content. The content generated is based on information already available, therefore already created by somebody else. AI simply uses the information from the datasets to create new content, but there’s no creativity or originality involved. AI machines are not able to think out-of-the-box or work out of context, they can only perform based on what they have been trained on. On the contrary, human intelligence can be creative and always have new ideas if properly stimulated.
3. No feelings/emotions: even if this is considered as an advantage, in most case scenarios, it can sometimes turn into a disadvantage if the machine is not properly used by the user.
4. Dependency on machines: Sharma and Garg (2021) explain this disadvantage as mainly applicable to humans. When everything can be easily delegated to a machine, human mental capabilities are not stimulated enough, and the person tends to get progressively lazier. Nowadays, people depend on their devices for

many daily tasks, even the most basic ones. AI and technology in general should be utilized in a way that does not make us dependent on machines.

Chapter 2:

The EU AI Act and AI Applications

2.1 The EU AI Act

The global race to AI gave raise to competition and huge investments in developed countries, but it also brought along issues and concerns with resonance worldwide, calling Governments into action. Considering the potential that the implementation of AI can have on a Country's economy, gaining leadership in this field is set to be one of the biggest challenges for the future. The effort is not only technological and financial, but it also encompasses various dimensions; among these, trustworthiness is considered by current literature as the most remarkable one, also in terms of impact on citizens and society in general.

2.1.1 From the Proposal to the Act

The urgency to address the emerging trend of AI can be traced back to 2017 when the European Council included the issue of artificial intelligence into its priorities, while also placing it side by side with the related issues of data protection and ethical standards (European Commission, 2021, p. 2)[16]. From this point, the Council made ensuring the respect of European citizens' its priority. The relevant legislation concerning digital rights and all the fields currently and potentially impacted by artificial intelligence have been reviewed starting from 2019 to face the new challenges brought into society by the development of AI. From this year forward,

[16] European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*, Brussels, 21.04.2021, Brussels, 2021, p. 2

ensuring the protection of European citizens' rights in the context of artificial intelligence and its implementation has been a top priority in the context of the European Union.

President Von Der Leyen expressed her commitment and the necessity for a harmonized and coordinated approach to the implications of AI in her political guidelines for the 2019-2024 Commission (European Commission, 2021) giving a clear sign of the importance of this matter for the future. Later, on February 2020, the Commission published the White Paper on AI which "sets out policy options on how to achieve the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology" (European Commission, 2021, p. 1)[17]. The focus point of the Proposal was to develop a legal framework that would ensure the trustworthiness of AI and its applications to achieve support among both regular users and business organizations. The ultimate aim of AI is to make people's lives easier and serve their goals in an efficient, accurate and safe way. To achieve this aim, it is necessary to gain people's trust by proving the trustworthiness of these technologies while also showing the risks and how to prevent them from happening. The implementation of a specific legal framework for a trustworthy artificial intelligence based on EU values and fundamental rights aims to give citizens "the confidence to embrace AI-based solutions, while encouraging businesses to develop them" (European Commission, 2021, p. 1)[18].

In April, 2021, the European Commission published the Proposal for a "Regulation of the European Parliament and of the Council - Laying down harmonized rules on Artificial Intelligence (AI Act) and amending certain Union Legislative Acts". The proposal responds to the increasing requests coming from the European Parliament

[17] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ..., cit., p. 1
[18] Ivi, p.1

and Council for appropriate legislation that would address both the benefits and especially the risks of artificial intelligence systems, so that the growing market created by AI could thrive in the respect of human fundamental rights (European Commission, 2021, p. 1)[19]. These requests support the mission of the European Union of becoming a global leader in the market, not only by improving and developing AI related technologies, but also by ensuring that this progress will be based on a technology that is secure, ethical and trustworthy.

As stated on the official document of the Proposal, the main objectives of the regulation of AI are:

“

1. Ensuring that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
2. Ensure legal certainty to facilitate investment and innovation in AI;
3. Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
4. Facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation”.[20]

The legal intervention introduced with the regulation sets a comprehensive framework for the future that is designed to approach the consequences and possibilities created by AI with an approach that is risk-based. This approach avoids unnecessary restrictions that could hamper future developments in the field and the possibility for the Union to gain global leadership in AI. The legal intervention introduced with the Proposal “sets harmonized rules for the development, placement on the market and

[19] Ibid.

[20] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ..., cit., p. 3

use of AI systems in the Union following a proportionate risk-based approach" (European Commission, 2021, p. 3)[21]. The application of the rules contained in the Proposal will be enforced by every single Member State individually by adapting the governance system to the already existing structures (European Commission, 2021). The official Proposal also introduces a European Artificial Intelligence Board that will manage the cooperation mechanisms between the Member States. The rules and measures are not only meant to regulate AI and its applications, but they also aim to support innovation and research in this field, in particular with tailored measures for Small and Medium-sized enterprises (SMEs) and start-ups that operate with AI systems (European Commission, 2021). To sum up, we could say that one of the main objectives of the Proposal is to both regulate and support innovation of AI technologies.

In 2021, the area of biometric techniques applied to AI was taken into consideration in the context of the Proposal. In August 2021, the European Parliament's Policy Department for Citizens' Right and Constitutional Affairs commissioned and published a study regarding the use of biometric techniques applied to AI systems from both a legal and ethical perspective (FLI, 2024)[22]. Four months later, the EU Council shared a:

"

> first compromise text on the AI Act draft with major changes in the areas of social scoring, biometric recognition systems, and high-risk applications. The degree of risk of any AI application has been a focus point in the definition of this proposal, marking whether an area of application needed a strict regulation or not" (FLI, 2024)[23].

[21] Ibid.

[22] Future of Life Institute FLI, *Historic Timeline*, in "EU Artificial Intelligence Act", 2024 (https://artificialintelligenceact.eu/developments/, Accessed on 09/08/2024).

[23] Ibid.

At the end of 2022, the Council of the EU agreed on the adoption of its common position on the AI Act, but it was only in the June of 2023 that if finally adopted its negotiating position on the Act with 499 votes in favor, 28 against, and 93 abstentions (FLI, 2024). This led to a provisional agreement between the Parliament and the Council on the AI Act in December 2023.

In February 2024, the EU's 27 Member States finally reached a unanimous agreement further affirming the position assumed only a few months earlier, leading to the official endorsement of the AI Act. On May 21st, 2024, the European Council formally adopted the EU AI Act, and on July 12th the Act was officially published in the Office Journal of the European Union (FLI, 2024) where it is now available for consultation.

The Act consists of twelve chapters, and each one of them contains a set of articles that further explain its content. Alongside with the text of the Act, thirteen annexes were published to provide supplementary information.

2.1.2 Trustworthiness and Acceptability of Risks in the AI Act

In the European Union AI Act, the trustworthiness of AI is intended as the acceptability of its risks (Laux et al., 2024)[24]. Developing trustworthy AI has been the objective of the Union in the making of its policies. The aim of this emphasis on trustworthiness is to "induce people to place trust in AI so that they will use it more and, hence, unlock the technology's economic and social potential" (Laux et al., 2024, p. 1)[25]. The AI Act is the result of years of consultation between the Member States and the European Council and Parliament, whose purpose was to both promote the uptake of AI and its use, but also to address the risks that come with its development

[24] Laux, Johann; Wachter, Sandra; Mittelstadt, Brent; *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, in "Regulation & Governance", 2024, pp. 3-32

[25] Ibid.

and application. The importance of trustworthiness is stated explicitly also in the 2020 White Paper in which it is defined as a prerequisite for AI broad adoption in Europe, and its lack would hold back any possible broader uptake in the future (Laux et al., 2024).

The AI Act adopts a risk-based approach based on stricter rules where the potential risk for individuals and society is greater. AI risk types are divided into four main categories: unacceptable risk, high-risk, limited risk, and minimal risk. The first category, unacceptable risk, such as social scoring systems and manipulative AI, is completely prohibited (FLI, 2024)[26]. Chapter II, Art. 5, of the AI Act addresses Prohibited AI systems describing them as follows:

“

- Deploying […] techniques to distort behaviour and impair informed decision-making, […].
- Exploiting vulnerabilities related to age, disability, or socio-economic circumstances […].
- Biometric categorisation systems inferring sensitive attributes […].
- Social scoring, […], causing detrimental or unfavourable treatment of those people.
- Assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, […].
- Compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage.
- Inferring emotions in workplaces or educational institutions, […].
- ‘Real-time’ remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except when: searching for missing persons, […]; preventing

[26] Future of Life Institute FLI, *High-level summary of the AI Act*, in “EU Artificial Intelligence Act”, 2024 (https://artificialintelligenceact.eu/high-level-summary/, Accessed on 12/08/2024).

> substantial and imminent threat to life, […]; or identifying suspects in serious crimes […].”[27]

The second category, which is High-risk AI systems, is the one the Act mainly focuses on. The risk concerns potential threat to fundamental rights, safety, health, democracy or environment which require strict regulation. As the AI Act text states, the majority of regulations regard providers and developers who intend to put on the market or offer high-risk AI systems services in the EU, regardless of where they are based (FLI, 2024). This also includes third-country providers whose systems are used in the EU. As the AI Act's website states, “AI systems are always considered high-risk if they profile individuals, i.e. automated processing of personal data to assess various aspects of a person's life, […]” (FLI, 2024)[28]. As previously mentioned, the requirements that fall on providers of this type of AI system are multiple, and they aim to ensure the safety of their users and the protection of their data. In particular, they must establish a risk management system and a quality management system to comply with the regulations, but also conduct data governance on the datasets utilized, design record-keeping systems to achieve traceability, cybersecurity and accuracy (FLI, 2024). Compliance to regulations will have to be demonstrated through technical documentation, and human oversight over the activity of high-risk AI systems is mandatory. As the AI Act text states:

“

> High-risk AI systems should only be placed on the Union market, put into service or used if they comply with certain mandatory requirements. Those requirements should ensure that

[27] Future of Life Institute FLI, *High-level summary of the AI Act*, in “EU Artificial Intelligence Act”, 2024 (https://artificialintelligenceact.eu/high-level-summary/, Accessed on 12/08/2024).

[28] Ibid.

> high-risk AI systems […] do not pose unacceptable risks to important Union public interests as recognised and protected by Union law" (AI Act, 2024, p.33)[29].

The third category mentioned in the Act is limited risk AI systems which are subject to a lighter regulation: these include chatbots and deepfakes for which the end-user must be informed that he or she is interacting with AI (FLI, 2024). This category of systems is considered to represent a certain degree of risk, but it is manageable enough to not require strict regulation. The Act imposes transparency requirements on developers of limited-risk AI systems: user awareness is fundamental when the interaction with this type of system can potentially influence the decisions or outcomes of the individual's actions. The most relevant examples of such systems are chatbots and virtual assistants that interact with users in a conversational way.

Lastly, the fourth category is minimal risk AI systems which do not represent a threat for users' safety or rights and, therefore, are not regulated. This category includes applications that have little to no significant impact on individuals, and are subject to minimal restrictions and regulations[30]. Although the Act doesn't impose stringent obligations to the developers of these systems, they are still encouraged to adopt ethical and transparent practices and codes of conduct. Examples from this category include certain types of AI-driven games, and basic content or products recommendation systems.

[29] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement*, Brussels, 26.01.2024, Brussels, 2024, p. 33

[30] Future of Life Institute FLI, *High-level summary of the AI Act*, in "EU Artificial Intelligence Act", 2024 (https://artificialintelligenceact.eu/high-level-summary/, Accessed on 12/08/2024).

2.2 Key Fields of AI Application

Artificial intelligence is revolutionizing a wide range of sectors, bringing innovation and new applications of these systems. The EU AI Act identifies several fields where its impact is particularly profound, and where AI systems are considered high-risk for the potential significant impact they could have on citizens' fundamental rights, decision processes, and freedom. Due to the potential consequences of these systems on individuals, the EU AI Act emphasizes transparency, accountability, and fairness, ensuring that AI technologies are used responsibly while promoting innovation and efficiency. The followings are some of the key areas of application of AI systems that are experiencing the most dramatic improvements and changes.

2.2.1 Healthcare and Medical Devices

The area of healthcare services is classified as high-risk according to the AI Act. The access and enjoyment of this type of service represent a fundamental right for every European citizen and, for this very reason, the impact of AI systems on this field has been carefully examined and regulated. In recent years, AI has been increasingly used to support medical professionals in their tasks representing an impactful leap forward for medicine and surgery. The application of this technology in support of human labor has helped saving lives and improving the quality of treatments offered to patients, from diagnosis to treatment recommendations, from medical imaging to robotic surgery.

However, the AI Act highlights how the use of AI systems for determining whether healthcare benefits and services should be granted, revoked or denied by public authorities, can represent a significant impact on individuals' fundamental rights and livelihood, and should therefore be classified as high-risk (AI Act, 2024, p. 40)[31]. The Regulation goes on explaining that the Act and the obligations it imposes are not meant to limit or hinder the process of development and application of such technologies. The aim of the Act is to safeguard legal and natural persons fundamental rights and safety, while at the same time guaranteeing that the use of AI systems will be beneficial to society (AI Act, 2024). The classification of healthcare as a high-risk area translates into an obligation for deployers of AI systems to carry out an impact assessment on fundamental rights prior to putting the technology into use: by doing so, they will be able to identify the actual risks, how individuals' rights are likely to be affected, and to identify the measures to be taken to face these risks (AI Act, 2024, p. 57).

An important focus is also dedicated to medical devices incorporating AI systems. Prior to the implementation of the AI Act in 2024, the Regulation (EU) 2017/745 on Medical Devices was the main legal framework on the subject. Following the new approach, the introduction into the market and putting into service of this type of product can only be permitted when the product complies with all applicable Union harmonization legislation (AI Act, 2024, p. 33). Providers of products that incorporate one or more artificial intelligence systems will have to guarantee compliance with all the applicable Union requirements. This is also explained by the fact that the previous regulation on this matter does not address artificial intelligence and its risks for a person's safety and health, which calls for a simultaneous application of all the applicable requirements for medical devices (AI Act, 2024).

Medical systems and the healthcare field have already undergone dramatic changes since AI made its appearance, and, ever since, they have been transformed but

[31] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement*, cit., p.40

especially enhanced. In the past few years, applications of artificial intelligence in healthcare have dramatically increased and they are projected to keep increasing in number and importance for the future of medicine.

When talking about the application of AI to healthcare and medicine, we mainly refer to three of the multiple subdomains artificial intelligence consists of: machine learning (ML), deep learning (DL), and computer vision are the ones that had the greatest impact on this field (Dakhole and Praveena, 2024)[32]. Starting from a dataset, ML can find hidden patterns and correlations in data by using an algorithm that will help assessing problems and find solutions: in the medical field, these algorithms are used for clinical decision-making scenarios and personalized patient treatments (Dakhole and Praveena, 2024, pp. 19-20). Nowadays, deep learning is widely used thanks to its algorithms' ability to utilize massive amounts of data to continuously improve its accuracy and performance (Dakhole and Praveena, 2024). Lastly, computer vision has been crucial in the field of radiology and interpretation of radiological images. In computer vision, the computer learns from a database of still or moving pictures (Dakhole and Praveena, 2024, p. 20). The implementation of AI into various medical fields has opened new possibilities for early discovery of cancer and other medical conditions, and AI-powered image-based diagnosis have revealed to be more precise and accurate than a human eye only diagnosis. However, AI is not expected to substitute health professionals in their tasks: these new technologies are only meant to help doctors by making quicker diagnosis and better manage their resources and time. The approach of AI to healthcare is based on a collaboration between the machine and the human professional to reduce the percentage of errors and supervise each other's work. The application of AI in medical sciences includes risk prediction and intervention, medical advice and triage, diagnostics, clinical

[32] Dakhole, Dipali; Praveena, K.N.; *History and Role of AI in Healthcare and Medicine*; in "Handbook of AI-based models in healthcare and medicine", Edited by Chander, B.; Guravaiah, K.; Anoop, B; Kumaravelan, G; CRC Press; 2024; pp. 19-31.

decision-making, and remote patient monitoring (Dakhole and Praveena, 2024, p. 21). A few examples of the medical advances made possible by AI include (Dakhole and Praveena, 2024, p. 22-24): discoveries in the field of protein interaction and DNA and RNA adaptation to predict hereditary diseases; algorithms capable of recognizing genetic disorders; robots assisting or even operating alone in surgery; evaluation of rehabilitation progress; melanoma and breast cancer detection; mortality prediction by utilizing the enormous amount of medical data available.

Another important use of AI in healthcare regards the administration of medical records and healthcare processes. Patients' medical records should be anonymized and digitized to be made available for both scientists and algorithms to process and make sense of, and the availability of real-time medical data will allow discoveries in medical sciences that will then be examined for clinical application and lead to a never-ending medical progress (Dakhole and Praveena, 2024). However, the availability of biometric and sensitive data poses some serious issues for patients' privacy and security, requiring strict regulations and compliance with all applicable European regulations on the matter.

2.2.2 Education and Training

The emergence of AI has impacted on the educational system altering the ways in which teachers educate and students learn. The introduction of AI into the educational landscape has brought some dramatic changes in terms of personalization of the learning experience, automation of teachers' tasks such as grading and real-time feedback to students, tutoring and support to students who require additional help[33]. The key advantages of AI applied to this field include time and cost efficiency for

[33] University of San Diego; *39 Examples of Artificial Intelligence in Education*, in "Artificial Intelligence" (https://onlinedegrees.sandiego.edu/artificial-intelligence-education/ Accessed on 20/09/2024).

both students and educators, enhanced learning outcomes and academic success, and global access to quality education, even in developing nations, providing financial benefits to both countries and individuals (Kamalov et al., 2023, pp. 15-17)[34]. However, the implementation of this type of technology into the schooling system has been accompanied by both advantages and disadvantages. A large percentage of people affected by AI in the education field is made up of minors and teenagers, carrying along risks like security and privacy that need a special attention given the young age of the individuals impacted.

The turning point in the vast scale adoption of AI happened in November 2022 when ChatGPT was released by OpenAI making it available for free to an audience that is no longer limited to the AI experts community (Kamalov et al., 2023, p.2). When students discovered the huge potential of this tool for everyday academic tasks, its popularity grew even more, together with the concerns regarding academic dishonesty and plagiarism. The release of ChatGPT sparked people's interest in AI and its potential; society soon became aware of the benefits this new technology could have brought into their lives and its future applications. Soon after its advent, this tool started being considered as a huge leap forward in society and its projection into the future, but raising concerns about AI potential dangers and threats to individuals' privacy and security started emerging as well. ChatGPT is a "large language model based on a generative pre-trained transformer (GPT) that is further tuned via supervised and reinforcement learning techniques" (Kamalov et al., 2023, p.4)[35]. It functions in a conversational way by responding to the prompts elaborated by the user that can vary from simple questions to essays or poems composition, academic research, and up to code creation. ChatGPT can respond to most prompts with a high

[34] Kamalov, Firuz; Santandreu Calonge, David; Gurrib, Ikhlaas; *New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution*, in "Sustainability", 15, 2023, pp. 1-27

[35] Kamalov, F.; Santandreu Calonge, D.; Gurrib, I.; *New Era of Artificial Intelligence in Education*..., cit., p. 4

level of accuracy and detail, while carrying out a sort of dialogue with the user, making it accessible to anybody (Kamalov et al., 2023). ChatGPT utilizes a transformer architecture that is trained on large datasets and can process an entire sentence simultaneously by providing context for the input sequence (Kamalov et al., 2023, pp. 4-5).

As explained in the article by Kamalov et al. (2023), the current main applications of AI in education include automation of assessment, personalized learning, intelligent tutoring systems, and teacher-student collaboration. Personalized learning makes it possible to tailor the learning process according to the individual student's needs based on their characteristics and learning process; in the same way, intelligent tutoring systems interact with students actively and give back feedback (Kamalov et al., 2023). Automation of assessments utilizes AI to automatically grade students work, including homework, exams and quizzes; the automation of this type of tasks, that would normally consume most of teachers' working time, helps facilitating their relationship with students by being able to spend more time supporting their learning process and offer valuable feedback (Kamalov et al., 2023). Each one of these applications presents both benefits and challenges that need to be addressed before their implementation into the educational system.

Providing a customized learning experience through Personalized learning allows students to learn in a more engaging way and at their own pace, adapting the speed and complexity of the material thanks to a learning experience that is tailored on their specific needs, with the possibility of receiving additional support (Kamalov et al., 2023, p. 9). However, this type of learning relies on students' data and their analysis to personalize the outcome of the learning experience which exposes data to privacy and security threats with risks of potential misuse or data breach.

Applying Intelligent tutoring systems (ITS) to the educational environment enhances students' learning outcomes and their performance through personalized guidance and feedback (Kamalov et al., 2023). ITS utilizes natural language processing that "enables AI to perceive and interpret written or spoken inputs from students, allowing ITS to engage in meaningful dialogues" (Kamalov et al., 2023, p. 13)[36]. This technology can also generate dynamic models of the students it interacts with based on their skills and knowledge demonstrated during their interaction with the system: this is the so called "student modeling" component of ITS (Kamalov et al., 2023). These systems can also facilitate access to quality education in unserved areas reaching all students. Just like personalized learning, even ITS present some drawbacks concerning not only data privacy and security, but also potential biases present in the training data utilized by the algorithm that could originate episodes of discrimination (Kamalov et al., 2023, pp. 10, 13).

Assessment automation is the automatic grading of students' work made possible by AI systems. The benefits of this technology are multiple and include a reduction of the time required for evaluations and grading, the elimination of human error and personal bias, and scalability to large numbers of students in an efficient and consistent manner; these tools can also detect patterns and identify whether additional assistance is required by making personalized interventions and data-driven decisions (Kamalov et al., 2023, pp. 11, 14). The main challenge presented by this technology is of ethical nature as the information could be sensitive or personal and raise concerns about its protection of student data.

Just like every other tool and technology, the impact of AI implementation into the education system has the potential to be extremely positive, but it requires strict regulations and constant supervision, especially to its ethical side.

[36] Ivi, p. 13

2.2.3 Public Administration and Law Enforcement

The applications of AI in public administration and law enforcement represent one of the most critical areas covered by the EU AI Act due to the wide range of subjects that would be impacted from an improper regulation of this field. These systems have significant impact on citizens' fundamental rights and their civil liberties, but also on public safety and national borders' security but, at the same time, are crucial to improve Countries' development.

Improving the quality of public services and productivity while cutting costs has been a priority for central and local administrations worldwide. Digitization and the increasing incorporation of artificial intelligence into State administrations have already been proved beneficial in improving managerial and economic efficiency, further motivating the huge financial investments in this sector.

Digital progress at the European level in 2024 can be studied through the analysis of the Digital Economy and Society Index (DESI) elaborated by the European Commission. Below, Figure 1 contains a comparative frame of the 28 State Members' progress from the year 2018 to 2024. The indicators of this time-line chart are the digital public services for citizens that are the share of administrative steps that can be done online for major life events for citizens, such as birth of a child or new residence, using a score from 0 to 100 as the unit of measure (European Commission, 2024)[37]. Malta resulted to be the most digitized European country registering the highest score throughout the entire timeframe examined, starting from 99.94 in 2018 and 100 in 2023. On the other hand, Romania continuously registered the lowest score

[37] European Commission, *DESI 2024*, in "DESI – Compare countries progress", 2024 (https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/compare-countries-progress?indicator=desi_dps_cit&indicatorGroup=desi2023-4&breakdown=total&period=desi_2024&unit=egov_score&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE, Accessed on 25/09/2024).

(45.56 in 2018 and 52.18 in 2023), while Italy is positioned below the average with a score of 59.59 in 2018 and 68.28 in 2023.

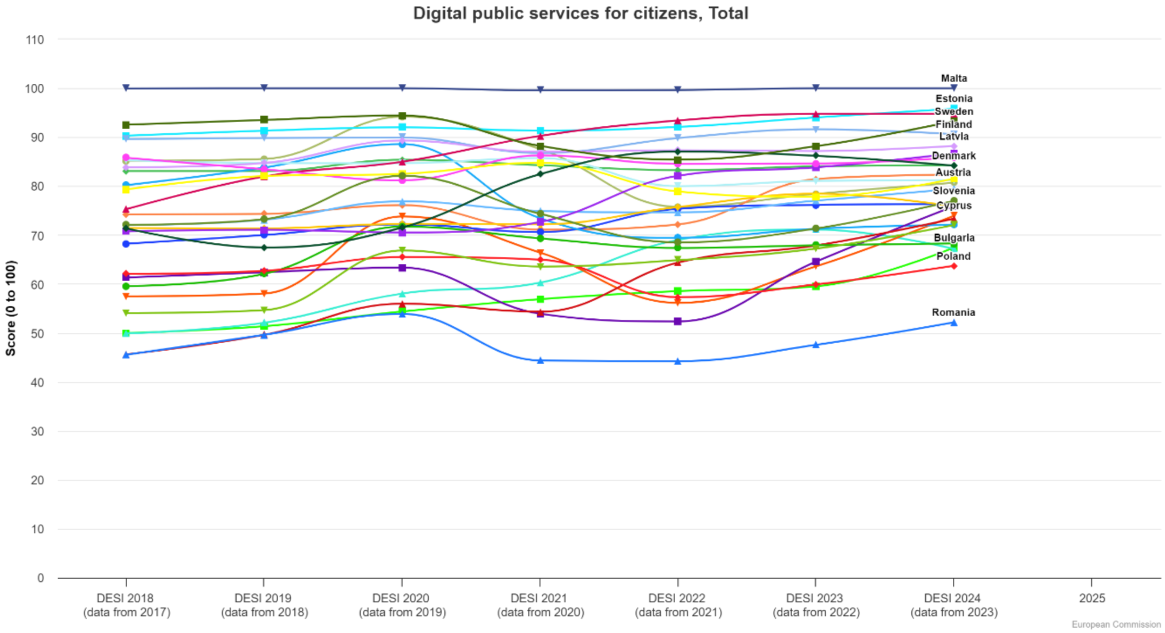

Figure 1- Digital public services for citizens, Total.

