LUISS

Degree Program in
Data Science and Management

Course of Privacy in the Digital Wolrd

A Bot-Based Solution to Manage GDPR Cookie Compliance: A Technological and Legal Perspective

Prof. Antonio Cilento
SUPERVISOR

Prof. Paolo Spagnoletti
CO-SUPERVISOR

Olimpia Sannucci 752341
CANDIDATE

Academic Year 2022/2023

Contents

1 Introduction

The digital age encompasses a broad range of technological advancements, which include virtual environments, digital services, intelligent applications, machine learning, and knowledge-based systems. These innovations shape the distinctive characteristics of our contemporary world, such as globalization, e-communications, information sharing, and virtualization.

On the other hand, the concept of privacy has existed long before the introduction of these new technologies. There has always been a need to protect the personal sphere of the individual, from general information, integrity, relationships and personal affairs, to one's intimacy; now there is a need for adaptation, a change to the direction these new technologies are taking. Hence, it is important to note that these technologies also pose a potential risk to security and privacy. The concepts of privacy and digital technologies in fact can no longer be studied separately, as one is encroaching on the sphere of the other. Advances in Information Technology have raised concerns about privacy and its impacts, and those new tools have brought up several challenges that need to be addressed. New balances and compromises must be found so that all subjects can be protected.

This paper aims to inform on the current privacy literature by providing general definitions and analyzing dissenting opinions, regulations to be adopted, and stakeholders, to the point of providing a technological tool that can help balance the technological and privacy worlds. One of the ultimate goals is to help people make informed decisions, considering both privacy protection and the benefits of new technologies.

The project stems from a company's need to have a tool that can help it be compliant with one of the current regulations for the protection of the individual's privacy. For this to happen, there is a need for a general knowledge of the concept of privacy, its evolution, and how it is interpreted. A study of these characteristics is therefore necessary, to understand how privacy has been considered a fundamental value for individual autonomy, dignity, and freedom; to understand how social, technological, and legal changes have affected its definition and facets. Moreover, understanding the history of privacy allows us to reflect on the implications of its erosion or violation. This awareness helps us develop more effective norms, laws and protection mechanisms to preserve individual and collective privacy.

The speed with which technologies are advancing and permeating every aspect of our lives has raised new challenges for privacy, necessitating constant adaptation of data protection regulations and policies. Studying those concepts helps us learn from the past and develop appropriate solutions to contemporary privacy challenges. Modern technologies are changing the way of life and habits, with impressive vehemence, and cannot be regarded as an enemy. Indeed, its incredible capabilities must be harnessed to achieve honest goals congruent with principles and values.

The goal of this project is therefore to provide an overview of privacy, analyzing, as much as possible given the vastness of the topic, its nuances, its regulation, taking into consideration the digital context of the current century. Finally, to provide a tool that can ease the technological transition toward respecting the rights of the individual. Companies collect information and personal data from data subjects on a daily basis, in enormous quantities, and then exchange and process it; many times individuals are unaware of anything that happens to their personal information. The amount of data collected on each individual every day is a tool that is being exploited in many economic and political environments in order to achieve predefined purposes, from advertising, using various forms of targeting, to electoral campaigns, being able to identify voters who are likely to switch or to turn out. The most prevalent technology to enable the collection and resale of individual-level information is based on cookies and related means of recording browsing data; these tools are capable of recording user movements and histories, and organizations collect all this information. Given the critical nature of the information collected, the use of cookies is subject to regulations, and companies are required to be fully compliant in order not to incur high penalties.
The tool provided in this work is a bot, or robot, programmed and automated to help the company comply with regulations and not violate consumer rights regarding cookie compliance. The bot has the ability to replicate human movements; because of this, it was possible to collect all cookies by simulating the action of the data subject, and providing the company with an effective and fast tool, with a minimal propensity for error, and supportive to be more privacy-compliant.

This work tells a story reminiscent of childhood tales: there are the protagonists placed in a particular setting, facing challenges and obstacles in their quest for the ultimate prize. In our case, the protagonists are consumers, organizations, governments, online platforms, and technologies. Initially, they may view each other as adversaries since each seeks to achieve their own objectives and happiness. However, they discover that unity and collaboration empower them, making the journey towards the resolution much simpler. The futuristic environment they find themselves in is the 21st century, where technologies reign supreme. Humanity struggles to remain true to itself and keep up with the rapidly evolving times while staying intact. There are numerous challenges to face: preserving fundamental principles, obtaining respect and control over personal data, avoiding deception by institutions, and asserting one's rights. On the other hand, organizations exist in the marketplace and must also survive competition. They gather data and scrutinize every detail of consumers to strive for excellence. Enters the European Union, which provides tools to strike a balance among the protagonists. Regulations are introduced to govern markets, address divergences, foster competition, and simultaneously safeguard vulnerable consumers. These tools are the GDPR (General Data Protection Regulation), DSA (Digital Services Act), and DMA (Digital Markets Act). However, they are not like magic spells: they require refinement, as they possess merits and flaws. A significant amount of work is necessary to achieve the desired end result.

This thesis work, this story, is divided into three chapters, starting from the general to the particular. In the first chapter, the literature of privacy is studied, its history and various definitions, interpretations and influences are reported. It also examines privacy within the context of technology and innovation, specifically the transition to information privacy. The General Data Protection Regulation (GDPR), a regulation that came into force to protect the rights of the data subject, is then introduced and explained. Additionally, taking into consideration the major role that platforms are playing in this period, how they influence and manipulate the markets and the businesses, the Digital Services Package is included. The Digital Services Act (DSA) is the new European regulation on digital services which defines the responsibilities and obligations of online platforms that offer intermediary services. While the Digital Markets Act (DMA) is the new European regulation on digital markets which It addresses abuses of dominance by large online platforms that act as "gatekeepers" between businesses and users.

In the second chapter, the point of view of the two key players in today's landscape is presented: consumers and businesses. From the former's point of view, there is an explanation of various rights that the latter has, along with the critical issues and opportunities that can be created. Organizations, their role and responsibilities, current and future procedures, methods of organization and adaptation are then described. In this way the reader has the opportunity to be informed and have a broader view. One of the challenges described for organizations is precisely cookie compliance, its definition and characteristics are then reported.

Finally, in the third chapter, the robot is described, how it works, how it was designed, results achieved, and minutiae for improvement.

2 Acknowledgements

This thesis project was carried out in collaboration with BGP Management Consulting SpA, which provided access to their data and resources, In order to achieve the project goals.

BGP Management Consulting Spa is a leading management consulting company that provides a wide range of services to help businesses achieve their strategic goals. With a team of experienced and skilled consultants, BGP offers solutions in areas such as business strategy, organizational design, operations, and technology. It offers consulting, services and platforms in the areas governed by the CFO and CIO, for the design, implementation and management of enterprise information systems starting from the specific needs of functional and industry areas to provide comprehensive ERP, Analytics, Performance Management and Managed Services solutions enabling Management to make informed decisions consistent with the state of the art opportunities offered by technological evolution, in Cloud and On-Premise, developing Cloud Native applications that extend the standard solutions by employing Blockchain, AI, ML, RPA and IoT technologies to automate tasks, increase control and granularity of data.

BPG is a company that operates in several territories, including the areas of technology, advisory,analytics, ERP solution, treasury, human capital and financial services.

BGP Technology operates in consulting and technology support for the implementation and governance of innovative SAP platforms (SAP HANA and SAP CLOUD PLATFORM). It collaborates easily and intuitively with the IT Function by studying new software applications or setting up maintenance programs for already operational applications.

BGP Advisory aims to support clients with specific skills in Management Consulting and Program / Project / Service Management.

BGP Business Intelligence & Analytics operates in the design and implementation of application solutions in Enterprise Data Warehousing as well as Analytics and Self-BI solutions both on premise and on-cloud.

BGP ERP Solution operates in the areas of Planning & Controlling, Financial and Logistics with a vertical organization by Competence Center able to support Administration, Controlling and Operations functions in developing a consistent, integrated and high value-added approach.

BGP Treasury operates exclusively in the Treasury area, supporting the Finance Function in its quest for greater efficiency in corporate treasury as a whole. Through the centralization of operations and financial risks in the organizational path for closer control of the banking universe.

BGP Human Capital operates as a support proactive to the Human Resources function in order to improve its performance and organizational climate with the power of In Cloud and Hybrid solutions.

BGP Financial Services Solution develops Industry-specific solutions and services operating in Insurance, Banking and Parabanking.

The company's team of consultants brings a wealth of experience and expertise to each engagement, offering insights and perspectives that enable clients to make informed decisions and take decisive action. BGP's approach is characterized by a commitment to excellence, innovation, and collaboration. The company's consultants are known for their ability to work closely with clients, leveraging their expertise to deliver measurable results and value. The various teams are also adept at managing complex projects, ensuring that they are delivered on time, within budget, and to the highest standards of quality. One of the key strengths of BGP is its ability to tailor its solutions to each client's unique needs and objectives. The company understands that every organization faces its own set of challenges and opportunities, and its consultants take the time to gain a deep understanding of each client's situation before proposing solutions. This approach ensures that BGP's solutions are relevant, effective, and sustainable.

3 Privacy & Regulations

In the digital age, privacy has become an increasingly important issue, as emerging technologies have made it easier for individuals and organizations to collect, store, and analyze vast amounts of personal data through search engines and social media platforms. The latter is being used for various purposes, including targeted advertising, data analysis, and even surveillance. While these advances have brought many benefits, they have also raised concerns about the potential misuse of personal information, and the erosion of privacy rights. New laws and regulations have been implemented in recent years to ensure the safety of the individual in the face of these social and technological changes. One of these is the GDPR (General Data Protection Regulation), a regulation created by the European Union to provide individuals with more control over their personal data and to regulate the way businesses handle that data.

Before talking about how this regulation addresses the goals of control and security of the individual's data, it is necessary to clarify what is meant by privacy.

3.1 Defining Privacy

Privacy is a concept that has been studied for many years, well before the advent of new technologies in this digital age. It is a broad concept that encompasses several subjects and areas, which many scholars have not yet been able to define.

Daniel J.Solove defines privacy as a "sweeping concept", an all-encompassing concept that includes various aspects, such as: the freedom of thought, autonomy over one's body, seclusion within one's dwelling, authority over personal information, freedom from monitoring, safeguarding one's reputation, and shielding oneself from invasive searches and interrogations. [1] Arthur Miller has expressed his opinion that privacy is a challenging notion to define because it is remarkably ambiguous and elusive. In his paper, Daniel J. Solove summarizes the concept of privacy under six headings: (1) the right to be let alone (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy. These headings often overlap, yet each has a distinctive perspective on privacy [1].

[1] In this Article, Professor Solove develops a new approach for conceptualizing privacy. He begins by examining the existing discourse about conceptualizing privacy, exploring the conceptions of a wide array of jurists, legal scholars, philosophers, psychologists, and sociologists. Solove contends that the theories are either too narrow or too broad.

1. *Right to be let alone*

   The concept of the right to be let alone was first introduced by the American lawyer Louis Brandeis and his colleague Samuel Warren in a famous law review article in 1890 *"Right to Privacy"*, and is perceived as the foundation of privacy law in the United States. They argued that the right to privacy is essential for personal autonomy and dignity, and that it should be protected by law. They defined privacy as the "right to be let alone," a phrase adopted from Judge Thomas Cooley [2]; but in his treatise he meant it as a way of explaining that attempted physical touching was a tort injury.[2] Warren and Brandeis observed that increasingly, "modern enterprise and invention have, through invasions upon his privacy, subjected [an individual] to mental pain and distress, far greater than could be inflicted by mere bloody injury". The authors noted that this type of harm was not typically protected by law. In its Fourth Amendment jurisprudence, the Court has often referenced Brandeis's definition of privacy as "the right to be let alone." *"[The right to privacy] is, simply stated, the right to be let alone,"* Justice Fortas observed, *"to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law"*[3]. But many commentators argue that this definition is too broad [3]. Although Warren and Brandeis used the term "inviolate personality" to describe the content of the private sphere, it is too vague and lacks elaboration. Legal scholar Ruth Gavison argues that the right to be let alone often refers to non-interference by the state but overlooks the fact that most privacy claims are protection against other individuals' interference, rather than the state's.[1]

2. *Limited Access to The Self*

   Daniel J. Solove writes that the limited access to the self is a *"concept that recognizes the individual's desire for concealment and for being apart from others. In this way, it is closely related to the right-to-be-let-alone conception, and is perhaps a more sophisticated formulation of that right".* [1] Limited access to the self is considered an essential aspect of privacy because it enables in-

[2] Around the same time that Warren and Brandeis published their article, the Supreme Court referred to the right to be let alone: "As well said by Judge Cooley: 'The right to one's person may be said to be a right of complete immunity; to be let alone."

[3] The right to be let alone views privacy as a tyope of immunity or seclusion. As many scholars lament, defining privacy as the right to be let alone is too broad. For example, legal scholar Anita Allen explains: "If privacy simply meant 'being let alone,' any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy. A punch in the nose would be a privacy invasion as much as a peep in the bedroom" [1]

dividuals to maintain autonomy and control over their personal lives [4]. It allows individuals to keep certain information and aspects of their life private, to avoid unwanted intrusion, and to protect themselves from harm [5]. E.L. Godkin, a well-known writer of the late nineteenth century, advanced an early version of the limited-access theory when he observed that *"nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion"* [4]. For philosopher Sissela Bok, privacy is *"the condition of being protected from unwanted access by others- either physical access, personal information, or attention".* The concept of limited access to the self is particularly relevant in the digital age, where personal information can be easily shared and accessed without an individual's consent. The right to control access to personal information has become an important issue in debates around data privacy and cybersecurity, as individuals seek to protect themselves from unwanted data collection, surveillance, and hacking.[1]

3. *Secrecy*

   According to Judge Richard Posner: *"[T]he word 'privacy' seems to embrace at least two distinct interests. One is the interest in being left alone-the interest that is invaded by the unwanted telephone solicitation, the noisy sound truck, the music in elevators, being jostled in the street, or even an obscene theater billboard or shouted obscenity.... The other privacy interest, concealment of information, is invaded whenever private information is obtained against the wishes of the person to whom the information pertains"*[5]. The latter privacy interest, *"concealment of information"*, involves secrecy. Posner defines it as an individual's *"right to conceal discreditable facts about himself"* [6] [6]. A number of theorists have claimed that understanding privacy as secrecy conceptualizes privacy too narrowly. Secrecy can be a component of privacy, as individuals

[4] This conception recognizes the individual's desire for concealment and for being apart from others.[1]

[5] Solove adds that "The limited-access conception is not equivalent to solitude. Solitude is a form of seclusion, of withdrawal from other individuals, of being alone. Solitude is a component of limited-access conceptions as well as the right-to-be-let-alone conception, but these theories extend far more broadly than solitude, embracing freedom from government interferences as well as from intrusions by the press and others. Limited-access conpetions recognize that privacy extends beyond merely being apart from others". [1]

[6] Poosner sees privacy as a form of self-interested economic behavior, concealing true but harmful facts about oneself for one's own gain. People "want to manipulate world around them by selective disclosure of facts about themselves"

may choose to keep certain aspects of their life private and not share them with others. The privacy-as-secrecy conception can be understood as a subset of limited access to the self. Secrecy of personal information is a way to limit access to the self. However, secrecy can also be used to deceive or hide information that others have a legitimate interest in knowing.[1] [7]