Source: European Commission, DESI 2024. Available from: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/compare-countries-progress?indicator=desi_dps_cit&indicatorGroup=desi2023-4&breakdown=total&period=desi_2024&unit=egov_score&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE

The more public services are digitized, the easier the implementation of AI-based applications is. However, ethical concerns and personal safety cannot be ignored. Many European States have already integrated AI into public administration and the economic sector obtaining remarkable results and improving transparency, accountability and efficiency. Public management is the term used for referring to the methodologies utilized for the improvement of public services and promotion of public interest, and for ensuring accountability and transparency: it is mainly concerned with the formulation and implementation of public policies, maintenance of law and order, and national security (Agba et al., 2023, pp. 3-4)[38]. The former is one of the areas mostly impacted by artificial intelligence as this type of technology provides data-driven solutions facilitate agenda setting, problem identification, policy formulation, and pattern detection of needs (Agba et al., 2023).

As previously mentioned, AI systems are increasingly being incorporated into public administration in both developed and developing nations to enhance efficiency, manage large volumes of data, but also streamline decision-making processes. The most remarkable uses of these systems include automating decision-making in public services such as tax assessments and welfare distribution, processing public data through permits and licenses, leveraging predictive analytics for resource allocation and fraud detection (Agba et al., 2023). Transparency about AI systems being utilized is one of the key focuses of the AI Act aiming to ensure that the user is always aware of interacting with an AI system. With regards to public administration, the Act also emphasizes fairness and non-discrimination to avoid bias, especially in areas related to public service access in which decisions must be equitable even when influenced by AI. Furthermore, the concept of accountability is crucial to the Act, requiring continuous human oversight over AI systems to ensure that decisions are always transparent and explainable.

Law enforcement consists of all those practices put in place to ensure the safety of citizens and society as a whole, as well as their freedom and justice. AI systems have been applied to this area in the past few years with remarkable results, encouraging further applications but also raising possible issues related to privacy and freedom. One of the most important examples of AI use in law enforcement are facial

[38] Agba, Michael Sunday; Agba, Grace Eleojo Micheal; Obeten, Amos W.; *Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies*, in "Journal of Public Administration, Policy and Governance Research", Vol. 1, No. 2, June 2023, pp. 1-14

recognition technologies (FRTs) which are utilized for automatic identification of individuals in smart environments (Mobilio, 2023)[39]. The cities that are currently using these technologies leverage the information gathered by cameras and sensors to collect data from behavioral pattern detectors, number plate readers, and facial recognition systems as automated policing tools; moreover, in recent years, biometrics enhanced authorities' capability to identify people in public spaces for security reasons (Mobilio, 2023). Biometrics such as fingerprints have a long history of utilization by law enforcement authorities (LEAs), however the introduction of FRTs in this field brought along privacy concerns for its invasive nature. Collecting fingerprints or DNA samples requires the physical presence of the person and, consequently, their acknowledgment and, in most cases, consent to being identified (Mobilio, 2023). Compared to this type of biometrics, capturing the image of a person and their face is much easier: FRTs happen at a distance without direct contact with the person who could also be in motion; this means that awareness and consent from the individual being captured are not always present (Mobilio, 2023). Moreover, this type of system can be perpetuated through a wide range of devices such as body cams, CCTV cameras but also drones, making recognition low cost but especially embedded. By harnessing AI, algorithms can automatically detect a person's face in a picture, extract the facial features and elaborate a numerical representation that will be unique to that person, and compare it to the other facial images present in LEAs datasets and watchlists (Mobilio, 2023). The possible uses of FRTs in law enforcement include repressive purposes like identifying a person wanted for a crime, investigative purposes such as monitoring a person's movements and interactions, but also preventive reasons (Mobilio, 2023).

[39] Mobilio, Giuseppe; *Your face is not new to me – Regulating the surveillance power of facial recognition technologies*, in "Internet Policy Review", Vol. 12(1), 2023, pp. 1-31

AI systems have been increasingly used also in surveillance with biometric captures and facial recognition. A remarkable application concerns borders control and visa processing that leverages the developments in machine learning to facilitate travelers' experience and enhance security at the same time.

The AI Act considers this category of systems as high-risk because of the nature of the personal and sensitive data involved, and the potential issues that could derive from an improper use of FRTs. In particular, in the case of biometric data a distinction between 'ex post' and 'real time' use has been made, considering the former less dangerous than the latter given its apparent minor impact on fundamental rights compared to real time use; however the intrusiveness of the type of use does not depend on the length of time necessary to process the biometric data, so this distinction is not accurate (Mobilio, 2023, p. 21).

Another set of problems regards biometric categorization systems and emotion recognition systems. The former categorizes people based on their physical characteristics opening the door for discrimination against minorities, while the latter is still not scientifically and objectively corroborated since the display of emotions varies depending on culture, situation and circumstances making it hard to assess a person's real emotions (Mobilio, 2023, p. 21). For these reasons, the Act itself states that technical inaccuracies of FRTs "can lead to biased results and entail discriminatory effects" (AI Act, 2024, Recital 33)[40].

In conclusion, Recital 33 of the EU AI Act considers 'real-time' remote biometric identification systems as to be used only when strictly necessary and proportionate to

[40] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement*, cit., Recital 33.

the degree of seriousness of the situation, confirming how an ‘ex-post’ use of data has a minor impact on fundamental rights. The Recital continues stating that:

“

> Law enforcement, border control, immigration or asylum authorities should be able to use information systems, in accordance with Union or national law, to identify persons who, during an identity check, either refuse to be identified or are unable to state or prove their identity, without being required by this Regulation to obtain prior authorization”.[41]

2.2.4 Transport and Mobility

AI applied to the transportation and mobility field is revolutionizing the way we move by improving efficiency, but also safety and sustainability. The emergence of autonomous vehicles can benefit both the environment and citizens with lower pollutant emissions and improved safety in urban areas (European Commission, 2024)[42]. From autonomous vehicles and traffic management systems to predictive maintenance and route optimization, AI-driven technologies are revolutionizing urban mobility and the way we think about traveling.

Nowadays, travel patterns have changed, and people are more prone to discovering new locations thanks to the new opportunities offered by AI systems and portable devices. The rapid urbanization that has been taking place in most developed countries has impacted not only the environment, but also security and the management of cities requiring countries worldwide to develop and adopt intelligent city programs to address the challenges brought by these changes (Bharadiya, 2023)[43]. Urban mobility

[41] Future of Life Institute FLI, *EU Artificial Intelligence Act*, 2024 (https://artificialintelligenceact.eu/recital/33/, Accessed on 25/09/2024).

[42] European Commission, *Transport and Mobility*, in “AI watch”, 2024 (https://ai-watch.ec.europa.eu/topics/transport-and-mobility_en, Accessed on 27/09/2024).

[43] Bharadiya, Jasmin Praful; *Artificial Intelligence in Transportation Systems - A Critical Review*, in “American Journal of Computing and Engineering”, Vol. 6 (1), 2023, pp. 35-45

has adapted to these changes in transportation planning and systems by developing AI-integrated solutions that are revolutionizing the way in which we think about traveling.

In recent years, the term ‘smart mobility’ has started being used to indicate the integration of advanced AI technologies into transport systems to ensure safety, efficiency, accessibility, and sustainability (Mitieka et al., 2023)[44]. Smart mobility relays on technology to operate: it combines transportation modes, including public transport but also walking and cycling, and real-time data collection, analysis and transmission to offer personalized transportation options to travelers (Mitieka et al., 2023). The big data collected in the process from various sources (GPS systems, sensors, etc.) are crucial to understand mobility patterns and improve traffic flow by identifying congestions and suggest alternative routes. In this process, the Internet of Things (IoT[45]) plays a critical role by integrating devices and sensors to form a connected network within transportation systems; this network enables real-time monitoring of traffic, collection of air quality data, and detection of accidents, enabling to improve safety and reduce congestion (Mitieka et al., 2023).

As Bharadiya (2023) explains in her article, some of the most remarkable examples of artificial intelligence in transportation systems include fully autonomous vehicles, enhanced traffic prediction and management, intelligent infrastructure and connectivity, personalized mobility services, sustainable transportation solutions and advanced safety systems.

[44] Mitieka, Douglas; Luke, Rose; Twinomurinzi, Hossana; Mageto, Joash; *Smart Mobility in Urban Areas: A Bibliometric Review and Research Agenda*; in “Sustainability”, 15, 2023, pp. 1-23

[45] The Internet of Things (IoT) indicates the network of physical objects, such as devices, vehicles, appliances, and sensors, that are embedded with software, sensors, and connectivity features, enabling them to collect and exchange data over the internet: these physical objects can communicate with each other but also with uses allowing smart homes, smart cities, up to applications to the industrial system and healthcare (Definition from IBM, *What is the Internet of Things (IoT)?* https://www.ibm.com/think/topics/internet-of-things, Accessed on 27/09/2024).

Autonomous vehicles combine AI algorithms, deep learning techniques and advanced sensor technologies to enable vehicles to navigate complex traffic scenarios while handling all driving tasks without any human intervention (Bharadiya, 2023). The introduction of Tesla's self-driving vehicles marks a milestone in both the automotive industry and AI advancements, redefining the boundaries of future mobility. Its autopilot and full self-driving systems leverage advanced AI, machine learning, and a network of cameras, sensors and radar enable these vehicles to function without any human help[46]. As stated on Tesla's official website[47], the autopilot system together with multiple external cameras and powerful vision processing provide a high degree of safety; however, these systems are meant to be used with a fully attentive driver prepared to take over in case of need. These vehicles can match their speed to the surrounding traffic conditions, assist in steering and lane change, but also auto park and detect pedestrians with a high degree of safety and efficiency[48]. Object detection and AI-powered vision processing improve both vehicle and pedestrian safety, reducing the risk of collision.

The application of AI in traffic prediction and management is poised to revolutionize the transportation system and, consequently, urban mobility. By analyzing huge amounts of real-time data from sources such as sensors, GPS systems data from vehicles, mobile applications and even social media feeds, AI algorithms can provide accurate and up-to-date traffic predictions (Bharadiya, 2023). Traffic predictions elaborated through AI will allow real-time adjustments, including dynamic routing, helping drivers to avoid congestion areas and reducing overall travel times with environmental benefits as well (Bharadiya, 2023). The benefits of integrating AI within the transportation system include congestion prevention by forecasting

[46] Tesla, *Autopilot and Full Self-Driving (Supervised*), in "Support" (https://www.tesla.com/support/autopilot, Accessed on 28/09/2024).

[47] Ibid.

[48] Ibid.

potential traffic jams and bottlenecks before they occur, which can also potentially help in the redesigning of the city road system (Bharadiya, 2023). Machine learning algorithms can therefore promote eco-friendly driving behaviors and an optimization of energy consumption making transportation solutions more sustainable (Bharadiya, 2023). Moreover, AI can also assist in vehicle maintenance by informing when this is needed, and minimizing the risk of mechanical failures (Bharadiya, 2023).

Related to traffic prediction and management is intelligent infrastructure and connectivity, which consists of an infrastructure system that communicates with vehicles to provide real-time updates through AI (Bharadiya, 2023): by integrating AI with smart infrastructure, such as adaptive traffic lights, traffic signals can be fully optimized and respond to fluctuations in traffic conditions instantly (Bharadiya, 2023).

Intelligent transportation systems (ITS) need three essential components to function: data collection, analysis, and transmission (Bharadiya, 2023). Based on the functionalities of these components, ITS can be divided into two main categories: Advanced traveler information systems (ATIS) and Advanced management systems (AMS). As Bharadiya (2023) explains, ATIS help travelers make decisions regarding the mode or route choice, departure time or day by providing this type of information, while AMS optimize transportation by coordinating infrastructures and operators, while also managing traffic, transit and emergency responses.

AI-systems integration into transportation involves the application of technologies such as machine learning and computer vision to improve efficiency and, above all, sustainability and safety of the transportation system and urban mobility.

2.2.5 Retail, Marketing and E-commerce

AI is transforming the retail industry by enhancing customer experience and decision-making, driving sales and optimizing business operations. From personalized shopping experiences and chatbots to automated customer service, AI applications in this industry are revolutionizing how retailers interact with customers and manage their supply chains. The implementation of these technologies ultimately leads to improved efficiency, sales boost, and a more tailored shopping experience for customers.

The reshape of the retail industry brought by the implementation of AI has experienced a boost since the outbreak of COVID-19. The pandemic has dramatically changed the dynamics of everybody's life as well as their spending habits, forcing business to adapt to this new reality and rethink their operations (Lu et al., 2023)[49]. During lockdown times, as people were forced to stay home for long periods of time, making purchases online was the only solution in case of need as physical stores were closed and mobility was restricted. E-commerce usage rose dramatically during the pandemic and became the new norm among large groups of people. The end of lockdown and the return to reality did not stop the popularity of making purchases online, in fact they led to new popular trends and phenomena, such as the so-called 'showrooming'. This term indicates consumers who will first visit a physical store to see and experience the product they intend to buy in person, and then may switch to purchasing it on online retail platforms for multiple reasons (lower prices, special offers, etc.) (Wang et al., 2024)[50]. However, online platforms still exhibit more disadvantages than physical stores, which prevent customers from purchasing online.

[49] Lu, His-Peng; Cheng, Hsiang-Ling; Tzou, Jen-Chuen; Chen, Chiao-Shan; *Technology roadmap of AI applications in the retail industry*, in "Technological Forecasting & Social Change", 195, 2023, pp. 1-11

[50] Wang, Qiang; Ji, Xiang; Zhao, Nenggui; *Embracing the power of AI in retail platform operations: Considering the showrooming effect and consumer returns*; in "Transportation Research Part E", 182, 2024, pp. 1-26

Some of these include the lack of a direct experience with the physical product since it is not possible to touch and feel it through the screen; moreover, consumers generally lack information about the product and its fitness before physically interacting with it (Wang et al., 2024). The multiple applications of AI to the retail industry are helping to solve these issues and improving the shopping experience.

According to Lu et al. (2023), the consumer shopping experience can be divided into three phases: the pre-purchase, purchase, and post-purchase. As they explain in their study, the pre-purchase phase is until the moment of the payment and actual purchase; the post-purchase phase starts right after with the customer using the product and evaluating her or his purchase. Every single one of these phases can potentially benefit from the implementation of AI technologies and the examples are multiple. Customers are motivated to purchase through product searches, and the online search is the first touch point of the customer journey that can be impacted by AI through image recognition, keyword search, and personalized advertising recommendations (Lu et al., 2023). AI technologies optimize the checkout phase as well by offering multiple payment methods, and utilizing image detection to reduce the time spent on the payment moment. During the post-purchase phase, virtual assistants and chatbots can assist the customer in multiple ways, including the return and exchange process.

The retail sector is characterized by a fast-paced evolution depending on trends and new competitors on the market. Given its dynamic nature, the retail field has started embracing AI technologies to face customers' demands and improve efficiency, enhance customer experiences, and optimize operations while staying competitive in an increasingly digital marketplace (Wilson et al., 2024)[51]. To make this possible, data collection is crucial. Collecting consumers' data about the shopping process and its

[51] Wilson, George; Johnson, Oliver; Brown, William; *Exploring the Integration of Artificial Intelligence in Retail Operations*, in "Creative Commons CC", 2024, pp. 1-18

features is considered more important than developing service applications and, to do so, cloud integration platforms have become indispensable tools (Lu et al., 2023).

As discussed in the article by Oosthuizen et al. (2020)[52], we can divide AI technologies in retail into four main categories. The first one is knowledge and insight management AI technologies, which provide valuable insights by managing and sharing information throughout the value chain: the translation of these data into knowledge can help anticipate customers' demands and source optimal assortments accordingly (Oosthuizen et al., 2020). The second category is inventory management. Sales forecasts are crucial to match supply to demand, and to fulfil customers' requirements while maximizing profits. AI solutions in this category include chatbots, intelligent applications, insight engines, and virtual assistants that work to anticipate demands, keep popular items stocked, and anticipate future customers' requirements (Oosthuizen et al., 2020, p. 268). The third category, operations optimization, includes the AI applications that assist in improving operations and minimizing operational capabilities: some examples are computer vision, deep learning and virtual assistants that improve production speed and manage inventory flow (Oosthuizen et al., 2020). Lastly, customer engagement AI technologies are considered by many as the most significant application of artificial intelligence in retail.

In an increasing competitive landscape, offering a customer-centric value chain is crucial to stand out and satisfy customers' expectations. One way of building connections and fostering customers' engagement is through a personalization of products and services to cater to their unique needs and preferences: AI enables retailers to satisfy these expectations through data collection and analysis, and providing tailored recommendations and customized shopping experiences (Wilson et al., 2024). A common example of such personalization is the use of chatbots that

[52] Oosthuizen, Kim; Botha, Elsamari; Robertson, Jeandri; Montecchi, Matteo; *Artificial intelligence in retail: The AI-enabled value chain*; in "Australasian Marketing Journal", Vol. 29(3), 2020, pp. 264-273

reduces costs but also help in building customer loyalty through personalization. AI-powered chatbots and virtual assistants can handle a wide variety of customer inquiries, providing accurate and 24/7 responding customer support; they also improve customer satisfaction with quick responses, and reduce operational costs since there is no need for human intervention (Wilson et al., 2024).

Interactive marketing is a new type of marketing that is gaining increasing popularity, and it is made possible with the implementation of AI to solve modern-day problems with innovative solutions that provide a modern and dynamic experience for customers. Modern-day retailing is characterized by the emergence of 'experience stores', a new concept store that offers a unique shopping experience to customers by leveraging emerging technologies to encourage more customer involvement, thus creating an interactive environment (Jasrotia, 2023, p. 186)[53].

The following are some remarkable examples of AI innovations applied to marketing and retail that are revolutionizing the shopping experience worldwide.

Smart mirrors are an interactive technology that has been gaining increasing popularity since its introduction in the market. It offers a real-world environment to the customer by just standing in front of it and interacting with the environment projected on the mirror screen. This technology has proved particularly beneficial for clothing firms: the Ralph Lauren Polo Flagship store in the United States represents a valid example of the implementation of these smart mirrors into their physical stores, and they have been proved increasing sales (Jasrotia, 2023). Not only can the customer see how the product would look like on them without having to try it on, but also, they can test different lighting, and the mirror can also make suggestions about different clothes or accessories based on the person's body type (Jasrotia, 2023). As Jasrotia

[53] Jasrotia, Sahil Singh; *Technological Innovations in Interactive Marketing: Enhancing Customer Experience at the New Retail Age*, in "The Palgrave Handbook of Interactive Marketing" by Cheng Lu Wang, Palgrave Macmillan, Switzerland, 2023, pp. 183-197

(2023) explains, smart mirrors benefit both the customer and the organization. On the customer side, smart mirrors provide different product combinations, and purchase recommendations based on body type or previous purchases; moreover, they can display what products are available in the store (Jasrotia, 2023). The benefits for organizations include a sales boost, customer data and insights, but also popularity derived from people's curiosity of trying such innovations (Jasrotia, 2023).

Virtual reality (VR) is a technology powered by AI that simulates an environment where the users can feel immersed (Kim et al., 2021)[54]. Virtual reality creates virtual worlds that enhance the user's experience by browsing 3D images of products in a store, check visual representation of products in different locations and much more (Jasrotia, 2023). Very similar to virtual reality is augmented reality (AR) that functions in a very analogous way. IKEA developed an AR application that allows people to virtually place furniture in their houses. As explained on the company website[55], this app marks an important milestone in IKEA digital transformation journey as it automatically "scales products based on room dimension with 98% accuracy. The AR technology is so precise that you will be able to see the texture of the fabric, as well as how light and shadows are rendered on your furnishings"[56]. The benefits of the implementation of this type of technology include superior customer service and a higher conversion rate (Jasrotia, 2023).

Checkout-free stores represent an innovative concept in retail, allowing customers to select products, pay via a mobile app, and leave the store without having to wait in

[54] Kim, J.-H., Kim, M., Park, M., & Yoo, J.; *How interactivity and vividness influence consumer virtual reality shopping experience: The mediating role of telepresence*, in "Journal of Research in Interactive Marketing", Vol. 15(3), 2021, pp. 502–525.

[55] IKEA, *Ikea Place App*, in "Inter IKEA Newsroom", 12/09/2017, (https://www.ikea.com/global/en/newsroom/innovation/ikea-launches-ikea-place-a-new-app-that-allows-people-to-virtually-place-furniture-in-their-home-170912/, Accessed on 29/09/2024).

[56] IKEA, *Ikea Place App*, in "Inter IKEA Newsroom", 12/09/2017, https://www.ikea.com/global/en/newsroom/innovation/ikea-launches-ikea-place-a-new-app-that-allows-people-to-virtually-place-furniture-in-their-home-170912/, Accessed on 29/09/2024.

checkout lines (Spanke, 2020)[57]. This seamless shopping experience not only enhances customer convenience and saves them time, but also frees up employees to focus on more essential tasks, such as assisting shoppers and improving store operations (Jasrotia, 2023).

Related to the previous example is facial recognition shopping, an innovative AI technology that allows customers to pay through a scan of their face making their shopping experience faster and smoother. To utilize it, the customer must have a specific app installed on his or her device, glance at the facial recognition system, and the app will automatically deduct the payment from their account (Jasrotia, 2023). Additionally, AI-driven analytics can monitor customer movements and behaviors within stores, providing valuable insights concerning shopping patterns and preferences (Wilson et al., 2024). This data enables retailers to design store layouts and product placement to better meet customer needs and gain their attention, ultimately enhancing their shopping experience (Pantano et al., 2017)[58].

Voice-based services like Google Assistant or Alexa are becoming increasingly popular as they can help with tasks with only the need for users' voice. Technologies based on this system simplify shopping as it can be done anytime and simultaneously to other activities, offering benefits such as product discoverability and ease to the customer, while also helping organizations in increasing conversions (Jasrotia, 2023).

One of the newest applications of AI in retail is the use of drones. This innovation became increasingly important during Covid-19 when social distance was mandatory to avoid contamination. The use of drones in the retail area reduces the human touch involved in delivering a product and enables a contactless experience (Jasrotia, 2023).

[57] Spanke, M.; *Easy checkout. Retail isn't dead*, 2020, Palgrave Macmillan, pp. 85–93

[58] Pantano, E., Priporas, C. V., Sorace, S., & Iazzolino, G.; *The effect of mobile retailing on consumers' purchasing experiences: A dynamic perspective*; in "Computers in Human Behavior", 77, 2017, pp. 367-373. (https://doi.org/10.1016/j.chb.2017.07.022).

Drones are flying robots that can be controlled remotely to fulfil last mile delivery and, by avoiding physical touch, they ensure safety (Jacob et al., 2022)[59].

Retailers are leveraging interactive retailing to enhance the customer experience and engage clients in unique ways within physical stores; this type of approach creates memorable interactions and encourages customers to share their experiences on social media, generating buzz around the brand (Roggeveen & Sethuraman, 2020)[60]. Interactive retailing offers several benefits to retailers: among these, it increases foot traffic, boosts brand reputation, and provides higher revenues (Jasrotia, 2023).

Despite all the benefits brought into the retail industry by AI systems, its massive usage of customers' data has raised concerns regarding data privacy and security. The risk of data breaches can have serious implications for both customers and retailers since it includes personal data, but also information about shopping preferences and patterns. As the AI Act states on Recital 12, "a key characteristic of AI systems is their capability to infer: […] (it) refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments"[61]. The nature of the data involved in these processes obligates providers to comply with strict regulations ensuring that personal data is protected throughout the entire lifecycle of the system by design, anonymization, and encryption. Moreover, it is necessary that customers are always informed whenever they are dealing with a robotic agent, especially if the interaction has the potential to influence the person's decisions.

[59] Jacob, B., Kaushik, A., & Velavan, P.; *Autonomous navigation of drones using reinforcement*; in "Advances in augmented reality and virtual reality. Studies in computational intelligence" by J. Verma & S. Paul (Eds.), Springer, 2022, pp. 159–176

[60] Roggeveen, A. L., & Sethuraman, R.; *How the COVID-19 pandemic may change the world of retailing*; in "Journal of Retailing", 96(2), 2020, pp. 169–171.

[61] EU Artificial Intelligence Act, 2024, (https://artificialintelligenceact.eu/recital/12/, Accessed on 28/09/2024).

2.2.6 Employment and Human Resources

AI systems are increasingly being adopted within businesses and one of the major areas of application is Human Resources Management. The impact of AI is transforming a wide range of procedures in business organizations, including the management of the workforce such as employer-employee relationships, workforce demographics, and the relationship between people and technology (Chowdhury et al., 2023)[62]. The benefits of AI adoption include increased business productivity through an optimization of business operations and resources, a business model transformation, facilitation of decision-making processes, and reducing employee costs while also enhancing their job satisfaction (Chowdhury et al., 2023).