4. *Control of Personal Information*
   According to Charles Fried, *"Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves".* According to Alan Westin: *"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". [1]* Charles Fried links his definition of the scope of personal information to the value of privacy. He defines privacy as *"control over knowledge about oneself"* that is necessary to protect *"fundamental relations" "respect, love, friendship and trust".* President Clinton's Information Infrastructure Task Force has defined privacy as *"an individual's claim to control the terms under which personal information- information identifiable to the individual-is acquired, disclosed, and used* "[7]. The Supreme Court has even stated that privacy is "control over information concerning his or her person"[8]. Scholars argue that in addition to failing to adequately define the scope of information, the conceptions of privacy as control over information fail to define what is meant by "control" over information [8]. According to Locke, privacy flows naturally from selfhood: *" Every man has the property in his own person"*[9]. While Inness writes that not all personal information is private; she contends that *"it is the intimacy of this information that identifies a loss of privacy".* In the digital age, personal information is often collected and processed by companies, governments, and other organizations, which can create privacy risks for individuals. Without proper safeguards, personal information can be used to profile, target, and discriminate against individuals, or to expose them to identity theft, financial

[7] In a variety of legal contexts, the view of privacy as secrecy leads to the conclusion that once a fact is divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private. Privacy is thus viewed as coextensive with the total secrecy of information [1]

[8] The theory is too vague because proponents of the theory often fail to define the types of information over which individuals should have control. Some theorists attempt to define the scope of what constitutes personal information over which individuals should exercise control, but their attempts run into significant difficulties. For example, legal scholar Richard Parker's theory defines the scope of personal information extremely broadly: "Privacy is control over when and by whom the various parts of us can be sensed by others" [1]

fraud, and other forms of harm. The control of personal information is therefore essential for protecting individual privacy and ensuring that personal data is used ethically and responsibly. [1]

5. *Personhood*
   The theory of privacy as personhood deviates from the previously discussed theories because it is constructed around a normative end of privacy, namely the protection of the integrity of the personality. This theory is not detached from other theories , and it often is used in conjunction with the other theories to explain why privacy is important [1] [9]. Building upon Warren and Brandeis' notion of "inviolate personality", Paul Freund coined the term "personhood" to refer to *"those attributes of an individual which are irreducible in his selfhood"*.[10]

6. *Intimacy*
   This theory appropriately recognizes that privacy is not just an essential to individual self-creation, but also human relationships [10]. In *Privacy, Intimacy, and Isolation*, philosopher Julie Inness advances an intimacy conception of privacy: *"[T]he content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas . . . I suggest that these apparently disparate areas are linked by the common denominator of intimacy-privacy's content covers intimate information, access, and decisions."*[11]

Daniel J. Solove writes also about DeCew's definition of privacy. He states that *"According to DeCew, there are three overlapping claims: informational privacy, accessibility privacy and expressive privacy. Informational privacy involves "control over information about oneself."* Accessibility privacy is the limited-access conception: *"accessibility privacy focuses not merely on information or knowledge but more centrally on observations and physical proximity. Expressive privacy "protects a realm for expressing one's self-identity ot personhood through speech or activity."*

[9] This theory is not independent from the other theories, and it often is used in conjunction with the other theories to explain why privacy is important, what aspects of the self should be limited, or what information we should have control over [1]

[10] We form relationships with differing degrees of intimacy and self-revelation, and we value privacy so that we can maintain the desired levels of intimacy. How is "intimate" information to be defined? For Fried and Rachels, intimate information is that which individuals want to reveal only to a few other people for each of our varied relationships. [1]

Thus, DeCew combines three theories of privacy: (1) control over information; (2) limited access; and (3) personhood.” [1] [11]

As we have observed, the definition of privacy is not singular, but rather encompasses various nuances that are applied to different concepts. To establish a more precise framework for this concept, it is essential to consider the historical reference period and socio-cultural context. Jeff Smith et al. highlight that recent evolution of privacy in general follows the evolution of information technology. They write about four periods of privacy development:

- Privacy Baseline (1945-1960): whose characteristics are the limited information technology developments, high public trust in governments and business sector, and general confort in information collection;[12]

- First Era of Contemporary Privacy Development (1961-1979): where there is the rise of information privacy as an explicit, social, political and legal issue. There is the early recognition of potential dark side of the new technologies, the formulation of the Fair Information Practices (FIP) Framework [12] and establishing government regulatory mechanisms established such as the Privacy Act of 1974;[12]

- Second Era of Privacy Development (1980-1989): there is the rise of computer and network systems, database capabilities, federal legislations designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national data protection laws for both private and public sectors; [12]

- Third Era of Privacy Development (1990- present): there is the right of the Internet, Web 2.0 and the terrorist attack of 9/11 dramatically changed the landscape of information exchange. Privacy concerns rise to a new level. [12]

[11] Other scholars also recognize that privacy cannot be consolidated in a single conception, and instead they cluster together certain conceptions. For example, Jerry Kang defines privacy as the union of three overlapping clusters of ideas: (1) physical space; (2) choice; (3) flow of personal information;

[12] The Privacy Act FIPs are based on the Code of Fair Information Practices, developed in 1972 by the Department of Health, Education, and Welfare. The Code is based on five principles: (1) There must be no personal data record-keeping systems whose very existence is secret; (2) there must be a way for a person to find out what information about the person is in a record and how it is used; (3) there must be a way for a person to prevent personal information that was obtained for one purpose from being used or made available for other purposes without the person’s consent; (4) there must be a way for a person to correct or amend a record of identifiable personal information; and, (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data [18]

They also give a definition of privacy following two distinct points of view: the value-based definition views general privacy as a human right integral to society's moral value system [13]; under the commodity view, privacy is still an individual and societal value, but it is not absolute, as it can be assigned an economic value and be considered in a cost-benefit calculation at both individual and societal levels [14].

3.2 What Privacy Is Not

Despite the many definitions of privacy, it is worth clarifying what Smith et al. define *"What Privacy Is Not"*: (1) Anonymity, (2) Secrecy, (3) Confidentiality, and (4) Security.

Anonymity is defined as the ability to conceal a person's identity which is central for the information collected for statistical purposes. It occurs when a person behaves in a manner that restricts the accessibility of identifiers to others. This lack of correlation between the data and the person allows for greater privacy control [15]. Nonetheless, alternative approaches to achieving such control also exist.

Secrecy has been defined as intentional concealment of information. Secrecy enables individuals to manipulate and control environments by denying outsiders vital information about themselves. Warren and Laslett also analyze the distinction between privacy and secrecy conceptually [16]. They argue that secrecy involves the concealment of information that is negatively perceived by those who are excluded from it. On the other hand, privacy protects behavior that is either morally neutral or deemed valuable by society[13].

[13] This view of general privacy is fundamentally normative, and some scholars claim that it may be at odds with the legal and societal frameworks of various cultures and thus cannot be treated absolutely. [12]

[14] To explain the phenomenon of voluntarily providing information online (so-called self-surveillance) social scientists recognize the economic component of privacy: individuals cooperate in the online gathering of data about themselves as economic subjects. This participation in surveillance is possible because of recent reconceptualization of privacy in the consumer's mind from a right or civil liberty to a commodity that can be exchanged for perceived benefits [12]

[15] Anonymity is not dichotomous, in that it varies in degrees : individuals can choose to be totally anonymous, pseudonymous, or identifiable [12].

[16] Although secrecy is easily distinguishable from privacy , they are often mistaken and confused with each other. "Privacy need not hide; and secrecy hides far more than what is private" [12]

Confidentiality [17] concerns the externalization of restricted but accurate information to a specific entity while privacy corresponds to the desire of a person to control the disclosure of personal information.[14]

According to Belanger et al. security corresponds to the concerns about the protection of personal information with three specific goals : integrity that assures information remains unaltered during transit and storage[15]; authentication which verifies a user's identity and eligibility to access data[16]; and confidentiality that requires data use is confined to authorized purposes by authorized people [17].

3.3 Information Privacy

The concept of privacy is evolving with new technologies; not only have we not yet been able to give a specific definition to the concept, but new concerns about how it is protected and managed by institutions and organizations are emerging from the literature.
Will Thomas DeVries writes that *"The modern evolution of the privacy right is closely tied to the story of industrial-age technological development"* [18]. The world around us is changing and evolving really quickly, as the advent of advanced information and communication technologies are changing the view around the concept of privacy. Digital technology-computing, databases, the Internet, mobile communications call for further evolution of privacy rights, both conceptually and in law[18]. The 21st century in fact proposes new technologies for communications, cloud computing, Internet of Things, Big Data Analysis and many more. Each of these technologies has its own development in the years and creates new opportunities for collaboration, remote storing data, smart application, processing very large data.[19] The amount of digital information generated is breathtaking.

In this framework, it is worth mentioning the concept of information privacy, which is a subset of the overall concept of privacy. Clarke defined information privacy specifically as *"the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves"*[20]. Numerous interpretations of information privacy exist, yet the fundamental components of these definitions tend to remain consistent. Typically, they involve a degree of authority over the

[17] Confidentiality corresponds to the controlled release of personal information to an information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.[12]

possible secondary applications of an individual's personal data, whereby secondary use denotes the utilization of information for objectives beyond its initial collection intent [17].
Informational privacy has been a concern way before the development of personal data. With the advent of modern industrial society, third party entities such as governments, banks, schools, began to acquire personal information of citizens and customers. Despite the private nature of those informations and the fact that often they were intimate, the individuals' right to have protection was unclear.[18] Today those new communications collect data on a daily and global basis. The internet is decentralized, open and interactive, so the way users engage to it is really easy; moreover the latter can reach others despite geographic, social, and political barriers.

The issue about redefining privacy in the digital age is fundamental to all policy, legal and cultural discussions, because the new growth of data we are facing needs to be addressed [20]. Jerry Berman and Deirdre Mulligan highlight three significant digital advancements that significantly impact privacy. These include: (1) the increase of data generation and the consequential accumulation of extensive amounts of personal data, caused by the recording of nearly every modern interaction [18]; (2) the globalization [19] of the data market and its accessibility for anyone to compile and scrutinize this data; and (3) the inadequacy [20] of control mechanisms for digital data that previously safeguarded analog data [21]. Individuals have minimal control in handling their personal information, and most people are not even aware what information has been collected or how it is being used [1]. Berman et al. list sources from which every day data are collected and taken, such as transactional data, click stream data, "mouse droppings", IP addresses, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites. This data, which may or may not be enough to identify a specific individual, is captured at various points in the network and available for reuse and disclosure[21].
In this new era of digitalization, there are many values that we still believe to be

[18] The amount of digital information generated is breathtaking. Every interaction with the Internet, every credit card transaction, every bank withdrawal, every magazine subscription is recorded digitally and linked to specific individuals. In the analog world, these transactions were either not registered at all or recorded on paper in a single page [18]

[19] All this information once it is collected in networked databases, can be sent instantaneously and cheaply around the world [18]

[20] Individuals have little ability to control this collection or manipulation. Not only does much of this happen far from the reach of regulators, but most people are not aware what information has been collected or how their information is being used [18]

present but are actually losing, such as the concept of anonymity [21]. The physical world is vastly different from the digital one: in a physical store, one can enter, look at the goods, and leave without being noticed by anyone. However, it's not the same on the internet; every movement is tracked and saved due to the trail of data that is carried during online browsing. The technologies' surveillance capacity to collect, aggregate, analyze and distribute personal information coupled with current business practices have left individual privacy unprotected. The Internet has changed the quantity and quality of data available about individuals' lives, but unfortunately our business practices, norms, and laws have not progressed to ensure individuals' privacy [21].

3.4 Other Factors Shaping Privacy

The study carried out by Smith et al. *"Information Privacy Research: An Interdisciplinary Review"* linked the concept of privacy to other factors not yet mentioned above. More specifically they highlight factors that influence the view of privacy.

First of all, privacy can be connected to experience, since they found out that individuals who have encountered or been subjected to personal information abuses tend to have heightened concerns about privacy experiences. Then, the concept of awareness [22] is worth mentioning, since it reflects the extent to which an individual is informed about organizational privacy practices. Other factors are personality differences [23]: personality traits (such as extroversion, agreeableness, emotional instability, conscientiousness, and intellect[22]) and demographic differences [24]: women have been found to be generally more concerned about the concept of privacy and the risks related to it and people with higher education are more sensitive and aware of potential privacy issues[23]. There are also behavioral factors to be taken into account, depending on the individual's actions during browsing on the Internet [25]

[21] As do other areas of privacy. For example, digital technologies jeopardize the ability to participate anonymously in the digital society because every interaction leaves identifiable fingerprints [12]

[22] Research suggests that consumers' privacy concerns are triggered when consumers become aware that organizations have collected and/or used their personal information without their permission [12]

[23] Bansal et al. (2010) examined the role of the "big five" personality traits in influencing individuals' perceptions of health information sensitivity. These five dimensions of personality are extroversion, agreeableness, emotional instability, conscientiousness, and intellect.[12]

[24] For example, Dinev et al showed that Italian society has a different concept of privacy that leads to lower privacy concerns but also to higher perceived risk [12]

[25] In one study of 477 U.S. households, researchers found that privacy concerns had a significant impact on online purchase intent, with the greatest negative impact being through its relationship with trust (Eastlick et al. 2006). Firms that are positioned as "safer" or "trustworthy" on the privacy dimension

(for example the willingness to disclose information while engaging in commerce); in reference to that, the role of trust has been playing an important role as a variable between privacy concerns and disclosure. This will be discussed in more detail in Chapter 2. In addition to behavioral reactions, an important influence is given by the regulation: Milberg et al. suggest that *"if consumers do not perceive firms as adequately protecting their privacy, they will distrust self-regulation and prefer state intervention, which can eventually lead to a regulatory response"*[24].

3.5 Privacy and Different Cultures

This work will mainly focus on the regulations and tools that protect data privacy within the European Union. However, it is important to note that there is not only a Western perspective. On the contrary, the concept of privacy and its implications can vary depending on where we are in the world. Although privacy regulation exists in almost every culture, the specific behavioral and psychological mechanisms that people use to regulate privacy boundaries are unique to each culture. In the information age, cultural differences in how users interact with technologies and regulate their privacy have become a frequent topic of research and news. For instance, users in Western countries tend to view medical history as highly sensitive data, whereas Eastern countries may have a different perspective[23]. Li et al. conducted a study examining how users' privacy decision-making varies across different cultural contexts and situations [26] data collection strategies, and privacy regula-

will likely have a competitive advantage (Bowie and Jamal 2006). It has been found that consumers who trust the firm are less concerned about their privacy and more willing to provide personal information (Schoenbachler and Gordon 2002). [12]

[26] Their study was conducted taking into consideration Hofstede's model, which identifies six cultural dimensions: (1) Power distance which is the degree to which the less powerful members of a society accept and expect that power is distributed unequally. A high score of PDI indicates that people accept a hierarchical order;(2) Individualism is defined as a preference for a loosely-knit social framework in which individuals are expected to take care of only themselves and their immediate families. Low individualism is collectivism; (3) Masculinity represents a preference in society for achievement, heroism, assertiveness and material rewards for success. Such society is more competitive. Its opposite, femininity, stands for a preference for cooperation, modesty, caring for the weak and quality of life; (4) Pragmatism describes how a society has to maintain some links with its own past while dealing with the challenges of the present and future; (5) Uncertainty Avoidance is the degree to which the members of a society feel uncomfortable with uncertainty and ambiguity; (6) Indulgence (IDL) stands for a society that allows relatively free gratification of basic and natural human drives related to enjoying life and having fun. Its opposite is restraint.[23] Milberg et al. found that power distance, individualism and masculinity had a positive effect on overall information privacy concerns, whereas uncertainty avoidance had a negative effect. Bellman et al.found opposite results, namely that power distance, individualism and masculinity are negatively associated with privacy concerns, and that uncertainty has no significant effect. Posey et al. and Miltgen and Peyrat-Guillard found that focus groups in individualistic societies were more hesitant to disclose information than those in collectivistic societies. Similarly, Cho et al. found that Internet users from highly individualistic cultures exhibited greater concerns about online privacy. Steenkamp and Geyskens found

tions should be developed in response to the international context. Indeed most cross-cultural privacy studies compare privacy attitudes and behaviors at the country level[23]. The authors define individualism as *"a preference for a loosely-knit social framework in which individuals are expected to take care of only themselves and their immediate families"*; while low individualism is collectivism. Posey et al. and Miltgen et al. revealed that participants in focus groups from individualistic societies exhibited greater reluctance to reveal information compared to those from collectivistic societies[25][26]. Likewise, Cho et al. found that Internet users from highly individualistic cultures exhibited greater concerns about online privacy and give more importance to privacy protection and customization than collectivistic countries[27]. [27]

3.6 Right to Privacy and Right to Data Protection

Data protection appeared as an offspring of privacy and the two rights still seem inextricably tied up together. However data protection is trying to mark its own way in life. It is a relatively new concept that emerged with the rise of digital technologies and the collection and processing of personal data. In this paragraph, we will explore the differences between these two rights and how they relate to each other in the context of the modern digital age.