Organizations are investing in AI-enabled software packages to leverage employee data and guide decisions. One of the first uses of AI in human resources is linked to job evaluation and employee monitoring: these tools can help identify issues and share insights, guide decisions and encourage stakeholders to act (Peeters et al., 2020)[63]. However, one of the most discussed applications of AI in the field regards the recruitment process. AI recruitment systems help streamline applicant selection by filtering candidates from all the submitted applications; they can also assist in decision-making during interviews by evaluating a candidate's responses and matching them with the organization's needs; lastly, it can suggest an adequate salary and benefits based on the applicant qualifications (Chowdhury et al., 2023).

AI offers advanced tools for fast and automated resume scanning, reducing the time spent on manual tasks (Chowdhury et al., 2023). It also helps attracting the best-fit

[62] Chowdhury, Soumyadeb; Dey, Prasanta; Joel-Edgar, Sian; Bhattacharya, Sudeshna; Rodriguez-Espindola, Oscar; Abadie, Amelie; Truong, Linh; *Unlocking the value of artificial intelligence in human resource management through AI capability framework*, in "Human Resource Management Review", 33, 2023, pp. 1-21

[63] Peeters, T., Paauwe, J., & Van De Voorde, K.; *People analytics effectiveness: developing a framework*, in "Journal of Organizational Effectiveness: People and Performance", 7(2), 2020, pp. 203–219.

candidates by refining job description, performing sentiment analysis to monitor new hires and employee motivation, and screening and matching candidates with job roles more efficiently; moreover, utilizing these technologies helps in reducing subjective criteria from the hiring process and improves retention by predicting individual employee's needs (Chowdhury et al., 2023). Existing research highlights that AI's advanced computational power, data analytics capabilities, and ability to process large amounts of information can significantly enhance human decision-making, rather than replace it entirely (Jarrahi, 2018)[64]. So, the factors pushing the implementation of AI are leveraging big data for an optimization of productivity and the decision-making process.

Seeber et al. (2020)[65] argue that effective AI teammates go beyond the roles of simple social robots or digital assistants: they are envisioned to engage in complex problem-solving activities, such as defining problems, identifying root causes, and proposing, as well as evaluating, potential solutions. AI teammates would not only help select the most suitable options, but also actively participate in planning and taking action. Moreover, their ability to learn from past interactions makes them valid collaborators in dynamic problem-solving environments: this perspective highlights the potential of AI to act as capable and adaptive partners in decision-making processes (Chowdhury et al., 2023).

Additionally, AI can be used to help with writing job profiles, monitor and measure performances, tracking employee morale and identifying the underperforming ones, boosting employee retention through continuous monitoring, resulting in performance gains (Chowdhury et al., 2023).

[64] Jarrahi, M. H.; *Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making*, in "Business Horizons", 61(4), 2018, pp. 577–586.

[65] Seeber, I., Bittner, E., Briggs, R. O., De Vreede, T., De Vreede, G.-J., Elkins, A., & Randrup, N.; *Machines as teammates: A research agenda on AI in team Collaboration*, in "Information & management", 57(2), Article 103174, 2020.

Nevertheless, AI adoption in human resources faces multiple challenges. One of the biggest barriers regards ethical constraints, including privacy and data protection concerns and potential bias in the algorithms. As Chowdhury et al. (2023) explain, AI algorithms may identify a relationship between criterion affecting the candidate's selection, which could raise reliability issues, and the human recruiters rarely have enough tools to discover why the applicant was unsuccessful. Potential biases in the algorithm are another major barrier since they have found to disproportionally disadvantage certain ethnic groups that would consequently stay marginalized in the job market (Chowdhury et al., 2023).

Recital 57 of the AI Act classifies "AI systems used in employment, workers management and access to self-employment […] as high-risk since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights"[66]. The Recital continues with stating that these systems, including the ones used to monitor the performance and behavior of employees, may perpetuate patterns of discrimination against minorities and certain groups (women, elder people, persons with disabilities, etc.), and may also undermine their fundamental rights to data protection and privacy. The rules imposed by the AI Act seek to protect employees and applicants from unfair treatments made by AI systems, requiring transparency and accountability from providers.

[66] EU Artificial Intelligence Act, 2024, (https://artificialintelligenceact.eu/recital/57/ Accessed on 30/09/2024).

Chapter 3:

The EU General Data Protection Regulation (GDPR)

3.1 Importance of Data Protection in the Digital Age

The current landscape shaped by new technologies has dramatically changed how we act and how we perceive the world around us. The advent of the Internet and advanced technological devices have opened new opportunities as well as new challenges to address in the fields of data protection and the Information security as the innovation continues. Experts called this socio-technological landscape the 'Digital Age' which can be described as a combination of all the currently available technological solutions that determine the "specific characteristics of contemporary world globalization, e-communications, information sharing, virtualization, etc." (Romansky and Noninska, 2020, p. 5288)[67]. Since the end of the 20th century, the increasingly important role of computers and information technologies in society has continuously imposed up to date regulations and revisions of existing ones to ensure the protection and safeguard of users' information processing. During 1970s, multiple countries started realizing the huge potential of the Internet and the importance of protecting individuals' data, so it is during these years that the first laws on the subject start being passed by countries such as Germany, Sweden, France, and USA (Romansky and Noninska, 2020).

In a world where data is considered a strategic asset, the concepts of personal data and privacy have assumed relevance for both individuals and governmental authorities. Art. 4(1) of the GDPR defines personal data as "any information which are related to

[67] Romansky, Radi P.; Noninska, Irina S.; *Challenges of the digital age for privacy and personal data protection*, in "Mathematical Biosciences and Engineering", Volume 17, Issue 5, 2020, pp. 5288-5303

an identified or identifiable natural person”[68]. As Article 4 states, personal data includes name, identification number, location, online identifier, and any other information regarding the identity of an individual. On the other hand, privacy is internationally recognized as a fundamental right (in most countries), and it can be explained as the “ability of an individual or a group of individuals to protect the private life and private environment, including the information about themselves” (Romansky and Noninska, 2020, pp. 5288-5289). However, it is fundamental to distinguish between privacy and data protection. The two terms do not have the same meaning and relevance outside the European Union borders. The EU has one of the strictest regulations and highest standards regarding its citizens’ right to data protection, and it is constantly improving in ensuring that individuals’ personal data is treated according to a set of legal requirements that turned out to be considered as the gold standard worldwide.

As explained by Taylor (2023)[69], data protection is not a fundamental right all around the world, so the importance assigned to this concept greatly varies not only between developed and developing countries, but also among Western Liberal democracies. With technology becoming omnipresent, the EU has been constantly working to regulate how subjects’ personal data are processed and managed within its territory (Taylor, 2023). However, with the creation of a cyberspace[70], the international and intercontinental flow of data and its management can encounter multiple barriers in international jurisdictions (Taylor, 2023). One of the most relevant examples of the difference in the importance carried by data protection laws can be found in the

[68] Intersoft Consulting, *GDPR* (https://gdpr-info.eu/issues/personal-data/, Accessed on 10/10/24).

[69] Taylor, Mistale; *Transatlantic Jurisdictional Conflicts in Data Protection Law: fundamental rights, privacy and extraterritoriality*; Cambridge University Press; 2023

[70] The cyberspace can be defined as “A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Definition from: https://csrc.nist.gov/glossary/term/cyberspace, Accessed on 14/10/24).

comparison between the EU and the United States approach to this matter. In the Union, data protection represents a fundamental right and a shared value among the Member States, and it is associated with human dignity and the right to privacy (Taylor, 2023). On the other hand, U.S. privacy laws are mainly focused on their impact in the marketplace and, consequently, are less relevant in the legislation (Taylor, 2023). An interesting fact regarding the difference between the EU and the US approach to data privacy is that Europe places strong emphasis on privacy invasions by big corporations which involves consumers' rights and the safety of the single person's data, while the U.S. is more concerned about privacy invasions by big governments, which shows how different the priorities are for the two (Taylor, 2023): the latter prioritizes national security, access to documents, freedom of expression, and national trade, whereas the EU is more concerned with privacy and the protection of data processed throughout all those instances (Taylor, 2023, pp. 2-4).

As digital devices are now available to the largest part of the world population and are being utilized daily, there are two main aspects of the Internet of Things that threaten users' privacy and data protection. The first one is confidentiality that could be disturbed when data sent from one end point to the other contains sensitive (or not) information and reaches other networks (Romansky and Noninska, 2020); moreover, the increase in the number of sensors and all the data that these sensors collect could be accessed and lead to the share of personal information concerning one's health, habits, religion, etc. (Romansky and Noninska, 2020). Secondly, the security of these technological devices can be susceptible to different types of attacks, including cyberattacks, when the passwords used are not protected (Romansky and Noninska, 2020).

3.2 Background and Evolution of the GDPR

The General Data Protection Regulation, or more simply called GDPR, is the result of four years of drafting and negotiating between the EU Member States and various organizations that operate in the fields affected by it (Politou et al., 2022)[71]. Since its implementation in 2018, the GDPR has been considered as the ultimate standard for data protection laws all over the world. The Regulation replaces the 1995 Data Protection Directive which was adopted when the internet was still in its early stages[72]. Accordingly, the process that led to the implementation of the finalized version of the GDPR had many stages that developed throughout the past 30 years, and that will be explained below.

As mentioned before, the introduction of the GDPR aimed at replacing the Data Protection Directive 95/46/EC (DPD) which was introduced in 1995: over the last 30 years, technology has dramatically changed our lives which are inevitably impacted by it positively but also negatively, so a review of the legislation on the matter was necessary to keep ensuring the protection of citizens' rights; moreover, being a directive, the DPD of 1995 left room for interpretation when being integrated into each Member States' national laws (Politou et al., 2022). On October 1995, the Directive 95/46/EC was adopted by the European Union to ensure the protection of individuals' personal data processing and the movement of such data[73].

The first demands for a reform of the European 1995 data protection Directive arrive at the beginning of 2012 when the European Commission proposes a review of these rules to strengthen online privacy rights given the increasing popularity of social

[71] Politou, Eugenia; Alepis, Efthimios; Virvou, Maria; Patsakis; Constantinos; *Privacy and Data Protection Challenges in the Distributed Era*, in "Learning and Analytics in Intelligent Systems", Volume 26, Springer, 2022.

[72] European Data Protection Supervisor; *The History of the General Data Protection Regulation*, 2018 (https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en Accessed on 23/10/2024).

[73] Ibid.

media such as Facebook, and the incoming prospective of a European digital economy[74]. Following these demands, the European Data Protection Supervisor (EDPS) adopts an opinion on the reform package as an initial input to reinforce the position of data subjects, enhance the responsibility of controllers, and strengthen the role of supervisory authorities to reduce the legal fragmentation of data protection laws across Europe[75]. The reform package will translate into an actual proposal in March of the same year.

Even if prominent European personalities such as Viviane Reding (EU's justice Commissioner and Vice-President in 2013) remarked the importance of adapting to the new digital world and taking advantage of the new computing and information-sharing landscape, many companies and governments were reluctant to the idea of a reform in the data protection legislation as they saw it as an obstacle to the challenges of the digital age[76].

The turning point in the adoption of the GDPR arrives in 2014 when the European Parliament votes in plenary for the new Regulation with 621 votes in favor, 10 against and 22 abstentions[77]. The process of adoption of the GDPR was delayed multiple times due to inferences caused by some Member States' national reasons; however, on June 15th, 2015, the Council reaches a general approach on the GDPR after the original reform proposals were scrutinized and amended[78]. On December 9th, 2015, EU negotiators reached a key agreement on the General Data Protection Regulation (GDPR) and the Directive on Data Transfers for Policing and Judicial Purposes[79]; one week later, on December 15, the European Parliament's LIBE Committee (Civil

[74] Ibid.

[75] Wilhelm, Ernst Oliver; *A brief history of the General Data Protection Regulation (1981-2016*), in "iapp", 2016 (https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/#, Accessed on 24/10/2024).

[76] Ibid.

[77] Ibid.

[78] Ibid.

[79] Ibid.

Liberties, Justice and Home Affairs) formally adopted the GDPR with a strong majority: key provisions included clear consent requirements, protections for children on social media, the right to be forgotten, data breach notifications, plain language requirements, and fines up to 4 percent of a company's global annual revenue[80].

At the beginning of 2016, the Article 29 Working Party issued an action plan for the implementation of the GDPR and on May 24th, 2016, 20 days after the publication in the Official Journal of the EU, the Regulation officially enters into force[81]. As the data protection and technological landscape evolve, new regulations on the matter start being proposed to adapt the Regulation to the developments in progress.

After being implemented into Member States national legislations, the General Data Protection Regulation enters into force and starts being applied on May 25th 2018[82].

3.3 Key Principles of the GDPR

The enactment of the GDPR on the 25th of May 2018 imposed stricter legal requirements for data controllers operating within the EU territory and with European subjects' data. The new data protection regulations imposed by the GDPR affect businesses operating both within and outside the European borders as the new provisions impact also third parties involved in the movement and processing of European citizens' data. Being a regulation and not a directive, the GDPR immediately became enforceable in all the Member States without the need of any additional adaptation (Politou et al., 2022); moreover, it contributed to the harmonization of the data protection laws across the EU, enhancing the potential of its digital market (Politou et al., 2022).

[80] Ibid.

[81] European Data Protection Supervisor; *The History of the General Data Protection Regulation*, cit.

[82] Ibid.

The rules imposed by the GDPR apply to any companies or entities established in the European Union and that process personal data, regardless of where the data is ultimately processed, stored or used[83]. However, this Regulation complies with its ultimate objective of protecting data belonging to EU citizens and residents by being applicable also to companies that are not based in the Union. Article 3(2) GDPR specifies that the Regulation applies "to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union"[84] and whose activities concern the offering of goods and services to individuals in the Union, or the monitoring of their behavior only when it takes place in the EU[85]. With this article, the GDPR does not require the data subject to be an EU citizen or resident: he or she only must be physically present in the Union territory to benefit from the Regulation applied to. Article 3(3) further explains that the data protection applies also to the processing of personal data by an entity "not established in the Union, but in a place where Member State law applies by virtue of public international law"[86].

If on the one hand the regulation strengthens the data protection principles already established by the DPD, such as purpose limitation and consent, it also introduces new concepts such as the right to portability and data protection by design and by default (Politou et al., 2022). While most of the principles introduced by the GDPR were favorably welcomed by the academic community and business organizations, two of them have been the object of disagreement and controversy due to their unprecedented impact: the right to withdraw consent and the right to be forgotten (RtbF) represent a

[83] European Commission, *Who does the data protection law apply to?* (https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en Accessed on 25/10/2024).
[84] Intersoft Consulting, *GDPR*, cit.
[85] Ibid.
[86] Ibid.

turning point in the context of data protection legislation on an international level due to their groundbreaking nature (Politou et al., 2022).

Since its enactment in 1995, the DPD represented the international standard for all data protection legislation, and its key principles are reinforced on the GDPR. Article 5(1) of the GDPR concerns “Principles relating to processing of personal data” and states that personal data shall be:

“

(a) processed lawfully, fairly and in a transparent manner […] (‘lawfulness, fairness and transparency’);
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […] (‘purpose limitation’);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
(d) accurate and, where necessary, kept up to date […] (‘accuracy’);
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed […] (‘storage limitation’);
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)”[87].

Article 5(2) establishes that the controller of data movement and processing shall be responsible for and able to demonstrate compliance with the above-mentioned data

[87] Intersoft Consulting, *GDPR*, Article 5(1) (https://gdpr-info.eu/issues/personal-data/, Accessed on 25/10/24).

protection principles (accountability). According to the GDPR, the controller is also held accountable for the protection of subjects' data through technical and organizational measures. Article 25 GDPR ('Data protection by design and by default') states that the controller shall "implement appropriate technical and organisational measures […] which are designed to implement data-protection principles […], and to integrate the necessary safeguards into the processing in order to meet the requirements"[88] established by the Regulation. Therefore, the controller must ensure that only the personal data necessary for the specified purpose are processed, collected, and accessed. The measures adopted to do so should also ensure that such data will only be stored for a determined amount of time and will not be accessible by third parties without the individual's intervention[89].

3.4 Data Subject Rights under GDPR

Besides the above-mentioned, the GDPR introduces some new rights regarding data protection that represent an unprecedent element of novelty. Chapter 3 of the GDPR, namely 'Rights of the data subjects', contains the provisions on how subjects' data must be handled specifying the modalities, access to personal data, rectification and erasure, right to object and automated decision making, and restrictions for data controllers and processors. The regulation not only strengthens the principles already specified in the 1995 DPD, but also reinforces the measures on data protection by introducing the right of access by data subject (Article 15), the right to rectification (Article 16), right to erasure or 'right to be forgotten' (Article 17), right to restriction of processing (Article 18), right to data portability (Article 20), and right to object (Article 21). Among these, the right to withdraw consent (Article 7(3)) and the right to be forgotten (RtbF) represent the two most controversial principles introduced by

[88] Intersoft Consulting, *GDPR*, cit., Article 25
[89] Ibid.

the GDPR and derived from fundamental concepts of data protection (Politou et al., 2022).

3.4.1 Access to Personal Data

Article 15 of the GDPR ('Right of access by the data subject') states that data subjects have the right to know if their personal data are being processed by the controller and, if that is the case, to also access such data and any information regarding:

"

> the purposes the of the processing; the categories of personal data concerned; the recipients […] to whom the personal data have been or will be disclosed […]; where possible, the envisaged period for which the personal data will be stored, […]; the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing […]; the right to lodge a complaint with a supervisory authority; where the personal data are not collected from the data subject, any available information as to their source; the existence of automated decision-making, […] as well as the significance and the envisaged consequences of such processing for the data subject."[90]

Data subjects have the right to be informed about any transfers of their personal data to third countries or international organizations. Moreover, according to Article 15(3), the controller shall provide a copy of the personal data undergoing processing.

[90] Intersoft Consulting, *GDPR*, cit., Article 15

3.4.2 Rectification, Restriction, and Data Portability

Article 16 of the GDPR ('Right to rectification') states that data subjects have the right to obtain any rectification of inaccuracies in their personal data and shall have their incomplete personal data completed by the controller.

The Right to data portability (Article 20 GDPR) ensures that the data subjects shall receive the data their provided to the controller in a "structured, commonly used and machine-readable format"[91]. Moreover, the data subject has the right to transmit such data to another controller directly and where technically feasible.

Article 18 ('Right to restriction of processing') lists all the cases in which the data subject has the right to obtain restriction of processing from the controller including the case of the processing of data being unlawful, the accuracy of personal data being contested, or when the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims. Consequently, the data may be only stored by the controller but not further processed (Politou et al., 2022).

3.4.3 Right to Object

The Right to object (Article 21) was already specified in the 1995 DPD where "compelling legitimate grounds must be demonstrated by the data subject in order to object to the processing of personal data" (Politou et al., 2022, p. 22). However, the GDPR expanded the previous definition of this right and places the burden on the data controller that is responsible for demonstrating compelling legitimate grounds when the data subject objects to the processing of his or her data (Politou et al., 2022). According to Article 21 GDPR, the controller shall interrupt the processing of data

[91] Intersoft Consulting, *GDPR*, cit., Article 20

when requested by the data subject, unless the controller can demonstrate legitimate grounds for the processing such as interests, rights and freedom of the data subject, or the establishment, exercise or defense of legal claims (Article 21 (1)), but also if the processing is necessary for reasons of public interest (Article 21(6)). The only case mentioned in the Article in which data subjects can object to the processing of their data at any time is for direct marketing purposes (Article 21(2-3)).

3.4.4 Right to Erasure

Article 17 of the GDPR introduces the Right to erasure or Right to be Forgotten (RtbF) which has caused long debate among academics and business organizations for its groundbreaking impact on data protection legislations. One of the most important concepts introduced by the RtbF is retro-activity which allows the retro-active erasure of a subject's personal data from every data controller who is processing them, and not only the one who originally collected them (Politou et al., 2022).

The RtbF was first put forward back in 2012 to face the emerging challenges posed by the digital world, and in the wake of many European countries where the Right to Oblivion was anticipated (Politou et al., 2022). The RtbF encompasses the domain of the right to privacy and an individual's right to personal identity as it embraces not only the right to erase (need for a controller to delete data), but also the right to be forgotten which implies that the data will have to be removed from all possible sources that may contain them (Politou et al., 2022).

Article 17(1) of the GDPR lists all the cases in which the data subject has the right to obtain the erasure of own data including when personal data are no longer necessary (a), when data subject withdraws consent to processing (b), or when personal data have been unlawfully processed (d). The burden of the erasure of personal data is placed on the controller who is also responsible for informing other controllers which are processing such data that the data subject requested the erasure of any links, copy or replication of those personal data (Article 17 (2)). The erasure cannot be obtained when the processing of personal data is necessary for exercising fundamental rights, for compliance with legal obligations, reasons of public interest or legal claims (Article 17 (3)).

Resistance against the implementation of this right comes from multiple sources and for many different reasons. Free speech advocates claim that the RtbF represents a threat to expression and free speech on the internet because it doesn't apply only to the data directly provided by individuals, but also to all possible cases of data that may be found online[92]. Others label this Right as censorship and disastrous for the freedom of expression[93] claiming it can be seen as an antisocial act for its neglection of the role played by society in everyone's life. Scientists also warn that the enforcement of the RtbF would lead to preventive actions in the collection of data, such as the anonymization of databases per default, causing the loss of valuable amount of data (Malle et al., 2016)[94]. As Politou et al. (2022) state, another area of criticism comes from the fact that the enforcement of this right may represent an obstacle in data transfer between the EU and third countries.

3.4.5 Right to Withdraw Consent

Article 7 of the GDPR lists the conditions for consent and introduces in Section 3 the Right to withdraw consent, a fundamental concept of data protection and, at the same

[92] Fleischer, Peter; *The rights to be forgotten, or how to your your history*, in "Peter Fleischer: Privacy...?", 2012 (http://peterfleischer.blogspot.gr/2012/01/right-to-be-forgotten-or-how-to-edit.html, Accessed on 01/11/2024).

[93] Solon, Olivia; *EU 'right to be forgotten' ruling paves way for censorship*, in "Wired", 2014 (http://www.wired.co.uk/article/right-to-be-forgotten-blog, Accessed on 01/11/2024).

[94] Malle, B.; Kieseberg, P.; Weippl, E.; Holzinger, A.; *The right to be forgotten: towards machine learning on perturbed knowledge bases*, in "International Conference on Availability, Reliability, and Security", Springer, 2016, pp. 251–266

time, a source of disagreement for many. Consent aims at providing legitimate grounds for collecting and processing personal data for secondary use (Politou et al., 2022) and must be requested in a clear and concise way specifying what use will be made of personal data[95]. Consent must be freely given, unambiguous, specific and informed, and its request must include details on how to contact the company that is processing the data[96].

Article 7(3) states that data subject has the right to withdraw his or her consent at any time, and the withdrawal must be as easy as giving consent. The controller shall be able to demonstrate that the processing of data is based on the data subject consent (Article 17(1)).

The debate about consent can be distinguished into two main opinions. On the one hand, scholars believe that consent requirements represent the ultimate chance for individuals to have control over their personal information processing (Politou et al., 2022). On the other hand, many radical voices argue that requesting subjects' consent to process their data may jeopardize innovation and beneficial societal advances (Tene and Polonetsky, 2013)[97], so it should be required only for a limited number of specific cases.

3.5 Enforcement Mechanisms and Penalties in the EU

Article 82(1) of the GDPR states that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right

[95] European Commission, *How should my consent be requested?* (https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_en, Accessed on 02/11/2024).

[96] Ibid.

[97] Tene, O.; Polonetsky, J.; *Big data for all: Privacy and user control in the age of analytics*; Nw. J. Tech. Intell. Prop. 11, xxvii, 2013.

to receive compensation from the controller or processor for the damage suffered”[98]. Data Protection Authorities (DPAs) are responsible for the enforcement of the Regulation in each Member State and can impose fines as well as corrective actions on organizations violating the rules[99]. Compliance with the rules imposed by the GDPR is not mandatory only for EU based companies, but also for the ones based outside of the European territory if they process EU residents’ data. Although compliance with the strict rules imposed by the GDPR represents an additional burden for companies, adhering to the Regulation’s requirements can have a positive impact on a company reputation by building its stakeholders and customers’ trust, demonstrating commitment to subjects’ data protection, and ultimately enhancing the competitiveness in the market[100].

Article 83(2) lists the criteria to establish the amount of the administrative fine to be imposed for violations of the Regulation including the nature, gravity and duration of the infringement (a), the intentional or negligent character of the infringement (b), the degree of cooperation with the supervisory authority (f), and the categories of data affected by the infringement (g).

The GDPR establishes two different categories of administrative fines that can be imposed based on the seriousness of the infringement. For less serious infringements, the Regulation establishes fines up to €10 million or 2% of annual turnover (whichever is higher) (Article 83 (4)). This applies to violations of Article 8 (conditions applicable to child’s consent in relation to information society services), Article 11 (processing which does not require identification), Article 25-39 (general obligations of controllers and processors), Article 42 (certification), and Article 43

[98] Intersoft Consulting, GDPR, cit., Article 82(1)
[99] GDPR Advisor, *GDPR Fines and Penalties: what you need to know to avoid costly mistakes* (https://www.gdpradvisor.co.uk/gdpr-fines-and-penalties, Accessed on 02/11/2024).
[100] Ibid.