The EU Data Protection Directive (DPD) [28] sees data protection as the protection of *"the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"*. (Article 1 (1).) The notions of *'processing'* and of *'personal data'*, thus appear central for the understanding of the concept of data protection. In general terms, 'processing' can be seen as any operation performed upon the data, from their collection, recording, storage, use, to their disclosure, dissemination, erasure, and destruction. The data is considered personal when they can be linked to a certain individual [28].The ultimate goal of data protection is to promote fairness in the processing of personal data and, to some extent, fairness in the outcomes of such processing. To ensure this

that individualistic countries give more weight to privacy protection and customization than collectivistic countries.[23]

[27] Their study has the objective to discuss what culture measurement is more appropriate and why, considering whether the impact of non-cultural predictors on privacy decisions varies in different cultures.

[28] Adopted in 1995 by the European Union, the Data Protection Directive is officially known as Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Data Protection Directive is binding within the member states of the EU and regulates how personal data is collected and processed in the European Union.

fairness, a set of principles, commonly referred to as *'fair information principles'*[29] or *'data protection principles'*, have been developed. These principles include collection and purpose limitation, data quality, data security, openness and transparency of processing, accountability, and individual participation." [28] [30]

There are ongoing debates regarding whether the right to privacy and the right to data protection should be considered as distinct and autonomous or whether the right to data protection is simply a subset of the right to privacy [31]. To better understand their definitions, we must first identify the legal framework in which these two rights are situated.
Personal Data Protection (PDP) is a crucial aspect of privacy that governs the relationship between individuals and society, including government institutions, companies, public and private organizations, and other entities that process personal data. This is directly linked to the privacy of individuals. The growth of IT and increasing the use of computers and information processing in the 1960s and 1970s imposed a strong policy for the Data Protection Right and concrete rules for regulation of collecting, storing and processing personal data. The first significant document of the Council of Europe is Convention 108/1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data [32] [19].
While the US Constitution does not explicitly mention privacy or data protection, protection of both rights is explicitly established at the constitutional level in Europe: in addition to national constitutions, both the European Convention and the Charter of Fundamental Rights have a provision on privacy. At the constitutional level, the right to data protection is considered a fundamental right, along with the

[29] The right to data protection can thus be understood as a set of "fair information practices"30 or as the regulation and organisation of the conditions under which personal data can be lawfully processed.

[30] The Directive further enshrines the main principles of data protection which are the purpose specification principle (the processing and use of data must happen for specified, explicit and legitimate purposes), the fairness principle (all processing must be fair and lawful to the data subject) or the data quality principle (all data must be adequate, relevant and not excessive in relation to the purpose for which they are processed).[30]

[31] Although such an independent right exists at national level in some EU Member States, data protection is treated as a subset of the right to privacy in international human rights texts and by several other EU Member States, such as the Netherlands, Spain and Finland. For instance, section 10 of the Finnish Constitution, entitled 'The right to privacy' states 'Everyone's private life, honour, and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. At present, conceptions of the role data protection norms should play in society differ greatly between EU Member State [29]

[32] The Convention opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field. Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.

right to privacy, and is enshrined in the Charter of Fundamental Rights of the European Union, which constitutes primary EU law [29].Most literature tells us that these two rights are not identical; the right to privacy is considered by some to be a much broader concept. These two rights can be found in Articles 7 and 8.
Article 7 of Charter of Fundamental Rights of the European Union, *Respect for private and family life* stipulates that:
"Everyone has the right to respect for his or her private and family life, home and communications".
Article 8 of Charter of Fundamental Rights of the European Union, *Protection of Personal Data* stipulates that:

1. *"Everyone has the right to the protection of personal data concerning him or her.*

2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

3. *Compliance with these rules shall be subject to control by an independent authority."*

The EU secondary legislation currently in place does not fully consider the fundamental right to data protection outlined in the Charter of Fundamental Rights of the European Union, which has since become an integral part of EU primary law. These legal advancements prompt the question of whether the right to data protection is simply a subset of the right to privacy or if it offers additional protection. There is no corresponding provision on data protection in the Convention. Article 8 of the Charter establishes a distinction between data protection and privacy and outlines particular safeguards in paragraphs 2 and 3. These guarantees include processing personal data in a fair and specified manner based on consent or other lawful grounds; providing individuals with the right to access and correct data collected about them; and ensuring independent oversight of compliance with these regulations by an impartial authority. The Court has established that the article can encompass a broad range of matters, including but not limited to bodily integrity, access to information and public records, confidentiality of correspondence and communication, safeguarding of the home, protection of personal data, and more. In other words, the list of issues covered by this article is not exhaustive [30]. Data protection is also enshrined in a series of (quasi-)legislative EU instruments,

the most important of which is the Directive 95/46/EC known as the Data Protection Directive that introduced data protection principles within EU law and set the main benchmarks for the protection of personal data in the EU. The Directive enacts the principles for the legitimate processing of personal data, it provides rights for data subjects and imposes obligations upon data controllers [30].The right to data protection can thus be understood as a set of “fair information practices” or as the regulation and organization of the conditions under which personal data can be lawfully processed.
Although European law distinguishes between privacy and data protection, they intersect. While data protection applies automatically to any processing of personal data, privacy only comes into play if the European Court of Human Rights (ECtHR) determines that the processing in question constitutes an infringement of an individual’s right to privacy under Article 8 of the European Convention on Human Rights (ECHR) [30].

To the purpose of distinction of the rights, the Court differentiates between two types of data processing: those that pertain to an individual’s private life and those that do not. This distinction is based on two criteria: the nature of the data being processed and the scope of the processing. If the data is inherently connected to a person’s privacy, then it falls within the purview of Article 8 of the ECHR without requiring further analysis. However, if the data is not "fundamentally private," the Court will assess the extent of the processing to determine whether it constitutes an interference with an individual’s right to privacy.
Different opinions have also been formed regarding the scope of the two rights. Data protection is considered both narrower and broader than privacy. It is narrower because it deals only with the processing of personal data, whereas the purpose of privacy is considered much broader. On the other hand, it is broader because it applies to the processing of personal data even without taking into account the sphere of privacy. Similarly, privacy is both narrower and broader at the same time: it might apply to a processing of data which are not personal but nevertheless affects one’s privacy, while it will not apply upon a processing of personal data which is not considered to infringe upon one’s privacy. It can also be argued that the processing of personal data may have implications beyond privacy and affect other constitutional rights. This is particularly evident when the processing of data related to individuals carries the risk of discrimination [30].

3.7 Overview of the GDPR and Digital Services Package

In this digital era, online platforms play an increasingly important and influential role in society, the economy, and democracy. However, this power also brings challenges and risks to fundamental rights, respect of someone's privacy, competition, and innovation. To address these challenges, it is necessary to have adequate and up-to-date regulations that protect the fundamental rights of users and businesses. For this reason, the European Union has introduced three new legislative measures aimed at regulating the digital market and services: the General Data Protection Regulation, the Digital Services Act, and the Digital Markets Act. In this section, all three regulations are briefly described, outlining their fundamental principles and objectives, identifying the stakeholders involved, and summarizing the achieved outcomes.