(certification bodies)[101]. The second category includes infringements considered more serious because of their violation of the core principles of data protection for which the fines are up to €20 million or 4% of annual turnover (Article 83 (5)). This applies to violation of Article 5 (principles relating to processing of personal data), Article 6 (lawfulness of processing), Article 7 (conditions for consent), Article 9 (processing of special categories of personal data), Articles 12-22 (rights of the data subject), and Articles 44-49 (transfers of data to third countries or international organizations)[102].

DPAs are responsible for enforcing penalties for GDPR violations through monetary fines, but they can also utilize other tools such as bans on data processing, mandatory audits, or orders to meet compliance standards[103]. Monetary fines and these other enforcement mechanisms are not mutually exclusive.

[101] Ibid.

[102] Ibid.

[103] Ibid.

Chapter 4:

Data Protection in the United States

4.1 Historical Context and Legislative Landscape

In many ways, the European GDPR represents the gold standard for data protection worldwide as it places the focus on the protection of individuals' data throughout their entire lifetime, ensuring that subjects' privacy and safety are always prioritized. If the European Union adopts a data protection approach, in the United States the dominant approach is grounded in consumer protection regulations (Boyne, 2018)[104]. Accordingly, it is the Federal Trade Commission (FTC), a U.S. federal agency whose objective is to protect consumers from deceptive or unfair business practices[105], the primary privacy enforcement agency (Boyne, 2018) since the 1970s. The peculiar political geography of the United States can be used to explain why there is no all-encompassing federal legislation regulating the protection of personal data: the Country relies on a combination of legislation at the federal and state levels, administrative regulations, and industry specific self-regulation guidelines (Boyne, 2018, p. 299). Contrarily to Europe, the United States data protection legislation at the federal level follows a sectoral approach protecting data within sector-specific contexts (Boyne, 2018).

[104] Boyne, Shawn Marie; *Data Protection in the United State*s, in "The American Journal of Comparative Law", Volume 66 (1), 2018, pp. 299-343

[105] Federal Trade Commission, *About the FTC* (https://www.ftc.gov/about-ftc, Accessed on 07/11/2024).

4.1.1 Evolution of Privacy and Data Protection in the U.S.

The U.S. Constitution officially came into effect in 1789 and represents the foundational document for the government of the country[106]. Even if it does not explicitly guarantee the right to privacy, the Supreme Court has found the Constitution to implicitly support a broader concept of privacy rights in its First, Third, Fourth, and Fifth amendments[107].

The first important step towards the creation of a privacy legal framework is the enactment of the Fair Credit Reporting Act (FCRA) in 1970. The FCRA is considered as the first data privacy legislation in the United States and its aim was to promote accuracy, fairness and the privacy of personal information, in particular for consumers' investigatory reports, credit reports, and employment background checks[108]. The Act's objective is to ensure the protection of consumers' data in the context of credit agencies by imposing limits on data sharing and making it easier for consumers to correct reporting errors (Boyne, 2018).

A few years later, in 1973, the Department of Health, Education, and Welfare (HEW) published the report 'Computers and the Rights of Citizens' on automated personal data systems[109]. The report gave origin to a set of practices - the Code of Fair Information Practices (FIPs) - which constitutes the foundation of modern privacy legislation[110], and binds organizations dealing with personally identifiable information to comply with the Code or be subject to government sanctions (Boyne, 2018).

[106] University of Michigan, *History of Privacy Timeline*, in "Safe Computing", 2024 (https://safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline, Accessed on 15/11/24).
[107] Ibid.
[108] Epic.org, *The Fair Credit Reporting Act (FCRA)*, (https://epic.org/fcra/, Accessed on 15/11/2024).
[109] University of Michigan, *History of Privacy Timeline*, cit.
[110] Ibid.

In 1974, the Congress passed the U.S. Privacy Act, a federal law that governs “the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies”[111]. The U.S. Office of Special Counsel describes a system of records as “any grouping of information about an individual under the control of a federal agency from which information is retrievable by personal identifiers, such as name, social security number, or other identifying number or symbol”[112]. The Privacy Act provides protection to individuals’ personal information by guaranteeing the right to request a change of their records whether they are inaccurate, incomplete or not relevant, the right to protection against unwarranted use of their personal information that may result in an invasion of their privacy, and the right to request their records[113]; however, the latter is subject to twelve specific exemptions cases that do not require the subject’s consent to release information. The main purpose of the Privacy Act is to limit the amount of information collected about individuals while, at the same time, balancing the government’s need to store and maintain its citizens’ data with the individuals’ privacy right[114].

In the following years, more steps were taken to protect American citizens’ privacy rights. In 1974, the Family Educational Rights and Privacy Act (FERPA), also known as Buckely Amendment, was passed to safeguard the privacy of student’s education records[115]. The U.S. Department of Education describes FERPA as a federal law that affords parents to have access to their children’s education records, seek to have the records amended, and have control over the disclosure of personal information that

[111] U.S. Department of Justice - Office of Privacy and Civil Liberties, *Privacy Act of 1974* (https://www.justice.gov/opcl/privacy-act-1974, Accessed on 15/11/2024).

[112] U.S. Office of Special Counsel*, The Privacy Act of 1974* (https://osc.gov/Pages/Privacy-Act.aspx, Accessed on 17/11/2024).

[113] Ibid.

[114] Defense Privacy and Civil Liberties Office, *Introduction to The Privacy Act* (https://dpcld.defense.gov/Portals/49/Documents/Privacy/2011%20DPCLO_Intro_Privacy_Act.pdf , Accessed on 17/11/2024).

[115] University of Michigan, *History of Privacy Timeline*, cit.

could potentially identify the student[116]. The rights guaranteed under FERPA are automatically transferred to the student once he or she turns 18 years old.

In 1991, President George Bush signs into law the Telephone Consumer Protection Act (TCPA), which is still considered as the primary federal law governing solicitation calls and telemarketing regulations, and the foundation for further legislation regarding communications and telemarketing[117]. The TCPA regulates telephone solicitations including voice calls, text messages, but also faxes and VoIP calls encouraging purchases, rentals, and investments of goods or services[118]. Related to the TCPA and the regulation of telemarketing calling is the National Do Not Call Registry, a national registry created in 2003 by the Federal Trade Commission to allow citizens to register their phone numbers to it and stop unwanted sales calls from companies and telemarketers that follow the law[119]. This means that registered telemarketers won't be able to call numbers registered to the Registry; however, it does not prevent scammers from making illegal calls.

In 1999, the first Chief Privacy Officer (CPO) was established in the United States when privacy lawyer Ray Everett-Church was appointed for the new role in the Internet advertising firm AllAdvantage[120]. A CPO is an executive responsible for data concerns and managing risks related to privacy as well as ensuring compliance with

[116] U.S. Department of Education, *What is FERPA?*, in "Protecting Student Privacy" (https://studentprivacy.ed.gov/faq/what-ferpa#:~:text=The%20Family%20Educational%20Rights%20and,identifiable%20information%20from%20the%20education , Accessed on 17/11/2024).

[117] Contact Center Compliance, *What is the TCPA*? (https://www.dnc.com/what-is-tcpa/ , Accessed on 17/11/2024).

[118] Ibid.

[119] Federal Trade Commission, *National Do Not Call Registry FAQs*, in "Consumer advice" (https://consumer.ftc.gov/articles/national-do-not-call-registry-faqs#:~:text=The%20Do%20Not%20Call%20Registry%20stops%20unwanted%20sales%20calls%20%E2%80%94%20live,from%20scammers%20making%20illegal%20calls, Accessed on 17/11/2024).

[120] Brown, Justine; *Rise of the Chief Privacy Officer*, in "Government Technology", 2014 (https://www.govtech.com/data/rise-of-the-chief-privacy-officer.html , Accessed on 17/11/2024).

information privacy laws[121]. The first role as CPO dates back to 1991, but the position was truly solidified when Harriet Pearson became CPO at IBM in November 2000[122].

A turning point in the history of the United States is represented by the terrorist attacks that took place on September 11, 2001. In the wake of these events, homeland security and surveillance measures became a priority for governments worldwide as the world was preparing to face the threat of terrorism. In response to the attacks and in the name of national security, the U.S. Congress passed the USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) signed into law by President George W. Bush in October 2001[123]. The Act strengthens the government's authority and power over telephone and electronic communications by expanding the search and surveillance powers of intelligence agencies with the main objective of investigating and surveilling suspected terrorists, but also combat money laundering and regulate immigration[124].

The following year, in 2002, the Congress passed the E-Government Act in an effort to apply the advances happening in information technology to the governmental functions and services to adapt to the changing relationships among citizens, businesses and Government[125]. The passage of the Act aimed at promoting the use of the internet and electronic government services, providing access to Government information and services, and ensuring transparency and accountability[126]. One of the main implications of the E-Government Act can be found on Section 208 of the law which requires that "all federal agencies conduct a 'privacy impact assessment' (PIA)

[121] University of Michigan, *History of Privacy Timeline*, cit.

[122] Brown, Justine; *Rise of the Chief Privacy Officer*, cit.

[123] Duigan, Brian; *USA Patriot Act*, in "Britannica", 2024 (https://www.britannica.com/topic/USA-PATRIOT-Act, Accessed on 18/11/2024).

[124] Ibid.

[125] Department of Justice – Office of Justice Programs, *E-Government Act of 2002* (https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1287 , Accessed on 18/11/2024).

[126] Ibid.

for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII), or for a new aggregation of information that is collected, maintained, or disseminated using information technology"[127].

In 2003, California was the first state to implement a Data Breach Notification Law: the new legislation requires any businesses and state agencies to notify residents within the state that their personal information was acquired or is believed to have been acquired by a third unauthorized party[128]. Another significant step towards ensuring data protection for U.S. citizens takes place in 2008 when the Federal Trade Commission (FTC) and the National Credit Union Administration (NCUA) implement the Red Flags Rule designed to prevent and address identity theft[129]. The Rule is enforced by the FTC and several other agencies, and it requires businesses and organizations to implement a specific prevention program with the aim of detecting red flags and suspicious patterns of identity theft in their daily operations, as well as addressing crime prevention and mitigating its damage[130].

4.2 Major Federal Data Protection Laws

In addition to the legislation subject to the FTC's jurisdiction, the U.S. data protection legislation landscape is characterized by a limited number of major federal data protection laws that apply to specific sectors or categories of data subjects (Boyne, 2018).

[127] Department of Justice – Office of Justice Programs, *E-Government Act of 2002*, cit.

[128] Bonta, Rob; *Data Security Breach Reporting*, in "Office of the Attorney General" (https://oag.ca.gov/privacy/databreach/reporting, Accessed on 18/11/2024).

[129] University of Michigan, *History of Privacy Timeline*, cit.

[130] Federal Trade Commission, *Fighting identity theft with Red Flags Rule: A how-to guide for business* (https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business , Accessed on 18/11/2024).

4.2.1 The Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) was enacted in 1986 to prevent and punish hacking-related activities (Boyne, 2018). Since its passage in 1986, the Act has been amended several times, most recently in 2008, to cover unauthorized access to protected computers, as well as access exceeding the scope of their authorization[131]. By ‘protected computers’, the Act refers to “those used by financial institutions, the U.S. government, and computers used in or affecting interstate or foreign commerce or communication” (Boyne, 2018, p. 304). The actions targeted include the trespassing of a protected computer resulting in exposure of the computer-housed information, damaging or threatening to damage a protected computer, committing fraud through unauthorized access, trafficking in passwords, and lastly accessing a protected computer to commit espionage (Boyne, 2018, p.337). Penalties for the violation of CFAA range from one year of imprisonment, to life imprisonment in case of death resulting from intentional computer damage (Boyne, 2018).

4.2.2 Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA) of 1986 includes the Stored Wire Electronic Communications Act and represents the updated version of the 1968 Federal Wiretap Act which did not apply to computers and digital communications[132]. The ECPA protects wire, oral, and electronic communications including emails, telephone conversations, and data stored electronically throughout their lifetime, from when they are being made, to their transit, and lastly when they are stored in

[131] National Association of Criminal Defense Lawyers*, Computer Fraud and Abuse Act (CFAA)* (https://www.nacdl.org/Landing/ComputerFraudandAbuseAct , Accessed on 18/11/2024).

[132] Department of Justice – Office of Justice Programs*, Electronic Communications Privacy Act of 1986 (ECPA)* (https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 , Accessed on 19/11/2024).

computers[133], and it is the primary federal law regulating the monitoring of electronic communications in the workplace (Boyne, 2018). The Act prohibits wiretaps of third parties' communications without court approval or the party's prior consent, and the use and disclosure of any information acquired through such illegal practices (Boyne, 2018, p. 304).

Title I of ECPA prohibits the interception, use, disclosure, or procurement of any type of communication, and the use of it as evidence; Title II protects files and records held by service providers about subscribers, including their name, billing records, and IP addresses; Title III requires government entities to obtain court approval for the installation and use of a pen register and a trap and trace device utilized for the interception of communications[134].

4.2.3 The Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act was enacted in 1970, and it applies to consumer reporting agencies who use consumer reports and provide consumer reporting information (Boyne, 2018). Consumer reports are documents issued by consumer reporting agencies regarding "a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer's eligibility for credit or insurance" (Boyne, 2018, p. 304). The FCRA establishes a fraud alert whenever identity theft is suspected together with a notification informing victims of their rights, and a free annual credit report to consumers from the top credit reporting agencies (Boyne, 2018).

[133] Ibid.

[134] Ibid.

4.2.4 Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes federal standards protecting sensitive health information from disclosure without patient's consent[135]. To implement the requirements established with this law, the US Department of Health and Human Services issued the HIPAA Privacy Rule, a set of standards to regulate the use and disclosure of individuals' protected health information, but also to inform them about their rights[136]. The HIPAA Privacy Rule establishes a set of requirements with the aim of promoting high-quality healthcare while, at the same time, protecting subjects' health information and privacy. It also requires health care entities and contractors to adopt any administrative and technical measure to safeguard and protect the confidentiality, integrity, and availability of protected information (Boyne, 2018). The US Department of Health and Human Services is responsible for imposing monetary penalties on violators based on the level of negligence involved (Boyne, 2018). Like most U.S. data protection legislation, HIPAA is considered sector-specific meaning that it targets health care entities and a restricted category of businesses that contract with health care entities to protect individually identifiable health information (Boyne, 2018, p. 335).

4.2.5 Financial Services Modernization Act (Gramm–Leach–Bliley Act)

The Financial Services Modernization Act, more commonly known as Gramm-Leach-Bliley Act (GLB), was enacted in 1999 to protect consumers' nonpublic personal information when used by financial institutions (Boyne, 2018, p. 302). By 'nonpublic

[135] U.S. Center for Disease Control and Prevention, *Health Insurance Portability and Accountability Act of 1996 (HIPAA*), in "Public Health Law" (https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html , Accessed on 19/11/2024).

[136] Ibid.

personal information', the Act refers to personally identifiable financial information that is provided or obtained by a financial institution (Boyne, 2018).

Title V of the Act requires financial institutions to protect the privacy of consumers' personal financial information by developing and giving notice of their privacy policies at least once a year; moreover, consumers' must have the right to opt out from any disclosure of their personal financial information to such institutions' unaffiliated third parties[137]. In case of data breach, the financial institution must investigate whether customers' information has been or will be misused and, if so, customers' must be notified immediately (Boyne, 2018).

Penalties for violation under the GLB Act vary depending on the agency that brings the enforcement action, whether it is the Federal Trade Commission or the Federal Consumer Financial Protection Bureau, ranging from monetary sanctions to imprisonment (Boyne, 2018, pp.320,339).

4.2.6 Children's Online Privacy Protection Act (COPPA)

The U.S. Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998, but it only became effective in April 2000 after the issuing of the Children's Online Privacy Protection Rule[138].

The COPPA Act imposes specific requirements for online operators providing services or collecting personal information from children under 13 years of age: operators are required to provide notice to parents and obtain their consent "before

[137] Federal Trade Commission, *Gramm-Leach-Bliley Act* (https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act , Accessed on 20/11/2024).

[138] National Archives and Records Administration, *Children's Online Privacy Protection Rule*, in "The Daily Journal of the United States Government" (https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule , Accessed on 20/11/2024).

collecting, using, or disclosing personal information from children under 13 years of age" (16 CFR 312.3, 312.4, and 312.5.)[139]. Furthermore, parents can review the categories of personal information collected from their children, delete it, and prevent further use of future collection of such information[140].

4.2.7 Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)

In 2003 the Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) to address unwanted commercial electronic mail messages and to protect consumers from such messages received through email and wireless devices such as mobile phones[141].

The CAN-SPAM Act establishes requirements applicable to entities sending unsolicited commercial emails including the ban of false or misleading information and prohibiting deceptive subject lines[142]. Furthermore, the Act requires the labeling of sexually explicit commercial emails as such, and the provision of an opt-out option[143]. The Act regulates commercial and transactional emails, establishing that such emails must include non-deceptive sender and subject information, and a clear identification that the message is an advertisement or solicitation; entities failing to do so will be subject to criminal penalties (Boyne, 2018, p. 303).

[139] National Archives and Records Administration, *Children's Online Privacy Protection Rule*, cit.
[140] Ibid.
[141] Federal Communications Commission, *CAN-SPAM* (https://www.fcc.gov/general/can-spam , Accessed on 20/11/2024).
[142] Federal Trade Commission, *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act*) (https://www.ftc.gov/legal-library/browse/statutes/controlling-assault-non-solicited-pornography-marketing-act-2003-can-spam-act , Accessed on 20/11/2024).
[143] Ibid.

4.2.8 California Consumer Privacy Act (CCPA)

The passage of the California Consumer Privacy Act (CCPA) in 2018 represents a milestone in the United States data protection legislation history: the Act is considered one of the first comprehensive, state-specific data protection laws in the country significantly impacting the way businesses handle consumers' data and giving input to the other states to adapting their regulations. The CCPA had repercussions all over the country, influencing other states to comply with its regulations and provisions.

California's paradigm-shifting California Consumer Privacy Act (CCPA), which was enacted in 2018, was later amended through a ballot in 2020 with the California Privacy Rights Act (CPRA) introducing, among the others, new materials regulating data collection in the workplace[144]. The aim of the CCPA is to give consumers more control over the collection of their personal information including the right to know how the information is used and shared, how to limit its use, how to delete it, and the right to opt-out[145]. Ensuring consumers' this set of rights over their personal information represents an unprecedented milestone, empowering individuals to take control of their data.

The law requires businesses to give consumers a 'notice a collection' containing all the categories of personal data collected and the purposes for which they are being collected[146].

After California passed its Consumer privacy law in 2018, other states followed its example and started considering similar legislation. The U.S. legislation on data

[144] Squire Patton Boggs, *Overview of Privacy and Data Protection Laws: United States*, in "Privacy world" (https://www.privacyworld.blog/summary-of-data-privacy-protection-laws-in-the-united-states/ , Accessed on 21/11/2024).

[145] Bonta, Rob; *California Consumer Privacy Act (CCPA)*, in "Office of the Attorney General", 2024 (https://oag.ca.gov/privacy/ccpa , Accessed on 21/11/2024).

[146] Ibid.

protection and privacy is still fragmented at a sectoral and state level, however, state laws do possess some similarities with the GDPR (Fefer and Archick, 2020)[147].

U.S. policymakers and members of the Congress have expressed the need for a comprehensive national legal framework on data protection and privacy as the GDPR is projected to set a new global standard on these fields, and the risk of being shut out of the EU market would not only severely penalize U.S. firms, but could also limit the Country's influence in global trade negotiations (Fefer and Archick, 2020).

[147] Fefer, Rachel F.; Archick, Kristin; *EU Data Protection Rules and U.S. Implications*, in "Congressional Research Service", Version 11, 2020.

Chapter 5:

US and EU Legislation Comparative Analysis

5.1 Philosophical Differences: Fundamental Rights vs. Consumer Protection

The reasons behind the European and U.S. data protection legislation being so far apart can be found in a fundamental philosophical difference between the two that involves economical, historical and cultural reasons. The main difference between the U.S. and European data privacy framework is the importance attributed to the consumers' personal data protection: on one hand, Europe regulates and safeguard the individual's privacy as a fundamental right protected by European institutions and laws; on the other hand, the United States prioritizes the digital market and its growth, made possible by the collection and processing of huge amounts of data from American citizens.

5.1.1 The United States Framework

Contrarily to most countries, the U.S. legislation regulating privacy and data protection is not comprehensive nor unitary, but rather a patchwork of sector and state specific laws regulating how data can be collected, processed and stored depending on the industry of the organization collecting the data, and the territory[148].

[148] Squire Patton Boggs, *Overview of Privacy and Data Protection Laws: United States*, in "Privacy world" (https://www.privacyworld.blog/summary-of-data-privacy-protection-laws-in-the-united-states/ , Accessed on 21/11/2024).

The United States personal data framework is based on the marketplace and the conception of data marketability (De Bruin, 2022)[149]. According to this view, the digital market is the priority and everything else revolves around it, including consumers' personal data. The individual becomes a "trader of a personal commodity" which is represented by his or her personal data and is placed into this digital space unknowingly or without prior consent (De Bruin, 2022, p.130). Consequently, people's personal data becomes a commodity in the marketplace, and privacy laws are formulated accordingly.

This concept of data as a commodity for the market has been reinforced by the positive financial impact on the country's economy brought by technology companies that shaped the legal framework with the aim of protecting this sector's growth and future revenues (De Bruin, 2022). In recent years, the Obama Administration tried to balance both interests, the consumers' and the technology sector operators', by promoting the protection of consumers' trust while establishing more flexible privacy models (De Bruin, 2022). Nevertheless, the U.S. Constitution represents an obstacle in this shift of power from data processors to the consumers. Under the U.S. Constitution, the strongest protections are granted to data processors which represents a clear sign of the importance attributed to innovation as opposed to the consumers' right to information privacy (De Bruin, 2022); moreover, the Constitution has limited reach in the area of individual rights and does not require the government to create the conditions for the existence of fundamental rights (De Bruin, 2022, p.131). De Bruin (2022, p. 132) explains that through the State Action Doctrine[150] "individual liberties

[149] De Bruin, Ruben; *A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence*, in "Hastings Science and Technology Law Journal", Volume 13 (2), Article 4, 2022, pp.126-166

[150] Adherence to the State Action Doctrine requirements preserves individual freedom by limiting the reach of federal law and judicial power, avoids imposing responsibility on the State for what they cannot be blamed for, and it establishes that courts respect the limits of their own power (https://www.law.cornell.edu/constitution-conan/amendment-14/state-action-doctrine , Accessed on 22/11/2024).

shall be protected by ensuring that private action is not subject to constitutional limitations"[151]; this means that the Constitution prioritizes private action by not subjecting it to constitutional limitations, therefore, if a private company collects data from individuals without their notice or prior consent, the Doctrine prevents the application of individuals' rights because the actors are private (De Bruin, 2022, p.132).

This once again shows that the technological development and economic growth made possible with the acquisition of consumers' personal data, serve as an explanation of why the U.S. still does not have, and will likely not work on having, a holistic and comprehensive data privacy legislation. The current framework fails to recognize the cost of this lack of protection for consumers' privacy and keeps increasing policies in favor of the expansion of digital technology giants that make the current digital advancements possible (De Bruin, 2022).

5.1.2 The European Union Framework

The historical events that took place in Europe in the 20th century can be used to understand the current data privacy framework that governs individuals' personal data collection and processing.

Major historical events, above all the World War II, sparked the emergence of fundamental rights and the recognition of concepts such as dignity and personality that became central in European States' legal systems (De Bruin, 2022); however, it is not until the entry into force of the Italian (1947) and German (1949) Constitution that these rights start being incorporated into European's legal orders (De Bruin, 2022). The continent's experiences with totalitarian regimes sparked the creation of a

[151] Stephan, Jaggi; *State Action Doctrine*, Oxford Constitutional Law, 2017 (https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e473).

post-war identity and originated the interest in protecting individuals' privacy and personal data as a fundamental right and element of the European legal framework (Schwartz and Peifer, 2010)[152] anchored to concepts such as personality, dignity, and self-determination. The new role played by these fundamental values shaped the EU data privacy framework into a "rights-based perspective centered on the individual whose data is processed" (De Bruin, 2022, p.134).

The European Court of Justice and the European Court of Human Rights are the two main institutions governing and protecting the fundamental rights system and, in doing so, they apply two main documents, namely the Charter of Fundamental Rights and the European Convention of Human Right: the former serves as a constitutional document of the EU, whereas the latter represents an international treaty binding contracting states (De Bruin, 2022). The European data protection framework, contrary to the U.S. view, places the individual in a central position considering him or she as the ultimate bearer of rights.

The U.S. approach is based on the marketability and transferability of data as essential for the promotion of innovation and economic growth: this view stems from the positive impact brought into the U.S. economy by technology companies, therefore the ultimate goal of the law has turned out to be protecting the sector and its continuous growth (De Bruin, 2022). On the other hand, the EU shaped its data protection framework based on the 'lessons' learned throughout its history, from the two World Wars to the Cold War and the surveillance and data gathering practices that characterized those times (De Bruin, 2022): the current legal framework aims at protecting the individual's dignity, personality, personhood and autonomy with the objective of preserving peace in the continent (De Bruin, 2022).

[152] Schwartz, Paul M.; Peifer, Karl-Nikolaus; *Prosser's Privacy and the German right of Personality: Are Four Privacy Torts Better than One Unitary Concept*?, 98 CAL. L. REV. 1925, 1948-49 (2010).

5.2 EU legislation and U.S. Implications

As mentioned above, in contrast to the U.S., the European Union prioritizes the individual in the decision-making process regarding data protection, and the interests of data processors are not considered particularly relevant. This power balance between individuals and data processors began to pose issues and new challenges in the international law landscape. In particular, the official enactment of the European GDPR in May 2018 had repercussions not only within the European Union Member States, but also outside its borders. In particular, the GDPR prompted debate among U.S. companies and stakeholders with commercial relations in the EU for the challenges it poses on these relations.

Data from Eurostat[153] show that in 2023 the United States was the largest European partner for exports of goods (19.7%) and the second largest partner for EU imports of goods (13.7%) creating transatlantic transactions for more than 400 billion euros in 2023 as shown on the chart below. Between 2022 and 2023, both exports to and imports from the United States increased considerably compared to the previous years examined with petroleum oils being the most imported goods from the United States, and medicinal and pharmaceutical products being the most exported goods to the US.[154]

[153] Eurostat, *USA-EU - international trade in goods statistics*, 2024 (https://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_in_goods_statistics , Accessed on 22/11/2024).
[154] Ibid.

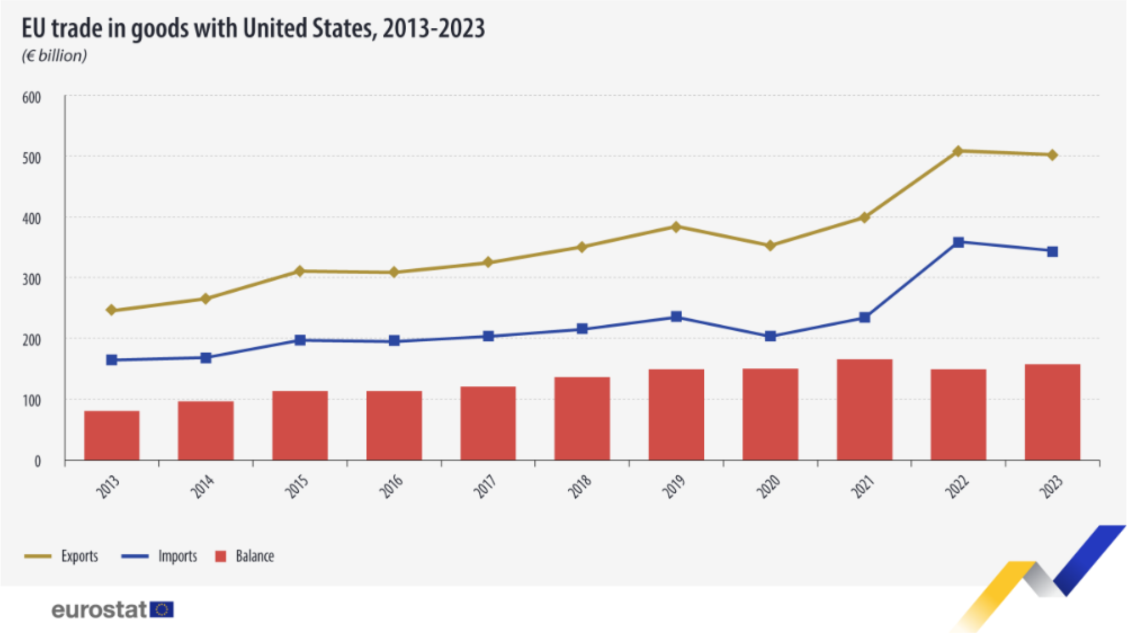

Figure 2 - EU trade in goods with United States (in billion euros), 2013-2023

Source: Eurostat. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_in_goods_statistics (Accessed on 22/11/24).

The transatlantic flow of data is now considered as a form of international trade for the fundamental value represented by consumers' data in today's economy. This flow of data is of critical importance for the European and U.S. economies as they remain each other's largest trade and investment partners (Weiss and Archick, 2016)[155]. The commercial relationships between the EU and the United States have, therefore, been greatly impacted by the new regulations in data transfers and data protection safeguards imposed by the EU law, with major U.S. firms voicing concerns about the GDPR, including the possible high costs for adhering to the Regulation and the need to construct a compliance bureaucracy (Fefer and Archick, 2020)[156].

[155] Weiss, Martin A.; Archick, Kristin; *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, in "Congressional Research Service", 2016, pp. 1-16

[156] Fefer, Rachel F.; Archick, Kristin; *EU Data Protection Rules and U.S. Implications*, in "Congressional Research Service", Version 11, 2020

The GDPR establishes a set of rules for the protection of personal data, and identifies the conditions for data processing, retention, storage limitation, and record keeping (Fefer and Archick, 2020), setting out a balance between the free flow of information and the protection of the data involved granting a privileged position to data subjects that is substantially different from the American one (De Bruin, 2022). As previously mentioned, the GDPR does not apply to European citizens only. The Regulation ensures the protection of data not only of EU residents, but also of any individual physically present in the European territory. Moreover, the GDPR applies to all businesses with an establishment in the EU, and that process data of individuals in the EU, regardless of where the processing takes place, and to all the businesses outside of the EU that offer goods and services or monitor the behavior of individuals in the EU (Fefer and Archick, 2020). Each Member State reports to a national Data Protection Authority (DPA) that supervises the enforcement of the GDPR and assesses fines for non-compliance.

In light of the billion-euros commercial relationships between US and EU firms, the former had to revise their data collection and processing terms to comply with European regulations. One of the main concerns voiced by US firms is the cost of adhering to European Regulations which can result in large resources invested in professional figures in charge of compliance with such laws (Fefer and Archick, 2020). This could discourage smaller firms from entering the European market and, consequently, create a trade barrier; furthermore, some US companies that already had businesses established in the European market opted to exit its market after the enforcement of the GDPR given the complexities and costs of adhering to its rules (Fefer and Archick, 2020). Another important consideration comes from industry surveys showing that American companies see GDPR's restrictions on the use and sharing of data as a possible barrier to the future development of new technologies and the innovation field, limiting new merges and acquisitions as well (Fefer and Archick, 2020).

5.3 EU Regulations on Data Transfers

Beyond safeguarding the privacy and data of individuals, the EU also protects the free flow of information (De Bruin, 2022, p.136). The right to data protection is mentioned in Article 8 of the Charter of Fundamental Rights of the European Union which also includes an extraterritorial dimension to it; accordingly, Chapter V of the GDPR establishes a system for the transfer of subjects' data from the EU to third countries, guaranteeing the right to continuous protection of such data (Naef, 2023, p.114)[157].

Data protection laws have always included regulations on data transfers in EU history beginning from the early 1970s; the first attempt at harmonizing the legislation on data transfers was in 1995 with the Directive 95/46/EC that served as a foundation for the rules consolidated with the GDPR in 2018 (Naef, 2023, pp.115-116).

The first draft of Directive 95/46/EC was formulated in 1990 and established that the transfer of personal data from an European Member State to a third country was only possible if the level of protection ensured by the third country was adequate, which should be interpreted as "protection essentially equivalent to that guaranteed within the European Union" (Naef, 2023, p.124). However, during the draft consultations, business associations started voicing their concerns regarding the trade barriers raised by the draft to international commercial relations with third countries not guaranteeing such level of protection, which led to a new amended version of the draft in 1992 (Naef, 2023): Article 27 of the amended draft authorized the transfer of data to these

[157] Naef, Tobias; *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, in "European Yearbook of International Economic Law", Volume 28, Springer, 2023

countries only in cases where the data exporter could demonstrate sufficient justification in the form of contractual provisions (Naef, 2023, p.125). Directive 95/46/EC was finally adopted in 1995 but, soon after, its case-by-case decision making system started revealing its inadequacy and a process to optimize its functioning was initiated.

5.3.1 Data Transfers under GDPR

It was with the adoption of GDPR in 2016 that the EU rules on data transfers were finally consolidated and harmonized at a Union level on the base of Directive 95/46/EC, leaving no room to Member States to implement individual rules (Naef, 2023).

The European system of data transfers is based on two major policy objectives, namely anticircumvention and protection of fundamental rights, and trust in the information society (Naef, 2023). The aim of the early European data protection laws was to regulate the export of personal data to avoid the circumvention of their rules and the consequent erosion of their level of data protection once such data arrived in third countries, therefore, the Union objective of anticircumvention is closely related to the safeguard of the fundamental right to continuous protection of personal data (Naef, 2023). The second objective, namely enhancing trust in information society, derives from the conception that considers the consumer's lack of confidence in an effective protection of personal data and privacy by the information society as a threat to the latter's development and, at the same time, as a precondition for the social acceptance of digital networks and services (Naef, 2023). Trust in the information society is therefore necessary for the development of digital trade and the consumers' acceptance of digital services.

Chapter V GDPR is dedicated to 'Transfers of personal data to third countries or international organisations'. The GDPR does not provide a specific definition of data transfers, but it does identify certain criteria for them: first, the controller or processor is subject to the GDPR for the given processing; the controller discloses or makes the data available to another organization; said organization is established in a country outside the EEA territory or is an international organization[158].

To transfer personal data to countries outside of the European Economic Area (EEA), organizations must comply with GDPR regulations by transferring data under three main conditions: the transfer must be to a country deemed as adequate in terms of data protection; the transfer must be through EU-approved standard contractual clauses or using legally binding corporate rules (Fefer and Archick, 2020). Personal data transfers to non-EEA countries or international organizations will only be possible if the conditions under Chapter V of the GDPR, as well as all the other rules established in this Regulation, are respected.

The GDPR identifies two main ways to transfer data to third countries which are on the basis of an adequacy decision or of appropriate safeguards[159]. Article 45 GDPR regulates transfers on the basis of adequacy decisions establishing that such transfers may take place "where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection"[160]. The criteria on which this assessment is based on include the rule of law, respect for human rights and fundamental freedoms as well as relevant legislation (Article 45, 2(a)), the existence and effective functioning of supervisory authorities enforcing and ensuring

[158] European Data Protection Board, *International Data Transfers*, in "Data Protection Guide for Small Business" (https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en , Accessed on 27/11/2024).

[159] Ibid.

[160] Intersoft Consulting, *GDPR*, cit., Article 45

compliance with data protection rules (b), and the international commitments, obligations, or participation in systems of such country or organization in relation to the protection of personal data (c). Article 46 GDPR regulates the transfers subject to appropriate safeguards establishing that, in the absence of an adequacy decision, the transfer can take place only if the controller or processor provides appropriate safeguards, and if enforceable data subject rights and legal remedies are available (1).

The third available condition for data transfers under the GDPR are binding corporate rules. Article 47 establishes that the competent supervisory authority shall approve binding corporate rules provided that they are legally binding (Article 47, 1(a)), expressly confer enforceable rights to data subjects (b), and fulfil the requirements expressed in this Article text (c).

Two years after the implementation of the GDPR, the European Commission elaborated a review on the implementation of this Regulation stating that it met its objectives with overall success, and leaving space for external comments (Fefer and Archick, 2020). The U.S. Administration commented by expressing its concerns related to the safety of citizens considered as threatened by the hindering of the sharing of data for health research, terrorism prevention, and criminal investigation, as well as the concerns regarding the lack of coordination between Data Protection Authorities and the limits on data transfers (Fefer and Archick, 2020).

5.4 US - EU Data Privacy Agreements

Since the passage of the data protection Directive in 1995, the U.S. and European governments have been trying to find a common ground on the regulation of data transfers to ensure the continuation of their mutual relations and investment businesses relaying on data flows. The conceptual differences on which their respective legislations are based on are continuing to make it complicated to find an agreement that will respect the strict European rules and ensure the protection of data subjects' rights.

5.4.1 Safe Harbor Agreement

Following the passage of the DPD in 1995, the substantial differences between the EU and U.S. approaches to data protection became even more clear, and the risks for the transatlantic flow of data and commercial relationships between the two required an urgent compromise. Soon after the DPD in 1995, the EU and U.S. Governments started negotiating on a mechanism that would allow the latter to comply with the adequate level of protection required by the DPD (Weiss and Archick, 2016). An agreement was finally found in 2000 when the U.S. Department of Commerce issued the Safe Harbor Principles, which were approved and recognized soon after by the European Commission[161], which limited their extent to national security, law enforcement requirements, and public interest (Weiss and Archick, 2016).

The Safe Harbor Agreement is considered as the first attempt to find a solution to the issue of international data transfers to bridge the gap between the EU and U.S. legal approaches (De Bruin, 2022).

Under the Safe Harbor Agreement, a U.S. firm could self-certify its compliance to the seven established principles and related requirements to the American Department of Commerce and, consequently, its respect of the European data privacy standards as well (Weiss and Archick, 2016). As explained by Weiss and Archick (2016), the seven principles were as follows:

[161] Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 (Weiss and Archick, 2016, p.5).

“

1. Notice: an organization must inform individuals about the purposes for which it collects and uses information […];
2. Choice: An organization must offer individuals the opportunity to choose (opt out) […]. For sensitive information, individuals must explicitly opt-in […];
3. Onward Transfer: In transferring information to a third party, organizations must apply the Notice and Choice Principles […];
4. Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it […];
5. Data Integrity: Personal information must be relevant for the purposes for which it is to be used […];
6. Access: Individuals must have access to the information about them that an organization holds and must be able to correct, amend, or delete that information […];
7. Enforcement: Effective privacy protection must include mechanisms for verifying compliance […]”[162].

Other than the necessity to regulate the vast amounts of transatlantic data trades, the main reason that made the Agreement acceptable by the U.S. was that the negotiated standards made the notably strict EU principles more tolerable to its counterpart (De Bruin, 2022).

However, in October 2015, the Court of Justice of the European Union (CJEU) issued a decision effective immediately that invalidated the Safe Harbor Agreement following complaints brought to the Irish DPA concerning Facebook’s data transfers from its European servers to the U.S. ones in 2013 (Weiss and Archick, 2016). Since the CJEU Decision of invalidity of Safe Harbor, it no longer provides a legal basis for

[162] Weiss, M. A.; Archick, K.; *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, cit., pp.5-6

transatlantic data transfers. The CJEU opinion in ‘Schrems v. Data Protection Commissioner’ voided the Safe Harbor agreement and marked a turning point in the relations between Europe and the United States (De Bruin, 2022).

5.4.2 Privacy Shield

The discussions on a revision of the Safe Harbor Agreement provisions and efficacy began two years before its ultimate invalidation subsequently to increasing concerns from EU institutions. The concerns regarded some significant loopholes in the Agreement requirements, as well as its obsolescence caused by the rapid developments of internet and new technologies.

In light of all these factors compromising Safe Harbor, multiple European officials called on the European Commission to suspend it but faced rejection due to the Commission's concerns of possible repercussions on EU business interests and the transatlantic economy (Weiss and Archick, 2016). However, the European Commission agreed on weakness in the Agreement scheme and, in 2013, issued 13 recommendations to enhance its safety focusing on enhancing transparency, strengthening enforcement, ensuring redress, and limiting access of U.S. authorities to data transferred under Safe Harbor[163].

The first draft of the EU-U.S. Privacy Shield as a replacement to Safe Harbor was announced on February 2nd, 2016, by both countries’ officials that worked to make transatlantic data flows possible while also complying with the requirements established with the CJEU Decision (Weiss and Archick, 2016). The Privacy Shield can be understood as a mixture of European and American standards that incorporated both systems of data privacy models (De Bruin, 2022). Less than a month after the

[163] European Commission, “*European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows*,” press prelease, November 27, 2013 (http://europa.eu/rapid/press-release_IP-13-1166_en.htm)

draft, EU and U.S. officials released the full text and supporting documentation: the new framework maintained the seven principles established with the Safe Harbor and added liability as a new category, but also included a supplemental set of principles concerning "sensitive data, secondary liability, the role of data protection authorities, human resources data, pharmaceutical and medical products, and publicly available data" (Weiss and Archick, 2016, p.9). New to Privacy Shield are also a set of commitments from U.S. national security officials and a model for arbitrating disputes, but especially clear safeguards and transparency obligations, and effective protection of EU citizens' rights with several redress possibilities to address the concerns raised by the CJEU (Weiss and Archick, 2016).

The Privacy Shield soon began to raise concerns regarding data protection that led to its invalidation in 2020 by the Court of Justice of the European Union. This decision took place following a complaint lodged by Maximilian Schrems, an Austrian lawyer and privacy activist, with the Irish Supervisory Authority seeking to prohibit the transfer of his personal data from the European to the U.S. Facebook servers (Batlle and Van Waeyenberge, 2024)[164]. The Privacy Shield was finally annulled by the CJEU on July 16th, 2022, an event also known as 'Schrems II Judgment' (Batlle and Van Waeyenberge, 2024).

5.4.3 Data Privacy Framework

The first steps towards a new agreement between the EU and U.S. on data protection and transfers were taken in March 2022. The invalidation of the Privacy Shield also raised concerns about U.S. surveillance practices and the adequacy of protections for European citizens' data which led to the Executive Order 14086 'Enhancing

[164] Batlle, Sergi; Van Waeyenberge, Arnaud; *EU–US Data Privacy Framework: A First Legal Assessment*, in "European Journal of Risk Regulation", Vol. 15, 2024, pp. 191–200

safeguards for United States signals intelligence activities', an order adopted by the White House in October 2022 to provide additional safeguards and guarantees regarding the limitations on the protection of European citizens' data arising from US intelligence activities (Batlle and Van Waeyenberge, 2024, p. 193).

It is at this point that the European Commission decides to update the previous EU-US Data Privacy Framework (DPF) by adopting a new adequacy decision that would promote transatlantic data transfers and address the concerns raised with the Schrems II judgement (Batlle and Van Waeyenberge, 2024).

On May 11th, 2023, the European Parliament passed a resolution criticizing the EU-U.S. DPF, stating that it failed to provide "essential equivalence" in data protection and urged the European Commission not to adopt the framework in its current form (Batlle and Van Waeyenberge, 2024); however, on July 10, 2023, the European Commission proceeded to formally adopt the DPF without making any changes to the draft decision (Batlle and Van Waeyenberge, 2024).

The EU-U.S. Data Privacy Framework (DPF) operates as a partial adequacy decision, meaning that it applies only to those U.S. organizations that voluntarily adhere to its principles by completing a self-certification process overseen by the U.S. Department of Commerce (Batlle and Van Waeyenberge, 2024). All organizations adhering to DPF must comply with the seven core principles introduced with the Safe Harbor (notice, choice, accountability, security, data integrity, access, liability, and enforcement) and additional principles related to specific contexts and subjects (Batlle and Van Waeyenberge, 2024).

Additional safeguards and guarantees regarding the limitations on the data protection of European citizens arising from U.S. intelligence are the American government's response to the first requirement of the Schrems II judgment and are intended to address the CJEU demands for stronger privacy protections and limitations on surveillance practices (Batlle and Van Waeyenberge, 2024, pp.194-195).

The third key element of the DPF is the creation of a two-layer redress mechanism represented by a dual administrative body (Batlle and Van Waeyenberge, 2024): the first layer involves the Civil Liberties Protection Officer (CLPO), who reviews complaints but does not confirm or deny intelligence activities; the CLPO's response indicates either that no violation occurred or that measures have been implemented (Batlle and Van Waeyenberge, 2024). Complainants can appeal decisions to the Data Protection Review Court (DPRC), an independent body of judges appointed by the U.S. Attorney General: if necessary, a special attorney may represent the complainant's interests before the DPRC; however, the grounds for decisions remain classified at all levels (Batlle and Van Waeyenberge, 2024, pp.195-196).

In conclusion, while the Data Privacy Framework represents a further step forward in aligning U.S. practices with EU standards for fundamental rights and data privacy, significant challenges persist. The lack of transparency and judicial remedies in the U.S. approach further complicates compliance with EU law, especially under the Charter of Fundamental Rights (Batlle and Van Waeyenberge, 2024). Without further efforts to address these concerns, the framework risks future invalidation by the CJEU, incrementing legal uncertainty and raising criticism on the perspective of a possible Scherms III decision (Batlle and Van Waeyenberge, 2024).

The European and United States conceptual differences in privacy approaches have historically created friction in finding a mutually acceptable legal compromise, which is further confirmed by the two main historical precedents of attempts in finding a common ground on data protection regulations, namely the Safe Harbor (Schrems I) and the Privacy Shield (Schrems III) (Batlle and Van Waeyenberge, 2024). Given the ongoing shortcomings of the DPF, it is widely expected that it could potentially lead to a Schrems III case (Batlle and Van Waeyenberge, 2024).

Chapter 6:

Data Sharing in Healthcare and the Role of AI

6.1 The Intersection of Data Protection, Innovation, and AI in Healthcare

The integration of AI systems in healthcare represents a transformative shift that led to a new era in medical practices and patient care encompassing diagnostics, treatment strategies, all the way up to healthcare administration. Leveraging artificial intelligence in healthcare has significantly enhanced accuracy and efficiency in diagnosis and medical treatments but also made possible an increasing personalization of treatments that can now be tailored to the single patient's needs. By harnessing AI capabilities of processing and analyzing vast datasets with unprecedent accuracy, healthcare operators are now able to offer increased efficiency in healthcare delivery including therapies targeted to the patient's needs, prevention of diseases and accurate predictions that ultimately result in markedly improved patient outcomes (Williamson and Prybutok, 2024)[165]. AI's predictive capabilities are among the most groundbreaking shifts in the way diagnosis and treatments are carried out: by analyzing previously collected data, AI can make predictions enabling proactive interventions, contributing not only to the single patient's health and safety, but also to public health by identifying potential health risks for the population and disease patterns (Williamson and Prybutok, 2024, p.6).

The integration of artificial intelligence into healthcare goes beyond mere technological advancements: it marks a significant milestone in the approach to patients and in improving people's health, but it also revolutionized healthcare

[165] Williamson, S.M.; Prybutok, V.; *Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare*. Appl. Sci. 2024, 14, 675 (Available from: https:// doi.org/10.3390/app14020675).

operators' work by optimizing resources and time (Williamson and Prybutok, 2024). The data-based knowledge provided by AI systems functions as a fundamental ally in uncovering hidden patterns and details that are not always visible to the human eye, and with significant anticipation which enables preventive treatment of the patient's disease. However, the potential offered by these advanced systems requires constant human supervision to ensure the correct functioning of AI. The collaboration between a human agent and AI offers multiple benefits including mitigating human biases in decision-making in circumstances of stress and time pressure that could affect a person's mental process (Williamson and Prybutok, 2024). Nevertheless, it is fundamental to ensure that AI assists rather than overrides healthcare professionals in their autonomy and decision-making processes which has caused raising concerns about the need to maintain this balance in medical decisions (Williamson and Prybutok, 2024).

6.1.1 Challenges of AI-Powered Healthcare

Despite the multiple benefits brought by the integration of AI into healthcare, it also poses significant concerns related to the sensitivity of the data involved and the consequent vulnerability it exposes patients to. Projections on the growth of AI in the healthcare market show a 47.6% annual increase expected from 2023 to 2028 when the value of the market is expected to reach $102.7 billion, resulting from the increasing amount of healthcare data that is being constantly generated (Kamrul et al., 2024, p.2430)[166].

[166] Kamrul Islam Riad; Abdul Barek; Mostafizur Rahman; Shapna Akter Tahia Islam; Abdur Rahman; Raihan Mia; Hossain Shahriar; Fan Wu; Sheikh Iqbal Ahamed; *Enhancing HIPAA Compliance in AI-driven Health Devices Security and Privacy*, for "2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)", 2024, pp. 2430-2435

This new era in the health and medical domain brings profound ethical implications, highlighting the need for a comprehensive framework addressing these new challenges, and the need for an exploration of '*algorethics'* (the intersection between algorithm design and ethical considerations) (Lastrucci et al., 2024)[167]. The data used by AI technologies in healthcare are patients' sensitive health information concerning their medical records and current medical conditions and state. The sensitive nature of these data necessitates adequate regulation to safeguard patients' privacy and data from the risk of data breaches and misuse, amplified by AI's extensive reliance on such data (Williamson and Prybutok, 2024). The predictive capabilities of AI are only made possible by its ability to process and analyze extensive health datasets containing all kinds of patient's data, from their medical history to diagnostic information, up to their treatment outcomes which necessitate extreme focus on data integrity and security (Williamson and Prybutok, 2024, p. 6).

Another issue emerging from the training of AI algorithms with datasets is the potential for biases. Biases are the result of an algorithm training process based on datasets that are not representative of a diverse demographic population which would ultimately lead to unfair treatment of patients and inequitable health outcomes (Williamson and Prybutok, 2024, p. 6, 16). Mitigating these algorithm biases through the inclusion of diverse datasets reflecting diverse patient demographics is essential to ensure fairness, transparency, and an equitable treatment of patients in AI-driven healthcare (Williamson and Prybutok, 2024, p. 16).

[167] Lastrucci, A.; Pirrera, A.; Lepri, G.; Giansanti, D. *Algorethics in Healthcare: Balancing Innovation and Integrity in AI Developmen*t. Algorithms 2024, 17, 432 (Available from: https://doi.org/10.3390/a17100432).