3.7.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR)[33] is a comprehensive privacy law that came into effect in the European Union (EU) in May 2018. The GDPR replaces the outdated Data Protection Directive of 1995 and provides a modern and more robust framework for protecting personal data in the digital age. The directive no longer met the privacy requirements of the new digital landscape, while the new regulation introduces significant changes regarding personal data and privacy, aiming to give more control to citizens over their personal data to ensure a harmonized, unified and sustainable approach to data protection [31]. For this matter, the GDPR is said to introduce a higher level of harmonization of data protection law throughout the European Union.

First it is important to highlight the difference between a directive and a regulation. The first one lays down certain results that must be achieved and each Member State is free to decide how to transpose directives into national laws. Regulations, however, have binding legal force throughout every Member State. Therefore, GDPR is applicable in every member state without the need for a national legislation implementation, unifying the European Union rules and laws. In con-

[33] GDPR's life-cycle started in January 2012 with a proposal from the European Commission. After a long-run discussion, the regulation was approved on April 27, 2016. However, the European Union established a two year transitional period for organizations to achieve compliance, so that these were able to implement the necessary changes in the meantime, until May 25, 2018 (Lopes and Oliveira, 2018; Sirur et al., 2018). [31]

trast to this legal framework, the US takes a sectoral approach (for example by separately regulating children's privacy or insurance and health privacy); yet it does not have an overall federal protection law.

The objective of this regulation by the EU is to empower citizens with greater control over their personal data, strengthen their rights, change the way organizations [34] handle and govern such information, and eliminate barriers to cross-border trade. These measures will facilitate the expansion of businesses throughout Europe while also safeguarding the unrestricted flow of personal data among member states [31]. Possible reason behind the GDPR implementation is that the EU aims at regaining the people's trust in the responsible treatment of their personal data in order to boost the digital economy across the EU-internal market. Considering the difficulties presented by a global economy, emerging technologies, and new business models, the lawmakers have established a comprehensive framework that will have far-reaching implications for many businesses. As not only data protection duties but also the impending fines have been significantly increased, companies should carefully reorganize their internal data protection procedures in order to reach compliance with the GDPR [32].

This regulation applies to anyone processing or controlling the processing [35] of personal data. Given the exponential growth of data and its importance for business processes and objectives, companies will be affected.
The notions of controller and processor are used to delineate and assign the tasks, responsibilities and liability of entities that processes personal data under the GDPR. They were already present in the 1995 Directive; however, the GDPR has assigned more responsibilities to data processors [33]. The controller is defined as a *"natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data"*

[34] The EU legislator made the decision to uphold a principle- and rights-based approach for the GDPR, which maintains a neutral stance towards technology. This choice aligns with the comprehensive nature of the GDPR, which aims to encompass a wide range of situations. To achieve this, the GDPR relies on general principles that processing entities must follow to ensure compliance. This approach, known as the 'risk-based approach,' requires organizations to assess their operations internally and continuously take appropriate measures to adhere to the GDPR. In doing so, organizations must ensure that their level of compliance is proportionate to the inherent risks associated with their processing activities. [33]

[35] Processing with respect to personal data may include, but is not limited to, the following: "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

(Article 4(7) GDPR), while the processor is *"a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller."* [36](Article 4(8) GDPR) [32]. Thus, the existence of a processor depends on a decision taken by the controller, who can either process data within its organization or delegate all or part of the processing activities to an external organization, rendering the latter a 'processor'. For an entity to be considered a processor, two criteria must be met: firstly, it must be a distinct legal entity or individual separate from the controller, and secondly, it must process personal data on behalf of the controller [32]. Those who process personal data [37] – that is, both the data controller and the data processor – must comply with the rules of the Regulation to avoid any manipulation of individuals' personal data [34].
Personal data are defined as *"any information relating to an identified or identifiable natural person ('data subject'),"*(Article 4(1) GDPR) and may include location data, online identifiers, and other forms of information that may be used to identify a data subject directly or indirectly, in addition to classic identifying data such as names and identification numbers. According to Article 9 GDPR, special categories of personal data, also referred to as 'sensitive personal data', include (i) racial or ethnic origin, (ii) political opinions, (iii) religious or philosophical beliefs, (iv) trade union membership, (v) genetic data, (vi) biometric data, (vii) data concerning health, (viii) sex life or sexual orientation [31].

The literature identifies the material and territorial scope of the regulation. With regard to the material scope, the GDPR applies to both public bodies as well as private organizations. However, distinct rules for the EU institutions, bodies and agencies exist (Article 2(3) GDPR). The GDPR applies to the processing of personal data (Article 2 GDPR). Two notions have to be considered here: (i) the notion of personal data and (ii) the notion of processing [31].
For what concerns the territorial scope, despite being a European Regulation, the GDPR's reach extends beyond the borders of Europe. Its transnational application is designed to ensure the comprehensive privacy protection of individuals and promote fair competition within the EU's internal market. Its territorial scope is broader than the one of the Data Protection Directive. under the GDPR, processing

[36] The consideration of a processor's activities in determining the territorial scope of the GDPR reflects the greater accountability of processors under the GDPR, when compared to the Data Protection Directive.

[37] Numerous different combinations of controllership and processor relations are possible (controller and processor are one entity; controller and processors are separate entities; joint controllers; sub-processors; etc.) [33].

merely must occur *"in the context of the activities of an establishment of a controller or a processor in the Union".* The GDPR also applies to the *"processing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the [European] Union"* so long as the processing is related to *"the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union"* or the monitoring of such data subjects' behavior *"as far as their behavior takes place within the [European] Union."* [38] (Article 3(2) GDPR) [32].

The extensive territorial reach of this regulation, coupled with its mandatory compliance requirements for both public agencies and private organizations, can be described as an "omnibus approach."

Article 5 GDPR lays down the principles allowing for lawful processing of personal data. These principles are:

1. *Lawfulness, Fairness and Transparency.*
   'Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject'. The processing of personal data is lawful when it is based on one of the six legal bases listed in Article 6 GDPR. The principles of fairness and transparency relate to the fact that data subjects must be informed in a comprehensive manner about the purpose and scope of the processing as laid down in Articles 12–14 GDPR. Individuals need to be enabled to understand what is happening to their personal data. Transparency must be ensured, whereby individuals are made aware of the collection, utilization, consultation, or processing of their personal data, and the extent to which it is or will be used [33].

2. *Purpose Limitation*
   Data is *"collected for specified, explicit, and legitimate purposes".* In line with the principle of transparency, data can only be processed for a specific purpose, which has to be communicated to the data subject. The General Data Protection Regulation stipulates that data cannot be processed for purposes that are not consistent with the original intention [39]. However, there are some

[38] For example, the GDPR applies to a U.S. provider's cloud-based-services offering to individuals in the European Union, even where the offering requires no payment and the provider has no establishment in the European Union, to the extent that the offering involves processing those individuals' personal data.

[39] Allowing the controller to evaluate whether personal data processing for a purpose other than the one for which the data were originally collected enjoys such a basis, where it is not based on the law or the data subject's consent. This compatibility determination considers, among other things, links between the two purposes, context (including the relationship between the data subject and the controller), the data's nature

exceptions [40] to this rule, such as archiving in the public interest, scientific or historical research, and statistical analysis [41]. These exceptions allow for additional data processing under certain circumstances [33].

3. *Data Minimisation*

   Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This principle requires controllers to minimize the data they collect and keep [33]. By doing this, two major benefits can be derived: first, in the event of a data breach, the unauthorized individual will only have access to a limited amount of data; second, data minimisation makes it easier to keep the data accurate and up to date.

4. *Accuracy*

   The data collected should be accurate and, where necessary, kept up to date. The controller is obliged to ensure the accuracy of the data [33]. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete [42].