6.1.2 Regulations on Ethical Implications

Governments worldwide and international organizations address the ethical implications of AI on the health domain through frameworks that encompass all aspects of these technologies and are often not specific to this sector. One of the most prominent actors in shaping the regulations on AI applied to healthcare is the World Health Organization (WHO), an international public health authority dedicated to ensuring a responsible and equitable development and use of AI technologies (Lastrucci et al., 2024). In June 2021, the WHO published a first guidance on this matter that served as the foundation for the new document released in 2024 on 'Ethics and governance of AI for health Guidance on large multi-modal models' (LMMs)[168]. LMMs are a type of fast-growing generative artificial intelligence technologies that have been widely applied to the healthcare domain for their ability to accept various types of data input (such as videos, text and images), their mimicry of human communication, and the ability to carry out tasks they were not explicitly programmed to perform[169]. The WHO guidance sets out over 40 guidelines for entities operating with this type of technology to ensure an appropriate use of LMMs across health care[170], and focuses on global health equity and a responsible use of AI across health sectors that respects human rights (Lastrucci et al., 2024). A fundamental contribution to AI regulation comes from the previously mentioned European Union's AI Act of 2024. This regulatory framework represents a comprehensive effort to regulate the usage of AI across all the Member States, with a focus on ethical practices and on how these technologies should be implemented in the health care domain (Lastrucci et al.,

[168] World Health Organization; *WHO releases AI ethics and governance guidance for large multi-modal models*, in "News", 18 January 2024; (https://www.who.int/news/item/18-01-2024-who-releases-ai-ethics-and-governance-guidance-for-large-multi-modal-models Accessed on: 17/12/2024).

[169] Ibid.

[170] Ibid.

2024). The EU AI Act sets legal standards aimed at balancing ethical responsibility with innovation in AI technologies and applications.

6.2 The Power of Health Data: Enabling Innovation Through Sharing

The sharing of health data holds a huge potential in terms of advancements in the medical field as well as drug discovery. A successful share of health data has been revealed to be fundamental for validating hypotheses in medical products development and therapies testing for its time and cost saving benefits.

6.2.1 The Role of Shared Health-Data in Advancing Medical Research, Drug Discovery and Innovation

The sharing of health data leverages information from previous similar medical cases to develop novel therapies for patients with similar conditions in a time-efficient manner that simplifies decision-making processes and supports the resulting outcomes, which can lead to important breakthroughs in disease treatment.

Medical products development is a complex and expensive process with a high degree of uncertainty that increases throughout the process together with the costs and risks associated with failure (Karpen et al., 2021)[171]. Data sharing initiatives can reduce both time and costs associated with medical product development and optimize clinical trials supporting innovation and improving public health (Karpen et al., 2021). According to Vention[172], AI will take over the healthcare sector in the procedures for

[171] Stephen R. Karpen; J. Kael White; Ariana P. Mullin; Inish O'Doherty; Lynn D. Hudson; Klaus Romero; Sudhir Sivakumaran; Diane Stephenson; Emily C. Turner; Jane Larkindale; *Effective Data Sharing as a Conduit for Advancing Medical Product Development*, in "Therapeutic Innovation & Regulatory Science", 2021, 55, pp. 591–600, (Available from: https://doi.org/10.1007/s43441-020-00255-8).

[172] Vention; *AI adoption statistics by industries and countries: 2024 snapshot*, in "Artificial Intelligence", 2024 (https://ventionteams.com/solutions/ai/adoption-statistics Accessed on 19/12/2024).

early diagnosis and remote patient monitoring, significantly improving patient outcomes. Data from Vention[173] also show that 1 out of 5 healthcare organizations worldwide started adopting AI systems in 2021 and, by the end of 2025, 90% of hospitals will implement AI technologies for early diagnosis and remote monitoring procedures. These developments in novel AI solutions are made possible by the increase in computational power but, more than anything, by the massive amounts of data available to train these systems and algorithms (Pereira et al. 2021)[174].

Regarding the characteristics of these data, the so-called 5Vs summarize the five ideal properties of data: volume, variety, velocity, value, veracity (Pereira et al., 2021, p. 2). The availability of large datasets is more likely to ensure the subsistence of all five dimensions. The collection and availability of high volumes of data is more likely to ensure variety in such data, covering the heterogeneity of the population by using multiple meaningful sources to ensure veracity at the same time (Pereira et al., 2021). A large dataset that covers the variability of the population should ensure the representativeness of all population features. Contrarily, small amounts of data would not ensure a sufficient degree of variety to exclude the possibility of biases in the algorithms trained on such datasets (Pereira et al., 2021).

Achieving a reasonable level of coverage and representativeness of the population characteristics is only possible through the collaborative sharing and integration of data collected from multiple institutions (Pereira et al., 2021). Drug development and medical devices development tools, as well as novel treatments, require significant data to be carried out. When such tools are developed collectively through partnerships and their use is made publicly available, the effort and resource burden on the single entity is significantly reduced, which results in considerable benefits for

[173] Ibid.

[174] Pereira, T.; Morgado, J.; Silva, F.; Pelter, M.M.; Dias, V.R.; Barros, R.; Freitas, C.; Negrão, E.; Flor de Lima, B.; Correia da Silva, M.; et al.*; Sharing Biomedical Data: Strengthening AI Development in Healthcare*, in "Healthcare", 2021, 9, 827 (Available from: https://doi.org/10.3390/ healthcare9070827).

developers, regulators, and most importantly patients (Karpen et al., 2021, p. 593). Therefore, we can affirm that successful and valuable data sharing relies on extensive partnerships.

6.2.2 Examples of Breakthroughs Enabled by Effective Data Sharing

Effective data sharing in healthcare can help in the development of innovative medical products and treatments while, simultaneously, foster knowledge and make it available to a wide community of professionals, researchers, innovators, and academics. Health data can be generated not only by health systems but also from wearable devices that create a flow of data crucial to developments in the medical field. In medical research, the utilization of shared health data has proved extremely beneficial from the continuous emergence of numerous success stories.

6.2.2.1 The Cancer Genome Atlas (TCGA)

The Cancer Genome Atlas (TCGA) initiative represents a groundbreaking example of how the collection and aggregation of data from patients can pave the way for more accurate medical treatments. As explained on the National Cancer Institute website[175], the TCGA is a cancer genomics program resulting from the effort between the National Institute of Health (NIH) and the National Human Genome Research Institute that started in 2006 in the United States. This joint effort brought together researchers from multiple institutions and different disciplines, and accomplished the extraordinary result of the molecularly characterization of "over 20,000 primary cancer and matched normal samples spanning 33 cancer types"[176]. In the following

[175] National Cancer Institute; *The Cancer Genome Atlas Program (TCGA)*, in "Center for Cancer Genomics" (https://www.cancer.gov/ccg/research/genome-sequencing/tcga Accessed on 19/12/2024).

[176] National Cancer Institute; *The Cancer Genome Atlas Program (TCGA)*, cit.

years, the data generated with TCGA amounted to over 2.5 petabytes of genomic, transcriptomic, epigenomic, and proteomic data which will remain publicly available for anyone to use, and have led to improvements in cancer diagnosis, treatment, but also prevention[177]. The TCGA represents a huge milestone not only in the understanding and treatment of cancer, but also in all the fields involved in the collection and analysis of the data, including science technology and computational biology. Twelve years after the beginning of this program, a rich data set of immense value has been produced thanks to the contributions from over 11,000 patients and all the thousands of researchers involved from 20 collaborating institutions[178].

6.2.2.2 The 23andMe Parkinson's Disease Research

23andMe is an American genetic testing company that in 2018 partnered with the pharmaceutical giant GSK to embark on research mainly focused on Parkinson’s disease[179]. The research community consists of more than 37,000 individuals affected by Parkinson’s, and millions of 23andMe customers who decided to voluntarily participate in the research to explore a person’s genetic likelihood to develop the disease[180]. The customer base is made up of approximately 12 million individuals who have undergone genetic testing; moreover, 80% of them consented to participate in research initiatives which make 23andMe boasts one of the world’s largest and most comprehensive collections of genotypic data[181]. This extensive genetic dataset is further expanded by billions of phenotypic data points, generously provided by

[177] Ibid.

[178] Ibid.

[179] Kaylor, Alivia; *Revolutionizing Clinical Trial Data Tracking, Analysis with Technology*; in “TechTarget”, 26 September 2023 (https://www.techtarget.com/pharmalifesciences/feature/Revolutionizing-Clinical-Trial-Data-Tracking-Analysis-with-Technology Accessed on 19/12/2024).

[180] 23andMe; *A New Era for Parkinson’s Research*, in “Research”, 13 August 2024 (https://blog.23andme.com/articles/a-new-era-for-parkinsons-research Accessed on 19/12/2024).

[181] Kaylor, Alivia; *Revolutionizing Clinical Trial Data Tracking, Analysis with Technology*; cit.

actively engaged participants, creating an invaluable resource for advancing genetic research and personalized medicine[182]. In 2019, the Michael J. Fox Foundation and the Parkinson's Foundation joined this research by establishing a new data and analytics platform dedicated to research on Parkinson's disease and getting closer to the goal of ending this disease[183].

6.2.2.3 The Project Data Sphere

Some of the most meaningful examples of new tools or treatments developed thanks to the sharing of health data and their public availability regard the medical field of oncology. This field is one of the leading examples of innovation in product development made possible through collaboration and data sharing across multiple initiatives and institutions (Karpen et al., 2021).

The Project Data Sphere (PDS) is an independent initiative funded and created by the American CEO of Roundtable on Cancer Life Sciences Consortium with the aim of voluntarily sharing, integrating, and analyzing previous cancer clinical trial data sets to advance future cancer research, and improve patient outcomes (Green et al., 2015)[184]. The ultimate aim of the PDS is to "provide a neutral, broad-access platform for industry and academia to share raw, deidentified data from late-phase oncology clinical trials using comparator-arm datasets" (Green et al., 2015, p. 464). As of October 2014, the PDS website registered data from 14 clinical cancer trials that covered approximately 9,000 individuals (Green et al., 2015). In 2021, the website was housing more than 150 datasets from over 100,000 patients which were made available to the public and were accessed nearly 20,000 times, supporting numerous

[182] Ibid.

[183] Ibid.

[184] ANGELA K. GREEN; KATHERINE E. REEDER-HAYES; ROBERT W. CORTY; ETHAN BASCH; MATHEW I. MILOWSKY; STACIE B. DUSETZINA; ANTONIA V. BENNETT; WILLIAM A.WOOD; *The Project Data Sphere Initiative: Accelerating Cancer Research by Sharing Data*, in "The Oncologist", 2015, 20, pp. 464-e20

publications on the matter (Karpen et al., 2021). The data openly accessible on the PDS website supported the development of innovative tools in cancer treatment and findings that will continue to improve the battle against cancer.

6.2.2.4 Therapies for COVID-19

The exceptionality of the situation caused by the spread of Covid-19 has caused a long and ongoing debate related to data sharing. The velocity with which the pandemic spread all over the world created urgency in the need of finding a solution to contrast the virus, limiting the infection, but especially the number of victims. The urgent need created by the rapid spread of the Covid pandemic exposed governments worldwide to the extreme need to internationally "cooperate, combine effort and share data and knowledge to enable scientific development at a pace never before experienced" (Pereira et al., 2021, p. 9) with the objective of finding effective solutions and develop rapid knowledge on the virus. However, this urgent need of collaboration was hindered by the limitations on data sharing imposed by certain countries.

One of the most impactful initiatives developed to face the global mobilization and coordination required to face the pandemic is the COVID-19 Data Portal (https://www.covid19dataportal.org/) that was first released on April 20th, 2020, as part of the European Covid-19 Data Platform that aimed at facilitating research on the virus through rapid and open data sharing and analysis (Harrison et al., 2021)[185]. The open datasets available on the Portal enabled researchers to easily obtain all the data needed to carry out their researchers and accelerate the finding of a solution.

[185] P. W. Harrison; R. Lopez; N. Rahman; S. Gutnick Allen; R. Aslam; N. Buso; C. Cummins; Y. Fathy; E. Felix; M. Glont; S. Jayathilaka; S. Kadam; M. Kumar; K. B. Lauer; G. Malhotra; A. Mosaku; O. Edbali; Y. Mi Park; A. Parton; M. Pearce; J. Francisco Estrada Pena; J. Rossetto; C. Russell; S. Selvakumar; X. Perez Sitja; A. Sokolov; R. Thorne; M. Ventouratou; P. Walter; G. Yordanova; A. Zadissa; G. Cochrane; N. Blomberg; R. Apweiler; *The COVID-19 Data Portal: accelerating SARS-CoV-2 and COVID-19 research through rapid open access data sharing*, in "Nucleic Acids Research", 2021, Vol. 49, W619–W623.

The Covid-19 outbreak triggered a global demand for preventative vaccines which became a priority to face the infection spread (Kalinke et al., 2022)[186]. The average time for vaccine development usually spans a period of 10 to 15 years or more due to the numerous steps necessary for its testing, regulatory process, and licensure and marketing (Kalinke et al., 2022). The emergency caused by the rapid spread and the number of victims caused by the pandemic required a much quicker response resulting from international collaborations. On February 21st, 2020, the WHO raised its threat assessment to its highest level and by April 8th, 2020, there were already 115 vaccines candidates for pre-clinical development and 5 were already at Phase I clinical trials (Kalinke et al., 2022). The necessity of a strong, multilateral global collaboration gave rise to a series of initiatives intended to form partnerships and promote information sharing with the aim of elaborating a collective response for the development of vaccines. The COVID-19 Evidence Accelerator is an example of such collaborative responses: it was founded to "provide a platform for government, research institutes, and health systems to allow for systematized, efficient information sharing" (Kalinke et al., 2022, p. 5). The previous experiences with SARS-CoV (2002-2003) and other pandemics made available a set of preexisting non-clinical data from past research on coronavirus and respiratory diseases outbreaks that allowed the usual early stages of vaccine design to be nearly bypassed, therefore accelerating the process (Kalinke et al., 2022). This prior experience made possible the use of platform technology approaches to extrapolate information from vaccine candidates, and the implementation of a platform-based program supporting the first in-human trials (Kalinke et al., 2022, p.6). The use of pre-clinical data and other data made available on platforms allowed an early response to Covid-19 with extremely quick development of vaccines, fundamental to overcome the pandemic worldwide.

[186] Ulrich Kalinke; Dan H. Barouch; Ruben Rizzi; Eleni Lagkadinou; Özlem Türeci; Shanti Pather; Pieter Neels; *Clinical development and approval of COVID-19 vaccines*, in "EXPERT REVIEW OF VACCINES", 2022, pp. 1-11

6.3 AI and Health Data in the United States: Balancing Privacy and Progress

6.3.1 The Role of AI in America's Healthcare

Despite the great examples of effective data sharing initiatives carried out by United States' entities, the world leaders in AI adoption across industries are on the other side of the planet. In 2024, India and China were leading the way with around 60% of their IT professionals indicating that their companies are actively adopting and incorporating AI into their processes[187]. The adoption rate in the United States is significantly lower (25%), also compared to European countries such as Italy (42%), Germany (34%), and France (31%)[188]. In the United States, large organizations are the ones reporting the highest implementation rates of AI with over 60% of the companies with 10,000+ employees leveraging AI capabilities[189]. The adoption rate across sectors is very heterogeneous, with the information sector reporting the highest adoption rate of 7% in 2024, followed by the healthcare sector reporting a 6% adoption rate[190].

There are multiple reasons that could explain why AI adoption in healthcare is not as advanced as it is in other sectors. An effective and productive use of artificial intelligence relies on the utilization of huge amounts of data that are necessary for the training of algorithms and reliable predictive outcomes. AI was first implemented across business sectors that produced large amounts of structured and quantitative data from the direct interaction between the customer and the systems or from the automatic collection of data that were eventually used to train algorithms with

[187] Vention; *AI adoption statistics by industries and countries: 2024 snapshot*, cit. (https://ventionteams.com/solutions/ai/adoption-statistics Accessed on 23/12/2024).
[188] Ibid.
[189] Ibid.
[190] Ibid.

promising outcomes (Sahni and Carrus, 2023)[191]. The challenges of implementing AI into healthcare settings range from the nature of data to the already complex clinical workflow: qualitative information, such as patients' treatments and outcomes, are harder to interpret, and multifactorial outcomes make algorithm training more complicated (Sahni and Carrus, 2023). For these reasons, many healthcare organizations are still in the early stages of AI implementation and are still testing the outcomes of its adoption.

Overall, there are three main domains of health care delivery that have proved apporting consistent benefits in the U.S. health system: reimbursement, clinical operations, and quality and safety (Sahni and Carrus, 2023).

Reimbursement is a key area for the financial health of any healthcare organization and the use of AI in this field is among the most advanced ones for its simplification of the patient's experience with medical payments (Sahni and Carrus, 2023). The reimbursement process aims at ensuring the right completion of the bills for the services provided by professionals so that the final amount paid to the organization is appropriate (Sahni and Carrus, 2023). The goal of applying AI to reimbursement models is to automate the process of finding bills that present elements of possible denial so that they don't move forward in the process, reducing the operational costs of manual revision and, ultimately, improving the patient's experience. These models have already proved extremely beneficial by reducing the percentage of claims denial from less than 80% to more than 90% and reducing administrative costs by 30% (Sahni and Carrus, 2023).

The second main area experiencing a large use of AI is the clinical operations domain which is not as advanced as reimbursement in terms of AI adoption but holds a huge

[191] Nikhil, Sahni; Brandon, Carrus; *Artificial Intelligence in U.S. Health Care Delivery*, in "The new England journal of medicine", 2023, pp. 348-358

potential. In the United States health system, a more effective use of operating-rooms can increase people's access to medical care, especially during times of staff shortages, and AI has started playing a central role in predicting rooms' use (Sahni and Carrus, 2023). Although the adoption of AI in this domain still remains in its early stage, its application has been successful in reducing cancellations and estimating mortality, predicting the estimate duration of procedures and possible complications, and finally predicting the likely postoperative outcomes and complications (Sahni and Carrus, 2023). Another fundamental benefit of AI in clinical operations is its ability to reduce the burden of updating electronic health records for physicians, which will ultimately make their job easier and give them more time to focus on patients, especially in times of physician shortages[192].

Lastly, the use of AI to enhance patient safety and experience shows significant potential. Some of the problems with the greatest potential for improvement with AI include adverse drug events, decompensation, and diagnostic errors which require the generation of actionable information (Sahni and Carrus, 2023). This process is powered by data collected with sensing technology devices, including wearable devices and sensors. Health systems adopting AI can also monitor vital signs and alert medical staff to intervene and take appropriate action, which have reportedly saved approximately 8000 lives in the first five years of implementation (Sahni and Carrus, 2023).

An important aspect of the implementation of AI in healthcare is the cost savings that these technologies would allow. In 2022, the cost of healthcare in the United States

[192] Roberts, Brooklyn; *Artificial Intelligence is Transforming America's Healthcare*, in "ALEC American Legislative Exchange Council", 17 January 2024 (https://alec.org/article/artificial-intelligence-is-transforming-americas-healthcare/ Accessed on 23/12/2024).

reached $4.5 trillion dollars[193]. A study by Sahni et al. (2023)[194] showed that the adoption of AI could result in savings of 5 to 10% of U.S. healthcare spending, or $200 to $360 billion annually, without compromising health services' quality and access for patients. All the subjects involved would benefit from it in monetary terms: for hospitals, the savings come from uses that improve clinical operations, quality and safety; for physicians, they come from improved clinical operations and continuity of care; for private payers, the savings come from improved claims, healthcare, and provider relationship management (Sahni et al., 2023). The savings resulting from the implementation of AI in American healthcare are not only monetary, but also non-financial, such as improved patient experience and satisfaction, and healthcare quality and access.

6.3.2 The Role of HIPAA in Supporting AI-Driven Healthcare Innovations

The data involved in the training of algorithms utilized to enable AI technologies to operate properly are of different nature, from physician notes to medical records and treatments outcomes, which could compromise patient safety and privacy if not properly handled. Privacy and data safety concerns require the implementation of a robust legal framework to prevent the risk of data breaches and unethical practices.

In the United States, the previously mentioned Health Insurance Portability and Accountability Act (HIPAA) represents the main guideline for the development and use of AI technologies in healthcare. HIPAA was initially established to protect U.S. patients' sensitive health information by setting strict standards for privacy and security of such data, granting individuals control over their data, limiting usage and

[193] Ibid.

[194] Nikhil Sahni; George Stein; Rodney Zemmel; David M. Cutler; *THE POTENTIAL IMPACT OF ARTIFICIAL INTELLIGENCE ON HEALTHCARE SPENDING*, for "NBER Economics of Artificial Intelligence Conference", September 2022.

disclosure, and ensuring appropriate sanctions for violations (Kamrul et al., 2024). The most relevant components of HIPAA are the Privacy Rule and the Security Rule, both later additions to the Act, which set privacy and data security standards with the objective of protecting patients' Protected Health Information (PHI or ePHI in the online context) (Sadri, 2024)[195]. The former establishes legal requirements for protecting identifiable patient information, while the latter sets criteria for a safe electronic transmission and storage of PHI (ePHI) (Sadri, 2024).

The Privacy Rule was enacted in 2003 by the United States Human Health Services (HHS) department and authorized by the Congress as a continuation of HIPAA to fill legal voids and further protect health information (Sadri, 2024). The Privacy Rule covers any PHI used or stored for treatment and diagnosis, establishing guidelines for obtaining consent to disclosure which can be written, informal or by the covered entity expressing their judgment for the individual's interest (Sadri, 2024, pp.27-28).

The Security Rule is a crucial component of HIPAA as it establishes a national standard for the creation, retrieval, and transmission of ePHI focusing only on electronic records contrarily to the Privacy Rule (Sadri, 2024). The Rule was introduced in 2004, and it is built on three fundamental principles, namely confidentiality, integrity, and availability, that enable "covered entities to develop new technologies to enhance patient care" (Sadri, 2024, p. 29). This principle sets the basis for a continuous development in AI applications to healthcare, leveraging the availability of patients' protected health information.

The principles of HIPAA are for a large part synonymous with the rules established by the European GDPR, which ensures broader protection of all types of data contrarily to HIPAA that only protects health data. Under HIPAA, PHI can be obtained

[195] Sadri, Mehri; *HIPAA: A Demand to Modernize Health Legislation*, in "The Undergraduate Law Review at UC San Diego, 2(1)", 2024

without patient's previous consent to it, who will also not be able to know where or how their data is being used (Sadri, 2024); on the other hand, GDPR requires the data subject's authorization to release their data, while also being aware of the use such data will undergo. Requirements in case of data breach are much more stringent under GDPR compared to HIPAA as the former requires patients to be notified within 72 hours, meanwhile HIPAA requires a breach notification only if more than 500 people are affected, which ensures an "unfair advantage to the bearers of personal information (Covered Entities) rather than the people to whom the data belongs" (Sadri, 2024, p. 43). The range of protections GDPR ensures to data subject is much wider than HIPAA as this one only protects data in healthcare. Moreover, the groundbreaking citizens' power introduced by the Right to be Forgotten is not provided by HIPAA which allows PHI to be shared without the patient's consent, further reinforcing covered entities and businesses freedom and flexibility (Sadri, 2024).

Nevertheless, many consider HIPAA as outdated and not adequately conforming to this century technological demands (Sadri, 2024), even if this could be the very reason of U.S. advancing support to AI-driven healthcare innovations.

6.3.3 NIH Data Sharing Initiatives

Among the entities involved in health data sharing promotion in the United States, the National Institute of Health (NIH) stands out for its commitment to improving health and saving lives through medical discoveries and efficient data sharing. The NIH is part of the U.S. Department of Health and Human Services, and it's the country's medical research agency[196]. For over a century, it has enabled medical discoveries and progress by sharing data and publications: currently, the areas in which NIH has

[196] National Institutes of Health; *Who we are*, in "About NIH" (https://www.nih.gov/about-nih/who-we-are Accessed on 02/01/2025).

sharing policies include scientific data, genomic data, research tools, model organisms, clinical trials, and research publications[197]. NIH is committed to making the results of the research it funds available to anybody to accelerate biomedical research, enable validation of research results, and provide access to high-value datasets[198].

In 2023, NIH implemented a new Data Management and Sharing Policy (DMSP) which requires anybody wanting to research and publish materials that will generate scientific data to submit a detailed plan explaining how data will be protected, stored, and ultimately shared[199]. The policy applies to individuals requesting funding from NIH to pursue their research and has two main requirements: the first one is a data management and sharing plan that must be submitted together with the research proposal, and the second one is continuous compliance with the approved plan through regular updates[200].

But the DMS Policy is not the only one. In 2015, NIH announced the final Genomic Data Sharing (GDS) Policy with the objective of promoting the "sharing, for research purposes, of large-scale human and non-human genomic data generated from NIH-funded research"[201]. The GDS Policy applies to all research funded by NIH that generates genomic data to share such data and translate it into knowledge, procedures and products to improve treatments in areas such as rare cancers examination, studies

[197] National Institutes of Health; *Expediting the translation of research results to improve human health*, in "Scientific Data Sharing" (https://sharing.nih.gov/ Accessed on 02/01/2025).

[198] National Institutes of Health; *Data Management and Sharing Policy*, in "Scientific Data Sharing" (https://sharing.nih.gov/data-management-and-sharing-policy Accessed on 02/01/2025).

[199] Columbia Research, *NIH Policy on Data Management and Sharing Plan (2023)*, Columbia University in the City of New York (https://research.columbia.edu/nih-policy-data-management-sharing-plan-23#:~:text=The%20National%20Institute%20of%20Health,%2C%20protected%2C%20and%20ultimately%20shared Accessed on 02/01/2025).

[200] Ibid.

[201] National Institutes of Health; *NIH Genomic Data Sharing Policy*, 27 August 2014 (https://grants.nih.gov/grants/guide/notice-files/NOT-OD-14-124.html Accessed on 02/01/2025).

on under-studied populations and mitochondrial DNA sequencing[202]. The Policy ensures that genomic research data are responsibly shared by establishing mandatory adherence to GDSP for all funded investigators[203].

Common Fund Data Ecosystem (CFDE) is another NIH initiative that aims to generate various datasets and knowledge to be used by the research community to accelerate discovery[204]. Other examples of NIH data sharing initiatives include the Cancer Moonshot Data Sharing Initiatives launched in 2016 to accelerate discovery, increase collaboration, and expand data sharing to deliver new insights into the causes of cancer, and how to prevent and detect it[205], and the NIH Human Connectome Project (HCP) launched in 2009 to map the neural pathways of brain functioning by acquiring and sharing data about the structural and functional connectivity of the human brain[206].

6.4 European Technological Gap and the EHDS: A Vision for the Future

6.4.1 The EU's Technological Gap

The EU has been renowned globally for its effort in promoting a safe digital space in which individuals' data are securely collected, stored and shared as a result of stringent

[202] National Cancer Institute; *About the Genomic Data Sharing (GDS) Policy*, in "NIH", 24 January 2024 (https://datascience.cancer.gov/data-sharing/genomic-data-sharing/about-the-genomic-data-sharing-policy Accessed on 02/01/2025).

[203] National Institutes of Health; *NIH Genomic Data Sharing Policy*, cit.

[204] National Institutes of Health; *Common Fund Data Ecosystem (CFDE*), in "Office of Strategic Coordination – The Common Fund" (https://commonfund.nih.gov/dataecosystem Accessed on 03/01/2025).

[205] National Cancer Institute; *Cancer Moonshot℠ Research Initiatives*, in "Research" (https://www.cancer.gov/research/key-initiatives/moonshot-cancer-initiative/implementation Accessed on 03/01/2025).

[206] National Institutes of Health; *Connectome Programs*, in "NIH Blueprint for Neuroscience Research" (https://neuroscienceblueprint.nih.gov/human-connectome/connectome-programs Accessed on 03/01/2025).

legal frameworks concerning data regulation and privacy protection. This effort has its main evidence in legal framework outcomes that have had global resonance for their outbreaking nature, such as the GDPR and the EU AI Act which are still considered as the gold standard in the field of data protection.

Nevertheless, despite the EU's continuous commitment to ensuring citizens' safety and security, the stringent protectionism surrounding artificial intelligence and people's data has started showing significant backlashes. The EU's economic security strategy focuses on the three Ps – protect, promote and partner – but the current technological landscape shows a focus mainly on 'protect', and very little on 'promote' and 'partner', which is furtherly proved by the fact that only 11 out of 100 of the world's largest tech companies are European (Digital Europe, 2024)[207]. All these factors have contributed to a significant technological gap between the EU and the U.S. and China. The disparity in technological leadership between Europe and the United States began in the 20th century when the latter was economically leading with innovations like automobiles and early developments in computers and internet technology, while Europe couldn't keep up with its counterpart and was left behind in key technologies sectors (Digital Europe, 2024).

The factors contributing to the lack of digital competitiveness of Europe can be mainly found in the shortfall in investments and the strict regulatory framework.

As explained on the study by Digital Europe (2024), both private and public investments in critical sectors related to technologies, such as AI and computing, experience a significant shortfall which affects the ability of the EU to develop robust industries able to compete globally. This investment shortfall marks a substantial disparity between the tech leading countries – U.S. and China – and Europe, which

[207] Digital Europe; *THE EU'S CRITICAL TECH GAP: Rethinking economic security to put Europe back on the map*, 2024 (Available from www.digitaleurope.org).

lacks in competitiveness. Technologies like AI require access to expensive infrastructures which, in most cases, is only possible through external funding. However, the current European's funding procedure has complex requirements that often discourage businesses and start-ups (Digital Europe, 2024). Moreover, the EU is facing a severe tech talent shortage in technological key areas enhanced by the lack of investment in AI start-ups which has been consistently lower compared to that of the U.S. (Digital Europe, 2024). The risks of not implementing measures to face these issues include the loss of potential talents who will migrate to regions where access to funding is more accessible and innovation in technology is fostered and promoted.

However, most experts consider the current stringent regulations as the main factor contributing to the technological gap between Europe and the U.S. The EU regulations on AI technologies and data sharing have no equivalent and impose a challenging environment for European businesses that results in a competitive disadvantage: in particular, the data processing legislation hinders the use of data for EU companies that face more barriers to train AI systems compared to their American counterpart (Digital Europe, 2024, p. 42). Restrictive funding and complex regulatory frameworks have impacted the European playing field for businesses, damaging its competitiveness and hindering its growth, therefore making these companies look for possibilities in other markets (Digital Europe, 2024). Moreover, the EU is also underdeveloped with regards to AI technologies: it currently stands at only 53% of the global leadership, and it "lags in early parts of the value chain, like advanced processing units and data centre capabilities, which are crucial for large language models (LLMs)" (Digital Europe, 2024, p. 12). The national variations within the EU Member States create regulatory overlaps that further complicate the already complex technological market for companies. A review of the current legal framework should also prioritize the removal of premature regulation of emerging technologies, giving space to innovation and the development of their full potential (Digital Europe, 2024).

The need for a less stringent regulation of AI and data sharing became clear in 2020 when Europe, just like the rest of the world, had to face the public health crisis caused by the Coronavirus outbreak. The Covid-19 pandemic has demonstrated the importance of collaboration and data sharing among health entities to face and overcome public health crises and speed up the process to develop innovative medical treatments and products. As previously mentioned, the availability of health data formerly collected and stored in platforms allowed scientists to develop vaccines against the virus in an exceptionally short time, making possible to control the disease and preventing the spread of the infection. The pandemic not only has shown the importance of making health data available in the health domain, but it has also accelerated the uptake of digital tools and applications in the everyday healthcare delivery.

6.4.2 The European Health Data Space (EHDS)

In the wake of the Covid-19 pandemic, improving health data sharing practices and extracting valuable insights from real-world data are perceived as a priority worldwide in the health domain (Marelli et al., 2023)[208], and Europe has started working towards a legal framework that would make these priorities feasible while always ensuring data protection and privacy.

In May 2022, the European Commission presented the Proposal for the European Health Data Space as a framework aimed at revolutionizing European health systems (Lucas and Haugo, 2024)[209]. The EHDS had the objective of improving the use of

[208] L. Marelli, M. Stevensc, T. Sharonc, I. Van Hoyweghenb, M. Boeckhoutd, I. Colussie, A. Degelsegger-Marquezf, S. El-Sayedg, K. Hoeyerh, R. van Kesseli, D. Krekora Zając k, M. Mateil, S. Rodam, B. Prainsackg, I. Schlündero, M. Shabanip, T. Southerington; *The European health data space: Too big to succeed*? in "Health Policy", 135, 2023.

[209] Jaisalmer de Frutos Lucas; Hans Torvald Haugo; *Moving forward with the European health data space: the need to restore trust in European health systems*, in "The Lancet Regional Health", Vol. 40, 2024

primary health data by providing all citizens with access and control over their personal electronic records and enabling the share of data with health professionals cross-border, but the most significant element of the Proposal was the creation of a solid legal framework for the secondary use of health data, such as innovation and research (Lucas and Haugo, 2024). However, the proposal soon encountered its first obstacle. In December 2023, the EC had to re-elaborate the original proposal after the European Parliament's request to include the right to opt-out of the health data processing for secondary use, and the stipulation of a opt-in mechanism for particularly sensitive data, such as genetic information (Lucas and Haugo, 2024, p.1), to really "empower individuals to have control over their health data" (European Commission, 2022)[210].

The European Parliament and the Council of the EU finally reached an agreement on the EHDS text on March 15th, 2024, after a three-month negotiations period (Lucas and Haugo, 2024). As the official EHDS website explains[211], thanks to these new rules, individuals will have easy access to their digital health data anywhere in the EU, and healthcare professionals will be able to access such data for eventual treatments even if they are in a different Member State. The EHDS not only ensures full compliance with EU data protection regulations, but also it allows the re-use of health data for research and innovation, helping in the development of new treatments and personalized medicines[212].

[210] European Commission; *European health union: a European health data space for people and science*. Brussels: European Commission; 2022 (Available from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711).

[211] European Health Data Space; *The European Health Data Space (EHDS)* (https://www.european-health-data-space.com/ Accessed on 04/01/2025).

[212] Ibid.

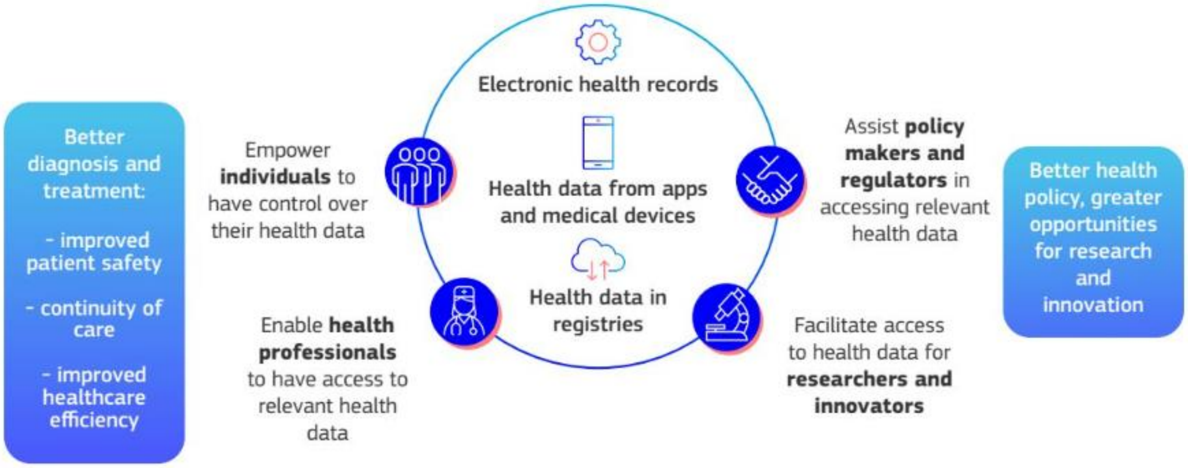
Better diagnosis and treatment:
- improved patient safety
- continuity of care
- improved healthcare efficiency
Empower **individuals** to have control over their health data
Enable **health professionals** to have access to relevant health data
Electronic health records
Health data from apps and medical devices
Health data in registries
Assist **policy makers and regulators** in accessing relevant health data
Facilitate access to health data for **researchers and innovators**
Better health policy, greater opportunities for research and innovation

Figure 3 - The EHDS functioning scheme

Source: European Health Data Space official website. Available from: https://www.european-health-data-space.com/

On April 24th, 2024, the members of the European Parliament approved the European Health Data Space with 445 votes in favor and 142 against[213]. The EHDS represents a turning point in the handling of health data as it finally releases the "research potential of health data in an anonymized or pseudonymized format"[214], which means that data including clinical trials, health records, public health registry information etc. can be processed for the so-called secondary use, which involves research, policymaking, and statistics[215].

6.4.2.1 Core Objectives and Implications of the EHDS

Data is constantly generated from a wide range of sources and devices that produce potential valuable insights not only in healthcare for researchers and healthcare

[213] Ibid.

[214] European Health Data Space; *The European Health Data Space (EHDS)*, cit.

[215] Ibid.

professionals, but for various types of businesses. Health data use is estimated to have a value of approximately 25/30 billion euros annually, and its worth is expected to reach 50 billion euros in the next 10 years[216]. The richness in health data holds a huge potential for the European health sector, but its potential has not been harnessed enough due to multiple reasons mainly concerned with stringent legal frameworks. In recent years, and with the passage of the EHDS, Europe is finally leveraging this huge potential and turning it into knowledge at the service of the European health system.

The European Health Data Space is an ecosystem for health data establishing rules, standards and practices, governance and infrastructures[217] with three main objectives clearly stated on the official European Commission website:

"

1. empower individuals to take control of their health data and facilitate the exchange of data for the delivery of healthcare across the EU (primary use of data);
2. foster a genuine single market for electronic health record systems;
3. provide a consistent, trustworthy, and efficient system for reusing health data for research, innovation, policy-making, and regulatory activities (secondary use of data)"[218].

The EHDS provides a secure and trustworthy environment that builds on the GDPR principles for secure access and processing of health data so that the EU will fully benefit from the sharing of these data to benefit patients, professionals, researchers and innovators[219].

[216] Ibid.

[217] Ibid.

[218] European Commission; *European Health Data Space*, in "Public Health" (https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en#latest-updates-and-documents Accessed on 04/01/2025).

[219] Ibid.

The Health Data Space distinguishes between two types of use of health data: primary and secondary use.

The primary use of health data requires all Member States to participate in a cross-border digital infrastructure to allow the exchange of health information[220] so that patients can receive medical treatment in every European country. Health professionals will be able to access the patient's medical records to deliver the best possible treatment based on this information and will then update such electronic records with the treatment received. As the EHDS website specifies, all Member States will be required to set up a digital health authority supervising over the respect of the rights of individuals in the implementation of the Data Space, and "mandatory requirements for interoperability, security, safety and privacy will be introduced, as well as mandatory self-certification of electronic health records covering interoperability and security"[221].

The secondary use of health data is the real point of separation from the traditional EU approach to the use of data, especially in the healthcare domain. The EHDS establishes a common EU framework to permit the use of health data for research purposes, innovation, personalized medicine and public health[222]. However, the secondary use of health data is subject to multiple conditions. Those who wish to re-use such data will have to apply for a specific permit from a health data access body specifying the purpose and how the data will be used[223]. The use of data will only be allowed in a secure environment with clear cyber security standards, and only anonymized data can be extracted, forbidding any attempts to re-identify the data subject[224]. Transparency will be the key word to any secondary use: all information

[220] European Health Data Space; *The European Health Data Space (EHDS*) cit.
[221] European Health Data Space; *The European Health Data Space (EHDS*) cit.
[222] Ibid.
[223] Ibid.
[224] Ibid.

about data access applications will be published, and the results and eventual findings of any uses will have to be made public by informing the health data access bodies[225]. These conditions apply to all researchers and innovators, not only those established in the EU territory, but also in third countries who will be subject to the same requirements and conditions.

As proved by the emergency caused by the Covid-19 pandemic, such innovation is fundamental for the future of the EU in multiple domains: the use of health data is crucial for the development of the health sector to allow innovation in the prevention, diagnosis and treatment of diseases[226]. The benefits of the implementation of the EHDS are also financial as "it is expected to save the EU around €11 billion over ten years: €5.5 billion will be saved from better access and exchange of health data in healthcare and another €5.4 billion will be saved from better use of health data for research, innovation and policy making"[227].

6.4.3 Italy's Healthcare System and AI

The Italian healthcare system is ranked as one of the most efficient in the EU and it provides universal coverage to all EU citizens and legal foreign residents thanks to the SSN (Italian National Health Service) founded in 1978 (European Observatory, 2024)[228]. The regions are responsible for the organization, financing and planning of healthcare delivery at the local level, while the central government oversees their work (European Observatory, 2024). The SSN represents a balance between centralized

[225] Ibid.

[226] European Commission; *Questions and Answers on the European Health Data Space*, in "Press Corner", 24 April 2024 (https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_2251 Accessed on 06/01/2025).

[227] European Commission; *Questions and Answers on the European Health Data Space*, cit.

[228] European Observatory on Health Systems and Policies, *Italy: Health system summary*, 6 December 2024 (Available from https://eurohealthobservatory.who.int/publications/i/italy-health-system-summary-2024).

policymaking and regional administrative autonomy which allows adaptation in the healthcare delivery to meet local needs in all regions (Rathi and Girvan, 2024)[229].

The regulation of AI in Italy includes the Law n.219 of 2017 which "regulates the aspects related to patient's informed consent to specific diagnostic and therapeutic interventions, including those provided with the help of AI medical devices" (Sablone et al. 2024, p.3)[230]. This law protects the right of the patient to be fully informed about the prognosis, diagnosis, risks and benefits of medical treatments, and any possible alternatives (Sablone et al. 2024). This requires an explanation of all the sides of the employment of AI in healthcare delivery, leaving the decision of whether to employ it or not to the patient, which represents a prerequisite for potential professional liability assessment (Sablone et al. 2024, p.3).

Despite its overall quality and efficiency, the 2024 World Index of Healthcare Innovation moved Italy to 29th overall out of 32 countries examined, improving only one spot from 2022 (Rathi and Girvan, 2024). The four dimensions examined are quality, choice, science and technology, and fiscal sustainability. Regarding the science and technology dimension, Italy's performance was below average, ranking 25th overall (Rathi and Girvan, 2024). Some of the criteria examined to determine this ranking included health IT and health digitization, medical advances, and scientific discoveries (Rathi and Girvan, 2024). This data is not surprising considering the implementation rates of AI in the country, especially in the healthcare sector. Even if

[229] Rathi, Anmol; Girvan, Gregg; *Italy: #29 in the 2024 World Index of Healthcare Innovation*, in "FREOPP", 23 December 2024 (https://freopp.org/italy-29-in-the-2024-world-index-of-healthcare-innovation/ Accessed on 07/01/2025).

[230] S. Sablone, M. Bellino, A. N. Cardinale, M. Esposito, F. Sessa, M. Salerno; *Artificial Intelligence in healthcare: an Italian perspective on ethical and medico-legal implications*; in "Frontiers in Medicine", 2024.

the use of AI by Italian businesses is growing steadily overall, only 26% of companies operating in healthcare planned to invest in AI in 2023[231].

Despite the financial costs derived from the implementation of AI into healthcare systems, its benefits are multiple. Italy is currently facing medical staff shortages that include both doctors and nurses: the use of AI would be beneficial in reducing the complications caused by staff shortages through a reduction of the workload of doctors and nurses who would have more time to dedicate to patients, a minimization of telephone communication, paperwork and bureaucracy times[232]. Therefore, the implementation of artificial intelligence in healthcare represents a promising perspective: in Italy, it could potentially reduce costs by around 10-15%, which can be translated into around EUR 21.74 billion per year[233].

6.5 Recommendations for the Future and the Potential of Blockchain

The creation of a secure and competitive ecosystem for data sharing has assumed growing relevance in governments worldwide. The benefits and potential of artificial intelligence can no longer be ignored, and investments in AI powered systems and technologies will determine the future technological leader. Despite the current technological gap of Europe, the implementation of the EHDS holds promising perspectives for the healthcare sector and is likely to influence the unleashing of data potential in other crucial sectors for the EU economy. Learning from the U.S. model in terms of data at the service of innovation would ensure Europe's global relevance and place it on the same level as China and the United States in terms of innovation for the future of healthcare. Enhancing the infrastructure for AI and data sharing has

[231] Rome Business School; *The impact of Artificial Intelligence in Italy from finance to healthcare*, in "Research", 10 July 2024 (https://romebusinessschool.com/blog/the-impact-of-artificial-intelligence-in-italy-from-finance-to-healthcare/ Accessed on 08/01/2025).
[232] Ibid.
[233] Ibid.

assumed more relevance in Europe in recent years, and the creation of a European Health Data Space is a clear example of the commitment towards leveraging the data that is constantly being generated towards the improvement of research and treatment in healthcare, while respecting the rules imposed by the GDPR.

In recent years, blockchain technology has assumed increasing relevance in the healthcare sector thanks to its core properties. With regard to the healthcare domain, the safeguard of patient data privacy represents the number one priority, especially when AI systems are involved. Blockchain technology represents a transformative shift as it

“

> provides a secure, decentralized method for storing and managing healthcare data, utilizing a distributed ledger system to ensure that patient records are immutable and verifiable, thereby thwarting unauthorized access and potential data breaches. It also enables secure data sharing among verified entities” (Williamson and Prybutok, 2024, p.7).

Blockchain technology introduces a valid solution responding to the ethical concerns emerging from the integration of AI into healthcare as it enhances data security and integrity by creating a secure and unforgeable record of patient data transactions – an absolute novelty that ensures the accuracy, consistency, and temper-proof of medical records (Williamson and Prybutok, 2024). The applications of blockchain are beneficial not only in terms of data storage, but it can also ensure the security of data sharing between healthcare entities, as well as enabling real-time monitoring of patient health information through its integration with IoT devices and AI systems (Williamson and Prybutok, 2024). The impact of blockchain technology in healthcare relies on some of its essential features including immutability, transparency, security, and interoperability. These attributes complement AI’s capabilities by creating a secure environment for sensitive health information, and presenting a promising future for addressing ethical concerns and data privacy challenges (Williamson and Prybutok, 2024).

Conclusions

This study provides an analysis of the emerging challenges and themes regarding data protection and artificial intelligence. The focus is placed on two main regulatory frameworks – GDPR and AI Act – for the analysis of the European scenario, while the American regulations review takes into consideration multiple federal laws representing the fragmented data protection landscape. By analyzing and comparing the EU and U.S. approaches to the regulation of both AI and data protection, this study highlights the radical differences between the two originating from the different historical background and the philosophical differences on such topics. The analysis reveals the importance of addressing people's trustworthiness and ethical concerns surrounding AI technologies for a correct and sustainable development of this sector. Moreover, ensuring proper data protection is not only fundamental, but can also lead to more individuals agreeing to unlock their data potential for research purposes.

Additionally, this study shows how both the European and American approach present backlashes. The former enforces stringent regulations on data protection and AI technologies that, if on the one hand guarantee the data subject's right, on the other hand limit the development of this sector and led to a technological gap. The latter is the complete opposite as it favors businesses handling data and collecting them for commercial purposes, reducing the individual's personal information to a marketable good, and not ensuring an adequate level of protection.

Nevertheless, recent years have shown significant steps forward in addressing these issues. Some American States are adopting regulations to address a proper consumer protection, and they are taking inspiration from the European model. Europe has taken a change of path with the creation of the European Health Data Space that promotes the secondary use of data for research and innovation. Accordingly, the focus of this study shifts to the healthcare domain. The sensitivity of the data involved in this sector requires an adequate balance between privacy and progress. We explored how the U.S. pursues innovation through effective data sharing initiatives enabling advancements in medical research and treatment. On the other hand, the Covid-19 experience and the sharing of health data to discover new vaccines awoke the urgency for a new approach to the handling of this type of data, which led to the creation of the EHDS. Regarding the European Health Data Space, the project has yet to be implemented and regulated by the Member States. The completion of these final steps is ought to be reached soon, as a prolonged timeframe would furtherly aggravate the European position in terms of secondary use of health data at a global level, especially for Research and Development activities (R&D).

This study provides a foundation for future research on data protection from a European and American point of view. This foundation can be furtherly expanded by a deeper exploration of the American tentative to better address data protection, and the European future intentions in terms of replicating a project similar to that of the EHDS in other fields. Finally, this study addresses the potential of blockchain technologies as a possible solution to a safe and transparent handling of data.

Bibliography

Joshi, Ameet; *Artificial Intelligence and Human Evolution: Contextualizing AI in Human History*; New York; Springer Science; 2024.

Shao, Zhou; Zhao, Ruoyan; Yuan, Sha; Ding, Ming; Wang, Yongli; *Tracing the evolution of AI in the past decade and forecasting the emerging trends*; in "Expert Systems with Applications"; Elsevier; 2022.

Sharma, Lavanya; Garg, Pradeep Kumar; *Artificial Intelligence: Technologies, Applications, and Challenges*; 1st Edition; New York; Chapman and Hall/CRC; 2021.

McCarthy, John; *Artificial Intelligence Tutorial – It's your time to innovate the future*, Dataflair Team, 27 November 2019 (Available from: https://data-flair.training/blogs/artificial-intelligence-ai-tutorial/).

Lungu, Mihai Adrian; *Smart Urban Mobility: The Role of AI in Alleviating Traffic Congestion*, in "Sciendo", 2024, DOI: 10.2478/picbe-2024-0118

Dunlop, Amelia; Woodward, Charlie; Ganoo, Saie; *AI Can Cut Costs: But at What Cost to the Workforce Experience?* Netherlands; Deloitte Digital; Natter; 2024.

European Commission; *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*, Brussels, 21.04.2021, Brussels, 2021, p. 2

Laux, Johann; Wachter, Sandra; Mittelstadt, Brent; *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, in "Regulation & Governance", 2024, pp. 3-32

Council of the European Union; *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement*, Brussels, 26.01.2024, Brussels, 2024, p. 33

Dakhole, Dipali; Praveena, K.N.; *History and Role of AI in Healthcare and Medicine*; in "Handbook of AI-based models in healthcare and medicine", Edited by Chander, B.; Guravaiah, K.; Anoop, B; Kumaravelan, G; CRC Press; 2024; pp. 19-31.