5. *Storage Limitation*

   This principle requires controllers to specify the time limit for after which data is deleted. In the context of research, Article 89 GDPR provides for certain derogations [43] if the requirements under that article are fulfilled. The storage period shall be limited to a strict minimum. In order to ensure this storage

(specifically, whether special data categories are involved), possible consequences for the data subject, and the existence of "appropriate safeguards," which could include data encryption or pseudonymization. [33]

[40] Whereas the Data Protection Directive allowed Member States to determine personal data storage periods for "historical, statistical or scientific use," the GDPR establishes a specific regime for personal data processing "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." [34]

[41] In addition, the GDPR allows Member States or the European Union to derogate from a data subject's rights to access or correct his or her personal data, and object to or restrict its processing, where the derogation is for scientific or historical research purpose—or statistical purposes if the data subject's exercise of such rights is "likely to render impossible or seriously impair the achievement of the specific purposes," subject to the safeguards mentioned above. Another provision permits certain derogations for archiving purposes in the public interest. Where the processing has multiple purposes, the derogation will only apply to the corresponding purposes [34]

[42] In addition, the GDPR specifies that inaccurate data must be erased or rectified "without delay," adding a time element to the "accuracy" principle already contained in the Data Protection Directive. [34]

[43] Instead, the data may be stored for longer periods subject to "implementation of the appropriate technical and organisational measures required . . . to safeguard the rights and freedoms of the data subject." These measures implement the "data minimization" principle, and they may include the use of pseudonymization (for de-identification), where relevant.[34]

limitation, time limits should be established by the controller for erasure or for a periodic review [33].

6. *Integrity and Confidentiality*
   Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures [33].

7. *Accountability*
   The principle of accountability calls for entities processing personal data to take a proactive and holistic stance towards compliance with the GDPR [44].

There are legal bases of GDPR in order to be able to process personal data in a lawful manner, the most important are listed below.

- Consent: to be a lawful legal basis, consent by the data subject must fulfil the conditions listed in Article 7 GDPR. Consent must be (i) freely given, (ii) specific, (iii) informed, (iv) unambiguous, (v) and the age of consent must be fulfilled. The consent must be given through a clear affirmative act (for example, pre-ticked boxes on a consent form are prohibited). The burden of proof to demonstrate that consent was lawfully obtained lies with the controller. Hence, good documentation and archiving of consent forms is required. When processing sensitive data, the GDPR mandates that explicit consent must be obtained from the data subject (Article 9(2) GDPR). Explicit [45] consent requires a clear and affirmative action by the data subject. This means that the data subject must provide a statement of consent that is expressly given. One way to ensure that consent is explicit is to obtain it in writing, with the data subject signing the statement to remove any doubts or potential lack of evidence in the future. However, the controller may also utilize other methods such as a two-step verification process or allow the data subject to provide the necessary statement by filling out an electronic form, sending an email,

[44] Finally, the “accountability” principle requires the controller to be able to demonstrate compliance with the other personal data processing principles. [34]

[45] Where consent is the processing basis, it must be unambiguous. The Data Protection Directive provided that “the data subject’s consent” meant “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” The GDPR sets out additional conditions for such consent beyond those contained in the Data Protection Directive, including a requirement that the controller be able to demonstrate that the data subject has given his or her consent. [34]

uploading a scanned document with their signature, or using an electronic signature.[33].

- Legitimate interest of the controller or by a third party: to establish this legal basis, an evaluation of the necessity and purpose of the processing operation is necessary, along with a balancing test between the data subject's interests and those of the controller and third parties. In other words, the legitimate interest of the controller and any stakeholders must be weighed against the fundamental rights and interests of the data subject, particularly those pertaining to data protection and privacy [46] [33].
- Compliance: Entities that process personal data must meet a set of compliance criteria to be accountable. These criteria include adhering to data protection principles when processing personal data. Additionally, entities must enable and ensure data subject rights, which involves responding to requests for access to personal data and providing fair and transparent information to data subjects about the processing of their data [33].

In line with the risk-based approach taken by the GDPR, it might become necessary to consult the supervisory authority prior to commencing a risky processing operation.

3.7.2 Digital Services Package

The e-commerce directive [47](introduced about 20 years ago) was the first step for the EU legal framework of digital services and introduced EU level conditional limitations for the liability of intermediary services for the third party content, but

[46] The outcome of the balancing exercise must be that the legitimate interest of the controller or any third party outweighs the interests and fundamental rights of the data subject in order for the processing to be lawful under this legal basis.[33]

[47] The E-Commerce Directive is a European Union directive that establishes harmonized rules on issues such as transparency and information requirements for online service providers; commercial communications; electronic contracts and limitations of liability of intermediary service providers1. The directive was adopted in 2000 and has since been amended several times. It limits damages liability of information society service providers when they act in one of the intermediary roles identified by the Directive, i.e. mere conduit, caching and hosting1. For the last 20 years, a core principle of the E-Commerce Directive has been that online intermediaries are not liable for the information transmitted through its service or posted by its users, provided it was not actively involved in the transmission or took action to delete or disable access to the illegal or even 'harmful' information upon obtaining knowledge or awareness.While the E-commerce Directive focused on establishing an appropriate European regulatory framework, it has also recognised the global nature of electronic communications. Hence, the directive aimed at contributing to the establishment of a common and strong negotiating position of the EU in international forums. The directive assumed that, in order to allow the unhampered development of electronic commerce, the legal framework must be consistent with the rules applicable at an international level so that it does not adversely affect the competitiveness of European industry or impede innovation in that sector.[66]

the e-commerce directive is still a sort of benchmark of the rules governing digital services in the EU market. In comparison with 20 years ago, digital services from an economic and political perspective have changed very much. Platforms have become a sort of public space where people share and access information, businesses reach the customers, politicians communicate with citizens, and there is a transformation of digital services into even more complex environments. Platforms create lots of opportunities, but at the same time several challenges, such as the proliferation of illegal content, and this is the reason why the EU has adopted in the past years many legislative initiatives and guidelines. Many initiatives have been adopted from each member state, leaving the national legal framework uncertain and fragmented; that is why Europe has the need to bring up a unified strategy.

A key question concerning the impact of each instrument on users' fundamental rights is how far the Digital Services Package [48] will help strengthen or complement the GDPR. The digital package focuses primarily on regulating the online market; when providing services, online businesses rely heavily on the collection of personal data, and therefore the intertwined application of the GDPR (General Data Protection Regulation), DMA (Digital Markets Act), and DSA (Digital Services Act) requires more exploration [63].

The Digital Services Act and Digital Markets Act aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. The digital package was created by the Commission to regulate and harmonize landmark rules concerning online platforms in the European Union (EU). With the proposed package, the Commission aims to make online platforms more transparent and accountable for how they track and use personal data. At the same time, it aims to empower users with the freedom of choice regarding the content they receive [63].

The Digital Services Act (DSA) and the Digital Market Act (DMA) form a single set of rules that apply across the whole EU. They have two main goals:

1. to create a safer digital space in which the fundamental rights of all users of digital services are protected;

2. to establish a level playing field to foster innovation, growth, and competitive-

[48] The Digital Services Act package was presented by the European Commission in December 20201. Both legislative acts were quickly adopted by the Council and the European Parliament in 2022. Following the adoption of the Digital Services Package in the first reading by the European Parliament in July 2022, both the Digital Services Act and Digital Markets Act have been adopted by the Council of the European Union, signed by the Presidents of both institutions and published in the Official Journal.

ness, both in the European Single Market and globally.

3.7.3 Digital Services Act

The Digital Services Act is a policy document setting the policy goals to achieve in order to have an European strategy for data economy. The DSA introduces a new regulatory framework for online platforms. Its goal is to encourage them to fight objectionable content while respecting users' fundamental rights. It will indeed give better protection to users and to fundamental rights online, respecting the principles of accountability and transparency for online platforms, providing a unified framework across the EU [64].
The DSA has been designed in full compliance with existing rules on data protection, including the General Data Protection Regulation (GDPR) and the ePrivacy Directive, and does not modify the rules and safeguards set out in these laws [49]. The European Parliament and Council reached a political agreement on the new rules on 23 April, 2022 and the DSA entered into force on 16 November 2022 after being published in the EU Official Journal on 27 October 2022 and it is directly applicable across the EU [64]. This Act aims to regulate the activities of "intermediary services" [50] that transmit or store third-party content for EU-based users. This includes social media services, messaging services, cloud infrastructure services, content delivery networks, etc.