Kamalov, Firuz; Santandreu Calonge, David; Gurrib, Ikhlaas; *New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution*, in "Sustainability", 15, 2023, pp. 1-27

Agba, Michael Sunday; Agba, Grace Eleojo Micheal; Obeten, Amos W.; *Artificial Intelligence and Public Management and Governance in Developed and Developing Market Economies*, in "Journal of Public Administration, Policy and Governance Research", Vol. 1, No. 2, June 2023, pp. 1-14

Mobilio, Giuseppe; *Your face is not new to me – Regulating the surveillance power of facial recognition technologies*, in "Internet Policy Review", Vol. 12(1), 2023, pp. 1-31

Bharadiya, Jasmin Praful; *Artificial Intelligence in Transportation Systems - A Critical Review*, in “American Journal of Computing and Engineering”, Vol. 6 (1), 2023, pp. 35-45

Mitieka, Douglas; Luke, Rose; Twinomurinzi, Hossana; Mageto, Joash; *Smart Mobility in Urban Areas: A Bibliometric Review and Research Agenda*; in “Sustainability”, 15, 2023, pp. 1-23

Lu, His-Peng; Cheng, Hsiang-Ling; Tzou, Jen-Chuen; Chen, Chiao-Shan; *Technology roadmap of AI applications in the retail industry*, in “Technological Forecasting & Social Change”, 195, 2023, pp. 1-11

Wang, Qiang; Ji, Xiang; Zhao, Nenggui; *Embracing the power of AI in retail platform operations: Considering the showrooming effect and consumer returns*; in “Transportation Research Part E”, 182, 2024, pp. 1-26

Wilson, George; Johnson, Oliver; Brown, William; *Exploring the Integration of Artificial Intelligence in Retail Operations*, in “Creative Commons CC”, 2024, pp. 1-18

Oosthuizen, Kim; Botha, Elsamari; Robertson, Jeandri; Montecchi, Matteo; *Artificial intelligence in retail: The AI-enabled value chain*; in “Australasian Marketing Journal”, Vol. 29(3), 2020, pp. 264-273

Jasrotia, Sahil Singh; *Technological Innovations in Interactive Marketing: Enhancing Customer Experience at the New Retail Age*, in “The Palgrave Handbook of Interactive Marketing” by Cheng Lu Wang, Palgrave Macmillan, Switzerland, 2023, pp. 183-197

Kim, J.-H.; Kim, M.; Park, M.; Yoo, J.; *How interactivity and vividness influence consumer virtual reality shopping experience: The mediating role of telepresence*, in "Journal of Research in Interactive Marketing", Vol. 15(3), 2021, pp. 502–525.

Spanke, M.; *Easy checkout. Retail isn't dead*, 2020, Palgrave Macmillan, pp. 85–93

Pantano, E.; Priporas, C. V.; Sorace, S.; Iazzolino, G.; *The effect of mobile retailing on consumers' purchasing experiences: A dynamic perspective*; in "Computers in Human Behavior", 77, 2017, pp. 367-373. (https://doi.org/10.1016/j.chb.2017.07.022).

Jacob, B.; Kaushik, A.; Velavan, P.; *Autonomous navigation of drones using reinforcement*; in "Advances in augmented reality and virtual reality. Studies in computational intelligence" by J. Verma & S. Paul (Eds.), Springer, 2022, pp. 159–176

Roggeveen, A. L.; Sethuraman, R.; *How the COVID-19 pandemic may change the world of retailing*; in "Journal of Retailing", 96(2), 2020, pp. 169–171.

Chowdhury, Soumyadeb; Dey, Prasanta; Joel-Edgar, Sian; Bhattacharya, Sudeshna; Rodriguez-Espindola, Oscar; Abadie, Amelie; Truong, Linh; *Unlocking the value of artificial intelligence in human resource management through AI capability framework*, in "Human Resource Management Review", 33, 2023, pp. 1-21

Peeters, T.; Paauwe, J.; Van De Voorde, K.; *People analytics effectiveness: developing a framework*, in "Journal of Organizational Effectiveness: People and Performance", 7(2), 2020, pp. 203–219.

Jarrahi, M. H.; *Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making*, in “Business Horizons”, 61(4), 2018, pp. 577–586.

Seeber, I.; Bittner, E.; Briggs, R. O.; De Vreede, T.; De Vreede, G.-J.; Elkins, A.; Randrup, N.; *Machines as teammates: A research agenda on AI in team Collaboration*, in “Information & management”, 57(2), Article 103174, 2020.

Romansky, Radi P.; Noninska, Irina S.; *Challenges of the digital age for privacy and personal data protection*, in “Mathematical Biosciences and Engineering”, Volume 17, Issue 5, 2020, pp. 5288-5303

Taylor, Mistale; *Transatlantic Jurisdictional Conflicts in Data Protection Law: fundamental rights, privacy and extraterritoriality*; Cambridge University Press; 2023.

Politou, Eugenia; Alepis, Efthimios; Virvou, Maria; Patsakis; Constantinos; *Privacy and Data Protection Challenges in the Distributed Era*, in “Learning and Analytics in Intelligent Systems”, Volume 26, Springer, 2022.

Malle, B.; Kieseberg, P.; Weippl, E.; Holzinger, A.; *The right to be forgotten: towards machine learning on perturbed knowledge bases*, in “International Conference on Availability, Reliability, and Security”, Springer, 2016, pp. 251–266

Tene, O.; Polonetsky, J.; *Big data for all: Privacy and user control in the age of analytics*; Nw. J. Tech. Intell. Prop. 11, xxvii, 2013.

Boyne, Shawn Marie; *Data Protection in the United State*s, in “The American Journal of Comparative Law”, Volume 66 (1), 2018, pp. 299-343

Fefer, Rachel F.; Archick, Kristin; *EU Data Protection Rules and U.S. Implications*, in “Congressional Research Service”, Version 11, 2020.

De Bruin, Ruben; *A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence*, in “Hastings Science and Technology Law Journal”, Volume 13 (2), Article 4, 2022, pp.126-166

Schwartz, Paul M.; Peifer, Karl-Nikolaus; *Prosser's Privacy and the German right of Personality: Are Four Privacy Torts Better than One Unitary Concept*?, 98 CAL. L. REV. 1925, 1948-49 (2010).

Weiss, Martin A.; Archick, Kristin; *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, in “Congressional Research Service”, 2016, pp. 1-16

Fefer, Rachel F.; Archick, Kristin; *EU Data Protection Rules and U.S. Implications*, in “Congressional Research Service”, Version 11, 2020

Naef, Tobias; *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, in “European Yearbook of International Economic Law”, Volume 28, Springer, 2023

Batlle, Sergi; Van Waeyenberge, Arnaud; *EU–US Data Privacy Framework: A First Legal Assessment*, in "European Journal of Risk Regulation", Vol. 15, 2024, pp. 191–200

Williamson, S.M.; Prybutok, V.; *Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare*. Appl. Sci. 2024, 14, 675 (Available from: https:// doi.org/10.3390/app14020675).

Kamrul Islam Riad; Abdul Barek; Mostafizur Rahman; Shapna Akter Tahia Islam; Abdur Rahman; Raihan Mia; Hossain Shahriar; Fan Wu; Sheikh Iqbal Ahamed; *Enhancing HIPAA Compliance in AI-driven Health Devices Security and Privacy*, for "2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)", 2024, pp. 2430-2435

Lastrucci, A.; Pirrera, A.; Lepri, G.; Giansanti, D. *Algorethics in Healthcare: Balancing Innovation and Integrity in AI Developmen*t. Algorithms 2024, 17, 432 (Available from: https:// doi.org/10.3390/a17100432).

Karpen, Stephen R.; White, J. Kael; Mullin, Ariana P.; O'Doherty, Inish; Hudson, Lynn D.; Romero, Klaus; Sivakumaran, Sudhir; Stephenson, Diane; Turner, Emily C.; Larkindale, Jane; *Effective Data Sharing as a Conduit for Advancing Medical Product Development*, in "Therapeutic Innovation & Regulatory Science", 2021, 55, pp. 591–600, (Available from: https://doi.org/10.1007/s43441-020-00255-8).

Pereira, T.; Morgado, J.; Silva, F.; Pelter, M.M.; Dias, V.R.; Barros, R.; Freitas, C.; Negrão, E.; Flor de Lima, B.; Correia da Silva, M.; et al.*; Sharing Biomedical Data:*

Strengthening AI Development in Healthcare, in “Healthcare”, 2021, 9, 827 (Available from: https://doi.org/10.3390/ healthcare9070827).

GREEN, ANGELA K.; REEDER-HAYES, KATHERINE E.; CORTY, ROBERT W.; BASCH, ETHAN; MILOWSKY, MATHEW I.; DUSETZINA, STACIE B.; BENNETT, ANTONIA V.; WOOD, WILLIAM A.; *The Project Data Sphere Initiative: Accelerating Cancer Research by Sharing Data*, in “The Oncologist”, 2015, 20, pp. 464-e20

Harrison, P. W.; Lopez, R.; Rahman, N.; Gutnick Allen, S.; Aslam, R.; Buso, N.; Cummins, C.; Y. Fathy; E. Felix; M. Glont; S. Jayathilaka; S. Kadam; M. Kumar; K. B. Lauer; G. Malhotra; A. Mosaku; O. Edbali; Y. Mi Park; A. Parton; M. Pearce; J. Francisco Estrada Pena; J. Rossetto; C. Russell; S. Selvakumar; X. Perez Sitja; A. Sokolov; R. Thorne; M. Ventouratou; P. Walter; G. Yordanova; A. Zadissa; G. Cochrane; N. Blomberg; R. Apweiler; *The COVID-19 Data Portal: accelerating SARS-CoV-2 and COVID-19 research through rapid open access data sharing*, in “Nucleic Acids Research”, 2021, Vol. 49, W619–W623.

Kalinke, Ulrich; Barouch, Dan H.; Rizzi, Ruben; Lagkadinou, Eleni; Türeci, Özlem; Pather, Shanti; Neels, Pieter; *Clinical development and approval of COVID-19 vaccines*, in “EXPERT REVIEW OF VACCINES”, 2022, pp. 1-11

Nikhil, Sahni; Brandon, Carrus; *Artificial Intelligence in U.S. Health Care Delivery*, in “The new England journal of medicine”, 2023, pp. 348-358

Sahni, Nikhil; Stein, George; Zemmel, Rodney; Cutler, David M.; *THE POTENTIAL IMPACT OF ARTIFICIAL INTELLIGENCE ON HEALTHCARE SPENDING*, for "NBER Economics of Artificial Intelligence Conference", September 2022.

Sadri, Mehri; *HIPAA: A Demand to Modernize Health Legislation*, in "The Undergraduate Law Review at UC San Diego, 2(1)", 2024

Digital Europe; *THE EU'S CRITICAL TECH GAP: Rethinking economic security to put Europe back on the map*, 2024 (Available from www.digitaleurope.org).

Marelli, L.; Stevensc, M.; T. Sharonc, I. Van Hoyweghenb, M. Boeckhoutd, I. Colussie, A. Degelsegger-Marquezf, S. El-Sayedg, K. Hoeyerh, R. van Kesseli, D. Krekora Zająck, M. Mateil, S. Rodam, B. Prainsackg, I. Schlündero, M. Shabanip, T. Southerington; *The European health data space: Too big to succeed*? in "Health Policy", 135, 2023.

Lucas, Jaisalmer de Frutos; Haugo, Hans Torvald; *Moving forward with the European health data space: the need to restore trust in European health systems*, in "The Lancet Regional Health", Vol. 40, 2024

European Commission; *European health union: a European health data space for people and science*. Brussels: European Commission; 2022 (Available from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711).

European Observatory on Health Systems and Policies, *Italy: Health system summary*, 6 December 2024 (Available from https://eurohealthobservatory.who.int/publications/i/italy-health-system-summary-2024).

Sablone, S.; Bellino, M.; Cardinale, A. N.; Esposito, M.; Sessa, F.; Salerno, M.; *Artificial Intelligence in healthcare: an Italian perspective on ethical and medico-legal implications*; in "Frontiers in Medicine", 2024.

Sitography

23andMe; *A New Era for Parkinson's Research*, in "Research", 13 August 2024 (https://blog.23andme.com/articles/a-new-era-for-parkinsons-research Accessed on 19/12/2024).

Amazon; *Amazon Go* (https://www.amazon.com/b?ie=UTF8&node=16008589011 Accessed on 20/06/2024).

Bonta, Rob; *California Consumer Privacy Act (CCPA)*, in "Office of the Attorney General", 2024 (https://oag.ca.gov/privacy/ccpa Accessed on 21/11/2024).

Bonta, Rob; *Data Security Breach Reporting*, in "Office of the Attorney General" (https://oag.ca.gov/privacy/databreach/reporting Accessed on 18/11/2024).

Brown, Justine; *Rise of the Chief Privacy Officer*, in "Government Technology", 2014 (https://www.govtech.com/data/rise-of-the-chief-privacy-officer.html Accessed on 17/11/2024).

Columbia Research, *NIH Policy on Data Management and Sharing Plan (2023*), Columbia University in the City of New York (https://research.columbia.edu/nih-policy-data-management-sharing-plan-23#:~:text=The%20National%20Institute%20of%20Health,%2C%20protected%2C%20and%20ultimately%20shared Accessed on 02/01/2025).

Contact Center Compliance; *What is the TCPA*? (https://www.dnc.com/what-is-tcpa/, Accessed on 17/11/2024).

Defense Privacy and Civil Liberties Office; *Introduction to The Privacy Act* (https://dpcld.defense.gov/Portals/49/Documents/Privacy/2011%20DPCLO_Intro_Privacy_Act.pdf Accessed on 17/11/2024).

Duigan, Brian; *USA Patriot Act*, in "Britannica", 2024 (https://www.britannica.com/topic/USA-PATRIOT-Act Accessed on 18/11/2024).

Epic.org; *The Fair Credit Reporting Act (FCRA*), (https://epic.org/fcra/ Accessed on 15/11/2024).

EPRS - European Parliamentary Research Service; *Artificial intelligence in healthcare: Applications, risks, and ethical and societal impacts*, in "European Parliament", June 2022 (https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf Accessed on 20/06/2024).

European Commission; *DESI 2024*, in "DESI – Compare countries progress", 2024 (https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/compare-countries-progress?indicator=desi_dps_cit&indicatorGroup=desi2023-4&breakdown=total&period=desi_2024&unit=egov_score&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE Accessed on 25/09/2024).

European Commission; *European Commission Calls on the U.S. to Restore Trust in EU-U.S. Data Flows*, in "press prelease", November 27, 2013 (http://europa.eu/rapid/press-release_IP-13-1166_en.htm Accessed on 27/11/2024.

European Commission; *European Health Data Space*, in “Public Health” (https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en#latest-updates-and-documents Accessed on 04/01/2025).

European Commission; *How should my consent be requested?* (https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_en Accessed on 02/11/2024).

European Commission; *Questions and Answers on the European Health Data Space*, in “Press Corner”, 24 April 2024 (https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_2251 Accessed on 06/01/2025).

European Commission; *Transport and Mobility*, in “AI watch”, 2024 (https://ai-watch.ec.europa.eu/topics/transport-and-mobility_en Accessed on 27/09/2024).

European Commission; *Who does the data protection law apply to?* (https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en Accessed on 25/10/2024.

European Data Protection Board; *International Data Transfers*, in “Data Protection Guide for Small Business” (https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en Accessed on 27/11/2024).

European Data Protection Supervisor; *The History of the General Data Protection Regulation*, 2018 (https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en Accessed on 23/10/2024).

European Health Data Space; *The European Health Data Space (EHDS*) (https://www.european-health-data-space.com/ Accessed on 04/01/2025).

Eurostat; *USA-EU - international trade in goods statistics*, 2024 (https://ec.europa.eu/eurostat/statistics-explained/index.php?title=USA-EU_-_international_trade_in_goods_statistics Accessed on 22/11/2024).

Federal Communications Commission; *CAN-SPAM* (https://www.fcc.gov/general/can-spam Accessed on 20/11/2024).

Federal Trade Commission; *About the FTC* (https://www.ftc.gov/about-ftc Accessed on 07/11/2024).

Federal Trade Commission; *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Ac*t) (https://www.ftc.gov/legal-library/browse/statutes/controlling-assault-non-solicited-pornography-marketing-act-2003-can-spam-act Accessed on 20/11/2024).

Federal Trade Commission; *Fighting identity theft with Red Flags Rule: A how-to guide for business* (https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business Accessed on 18/11/2024).

Federal Trade Commission; *Gramm-Leach-Bliley Act* (https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act Accessed on 20/11/2024).

Federal Trade Commission; *National Do Not Call Registry FAQs*, in "Consumer advice" (https://consumer.ftc.gov/articles/national-do-not-call-registry-faqs#:~:text=The%20Do%20Not%20Call%20Registry%20stops%20unwanted%20sales%20calls%20%E2%80%94%20live,from%20scammers%20making%20illegal%20calls Accessed on 17/11/2024).

Fleischer, Peter; *The rights to be forgotten, or how to your your history*, in "Peter Fleischer: Privacy…?", 2012 (http://peterfleischer.blogspot.gr/2012/01/right-to-be-forgotten-or-how-to-edit.html Accessed on 01/11/2024).

FLI - Future of Life Institute; *EU Artificial Intelligence Act*, 2024 (https://artificialintelligenceact.eu/recital/33/ Accessed on 25/09/2024).

FLI – Future of Life Institute; *EU Artificial Intelligence Act*, 2024, (https://artificialintelligenceact.eu/recital/12/ Accessed on 28/09/2024).

FLI - Future of Life Institute; *High-level summary of the AI Act*, in "EU Artificial Intelligence Act", 2024 (https://artificialintelligenceact.eu/high-level-summary/ Accessed on 12/08/2024).

FLI - Future of Life Institute; *Historic Timeline*, in "EU Artificial Intelligence Act", 2024 (https://artificialintelligenceact.eu/developments/, Accessed on 09/08/2024).

GDPR Advisor; *GDPR Fines and Penalties: what you need to know to avoid costly mistakes* (https://www.gdpradvisor.co.uk/gdpr-fines-and-penalties Accessed on 02/11/2024).

IBM; *What is the Internet of Things (IoT)?,* in "Think", 12 May 2023, (https://www.ibm.com/think/topics/internet-of-things Accessed on 28/09/2024).

IKEA*; Ikea Place App*, in "Inter IKEA Newsroom", 12/09/2017, (https://www.ikea.com/global/en/newsroom/innovation/ikea-launches-ikea-place-a-new-app-that-allows-people-to-virtually-place-furniture-in-their-home-170912/ Accessed on 29/09/2024).

Intersoft Consulting, *GDPR* (https://gdpr-info.eu/issues/personal-data/ Accessed on 10/10/24).

Intersoft Consulting; *GDPR*, Article 5(1) (https://gdpr-info.eu/issues/personal-data/ Accessed on 25/10/24).

Kaylor, Alivia; *Revolutionizing Clinical Trial Data Tracking, Analysis with Technology*; in "TechTarget", 26 September 2023 (https://www.techtarget.com/pharmalifesciences/feature/Revolutionizing-Clinical-Trial-Data-Tracking-Analysis-with-Technology Accessed on 19/12/2024).

LII - Legal Information Institute; Amdt14.2 State Action Doctrine, in "Cornell Law School" (https://www.law.cornell.edu/constitution-conan/amendment-14/state-action-doctrine Accessed on 22/11/2024).

National Archives and Records Administration; *Children's Online Privacy Protection Rule*, in "The Daily Journal of the United States Government" (https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule Accessed on 20/11/2024).

National Association of Criminal Defense Lawyers*; Computer Fraud and Abuse Act (CFAA)* (https://www.nacdl.org/Landing/ComputerFraudandAbuseAct Accessed on 18/11/2024).

National Cancer Institute; *About the Genomic Data Sharing (GDS) Policy*, in "NIH", 24 January 2024 (https://datascience.cancer.gov/data-sharing/genomic-data-sharing/about-the-genomic-data-sharing-policy Accessed on 02/01/2025).

National Cancer Institute; *Cancer Moonshot*℠ *Research Initiatives*, in "Research" (https://www.cancer.gov/research/key-initiatives/moonshot-cancer-initiative/implementation Accessed on 03/01/2025).

National Cancer Institute; *The Cancer Genome Atlas Program (TCGA*), in "Center for Cancer Genomics" (https://www.cancer.gov/ccg/research/genome-sequencing/tcga Accessed on 19/12/2024).

National Institutes of Health; *Common Fund Data Ecosystem (CFDE*), in "Office of Strategic Coordination – The Common Fund" (https://commonfund.nih.gov/dataecosystem Accessed on 03/01/2025).

National Institutes of Health; *Connectome Programs*, in “NIH Blueprint for Neuroscience Research” (https://neuroscienceblueprint.nih.gov/human-connectome/connectome-programs Accessed on 03/01/2025).

National Institutes of Health; *Data Management and Sharing Policy*, in “Scientific Data Sharing” (https://sharing.nih.gov/data-management-and-sharing-policy Accessed on 02/01/2025).

National Institutes of Health; *Expediting the translation of research results to improve human health*, in “Scientific Data Sharing” (https://sharing.nih.gov/ Accessed on 02/01/2025).

National Institutes of Health; *NIH Genomic Data Sharing Policy*, 27 August 2014 (https://grants.nih.gov/grants/guide/notice-files/NOT-OD-14-124.html Accessed on 02/01/2025).

National Institutes of Health; *Who we are*, in “About NIH” (https://www.nih.gov/about-nih/who-we-are Accessed on 02/01/2025).

NIST – Computer Security Resource Center CSRC; *Cyberspace*, https://csrc.nist.gov/glossary/term/cyberspace Accessed on 14/10/24).

Office of Justice Programs; *E-Government Act of 2002*, in “Department of Justice” (https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1287 , Accessed on 18/11/2024).

Office of Justice Programs*; Electronic Communications Privacy Act of 1986 (ECPA), in “*Department of Justice” (https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 Accessed on 19/11/2024).

Office of Privacy and Civil Liberties; *Privacy Act of 1974, in “*U.S. Department of Justice” (https://www.justice.gov/opcl/privacy-act-1974 Accessed on 15/11/2024).

Puk, Kamil; *How Smart Mirrors are Transforming In-Store Experiences*, in “Netguru”, February 27th 2024 (https://www.netguru.com/blog/smart-mirrors-in-retail Accessed on June 21/06/2024).

Rathi, Anmol; Girvan, Gregg; *Italy: #29 in the 2024 World Index of Healthcare Innovation*, in “FREOPP”, 23 December 2024 (https://freopp.org/italy-29-in-the-2024-world-index-of-healthcare-innovation/ Accessed on 07/01/2025).

Roberts, Brooklyn; *Artificial Intelligence is Transforming America's Healthcare*, in “ALEC American Legislative Exchange Council”, 17 January 2024 (https://alec.org/article/artificial-intelligence-is-transforming-americas-healthcare/ Accessed on 23/12/2024).

Rome Business School; *The impact of Artificial Intelligence in Italy from finance to healthcare*, in “Research”, 10 July 2024 (https://romebusinessschool.com/blog/the-impact-of-artificial-intelligence-in-italy-from-finance-to-healthcare/ Accessed on 08/01/2025).

Solon, Olivia; *EU ‘right to be forgotten’ ruling paves way for censorship*, in “Wired”, 2014 (http://www.wired.co.uk/article/right-to-be-forgotten-blog Accessed on 01/11/2024).

Squire Patton Boggs; *Overview of Privacy and Data Protection Laws: United States*, in “Privacy world” (https://www.privacyworld.blog/summary-of-data-privacy-protection-laws-in-the-united-states/ Accessed on 21/11/2024).

Squire Patton Boggs; *Overview of Privacy and Data Protection Laws: United States*, in “Privacy world” (https://www.privacyworld.blog/summary-of-data-privacy-protection-laws-in-the-united-states/ Accessed on 21/11/2024).

Stephan, Jaggi; *State Action Doctrine*, Oxford Constitutional Law, 2017 (https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e473).

Tesla; *Autopilot and Full Self-Driving (Supervised*), in “Support” (https://www.tesla.com/support/autopilot Accessed on 28/09/2024).

U.S. Center for Disease Control and Prevention; *Health Insurance Portability and Accountability Act of 1996 (HIPAA*), in “Public Health Law” (https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html Accessed on 19/11/2024).

U.S. Department of Education; *What is FERPA?*, in “Protecting Student Privacy” (https://studentprivacy.ed.gov/faq/what-ferpa#:~:text=The%20Family%20Educational%20Rights%20and,identifiable%20information%20from%20the%20education Accessed on 17/11/2024).

U.S. Office of Special Counsel*; The Privacy Act of 1974* (https://osc.gov/Pages/Privacy-Act.aspx Accessed on 17/11/2024).

University of Michigan; *History of Privacy Timeline*, in "Safe Computing", 2024 (https://safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline, Accessed on 15/11/24).

University of San Diego; *39 Examples of Artificial Intelligence in Education*, in "Artificial Intelligence" (https://onlinedegrees.sandiego.edu/artificial-intelligence-education/ Accessed on 20/09/2024).

University of San Diego; *43 examples of Artificial Intelligence in Education*, in "Artificial Intelligence" (https://onlinedegrees.sandiego.edu/artificial-intelligence-education/ Accessed on 21/06/2024).

Vention; *AI adoption statistics by industries and countries: 2024 snapshot*, in "Artificial Intelligence", 2024 (https://ventionteams.com/solutions/ai/adoption-statistics Accessed on 19/12/2024).

Wilhelm, Ernst Oliver; *A brief history of the General Data Protection Regulation (1981-2016*), in "iapp", 2016 (https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/# Accessed on 24/10/2024).

World Health Organization; *WHO releases AI ethics and governance guidance for large multi-modal models*, in "News", 18 January 2024;

(https://www.who.int/news/item/18-01-2024-who-releases-ai-ethics-and-governance-guidance-for-large-multi-modal-models Accessed on: 17/12/2024).

List of Figures