The key features of the Digital Services Act can be summarized in five points. Those points have been taken from the paper *"The Digital Services Act: a General Assessment*" by Florence G'sell.
The first one is that it is an asymmetrical regulation. This means that obligations are set for different types of intermediaries based on the nature of their services, as well as their size and impact [64]. This approach aims to prevent the misuse of services for illegal activities and promote responsible operations among providers. Specific substantive obligations are applicable solely to very large online platforms that play a major role in fostering public discourse and facilitating economic transactions [64]. Conversely, very small platforms are exempted from the majority of these

[49] The Digital Services Act sets the horizontal rules covering all services and all types of illegal content, including goods or services. It does not replace or amend, but it complements sector-specific legislation such as the Audiovisual Media Services Directive (AVMSD), the Directive on Copyright in the Digital Single Market, the Consumer Protection Acquis, or the Proposal for a Regulation on preventing the dissemination of terrorist content online.[64]

[50] An intermediary service is any act other than the furnishing of advice, performed by a person for or on behalf of a client or product supplier.

obligations. By adjusting responsibilities within the online ecosystem in line with the size of the players, the proposal ensures that the regulatory costs associated with these new rules remain proportionate [64]. These small enterprises are defined as companies with fewer than 250 employees and an annual turnover under €50 million or an annual balance sheet total under €43 million [64] [51].

Second point, the DSA preserves the exemption from liability established by the E-Commerce Directive in 2000, with additional clarifications. Before the implementation of EU Directive 2000/31/EC, it was not clear to what extent service providers were liable for the content posted on their platforms [65]. The liability regime is based on the prohibition of general monitoring [52]. The first thing that EU legislators intend to avoid is that internet providers could have the control of the natural/legal persons' rights about the processing and transmission and trading in the ecommerce. The intermediaries and the providers had the duty to help natural/legal persons to express the right to take their goods, to use the service they want and not to have the unlawful behavior of stealing and control the identity and aims of natural/legal persons (consumers/buyers). Article 6 of the DSA grants hosting providers immunity from being held liable for any illicit content that may be present on their platforms. However, this protection only applies if they act "expeditiously" to remove access to the content once they become aware of its illegality [65]. Similarly, Article 4 specifies that mere conduit service providers are not liable for the information transmitted or accessed if they do not initiate the transmission, select the receiver of the transmission, or modify the information contained in the transmission [65]. Article 7 of the DSA allows providers to carry out voluntary investigations or take other measures to detect, identify,and remove illegal content. The Good Samaritan clause [53] was added to the DSA in response to requests from online platforms for greater clarity and reassurance that they could take voluntary steps to remove illegal content without losing their liability exemption [65].

[51] By rebalancing responsibilities in the online ecosystem according to the size of the players, the proposal ensures that the regulatory costs of these new rules are proportionate. [64]

[52] The prohibition of general monitoring refers to the fact that intermediaries may not be obliged to monitor their service in a general manner in order to detect and prevent the illegal activity of their users1. A prohibited general monitoring obligation arises whenever content – no matter how specifically it is defined – must be identified among the totality of the content on a platform. [72]

[53] The Good Samaritan clause is a provision in the Digital Services Act that allows service providers to conduct voluntary investigations without losing liability relief. This means they can proactively search for illegal content without fearing losing their liability privileges

The third principle concerns the new obligations for content moderation [54]. These obligations are designed to enable hosting providers to effectively combat undesirable content while upholding users' fundamental rights, notably freedom of expression. Failure to comply with these obligations not only subjects providers to potential sanctions imposed by regulatory authorities but also grants affected users the right to seek compensation for any damages incurred, as outlined in Article 54. This ensures accountability and provides recourse for users in cases of non-compliance [65]. In Article 3 the DSA introduces a broad definition of content moderation as *"the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying, and addressing illegal content or information incompatible"* with the providers' terms and conditions, including *"measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal"*, or that affect the ability of users to publish or transmit information, such as the termination or suspension of a user's account. By encompassing this definition, the DSA acknowledges the crucial role played by platforms in content moderation, often relying on automated tools. As a result, the DSA introduces new obligations pertaining to content moderation that can be classified into four main categories: combating illegal content, upholding procedural safeguards during moderation processes, ensuring transparency, and managing systemic risks. These categories serve as a framework for the comprehensive obligations imposed on platforms in relation to content management under the DSA [65].

Alongside its focus on regulating moderation practices, the DSA also incorporates provisions aimed at safeguarding users of online services in a broader sense, with particular attention given to consumers utilizing marketplaces and collaborative economy platforms. These additional provisions seek to ensure a higher level of protection for users engaging in various online services, emphasizing the importance of consumer rights and their overall experience within these platforms. The DSA indeed includes specific provisions for recommendation systems [55], as online platforms must provide precise and intelligible information about the main parameters used; also it strictly regulates online advertising since they must disclose their prac-

[54] The Digital Services Act proposes rules on transparency of content moderation decisions.

[55] A recommendation system is a subclass of information filtering systems that seeks to predict the rating or the preference a user might give to an item. In simple words, it is an algorithm that suggests relevant items to users. These can be based on various criteria, including past purchases, search history, demographic information, and other factors [73]

tices and targeting methods to advertising recipients [65]. Online platforms that facilitate distance contracts between consumers and traders, including marketplaces and collaborative economy platforms, are subject to specific obligations that they are required to fulfill. These obligations encompass obtaining specific information about their professional users, such as their name, contact details, and identification and registration information. These platforms are expected to adhere to "know your business customer" [56] protocols as part of their obligations to ensure transparency and accountability in the transactions taking place on their platforms [65].

Lastly, the regulation contains specific implementations and enforcement procedures. The regulation is directly applicable and does not require a transposition law to be adopted by each Member State. However, implementing the DSA requires determining which authorities are competent to enforce it and which measures these authorities can take [65]. The competent authorities to control the implementation of the DSA are the national authorities. Member States will designate coordinators that will receive complaints from users, have investigative powers, and may impose sanctions. Penalties will be defined in national law and must be *"effective, proportionate, and dissuasive"*, as provided by Article 52 [65].

To summarize, the DSA introduces new measures that empower users to report unlawful online content, while enabling platforms to collaborate with designated "trusted flaggers" in order to detect and eliminate such content. This enables effective safeguards for users, as it includes a provision that grants users the right to contest content moderation decisions made by platforms. This is facilitated through mandatory disclosure of information to users when their content is removed or restricted, thereby providing them with an opportunity to challenge such decisions [64]. Users will indeed have new rights, including the right to complain to the platform or their national authority. New rules are set to trace sellers on online marketplaces, to help build trust and go after scammers more easily [64]. New measures for transparency for online platforms are set, including better information on terms and conditions, as well as transparency on the algorithms used for recommending content or products to users and many more implementations.

[56] Online marketplaces will also be requested to trace their traders ("know your business customer"). This will ensure a safe, transparent and trustworthy environment for consumers and discourage traders who abuse platforms from selling unsafe or counterfeit goods.[64]

3.7.4 Digital Markets Act

The purpose of the Digital Markets is to ensure equal opportunities for all digital companies, regardless their size. As stated in Article 1(1)[57] of the regulation *"The purpose of this Regulation is to contribute to the proper functioning of the internal market by laying down harmonized rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users."* Particular attention is given to large platforms, the so-called "gatekeepers" [58], whose specific definition is given in Articles 3 [59]and 4 of the regulation. The reasons behind the stipulation of this document is to ensure a fair equilibrium in the digital market: a gatekeeper is likely to lead, in many cases, to serious imbalances in bargaining power and, consequently, to unfair practices and conditions for business users, as well as for end users of core platform services provided by gatekeepers, to the detriment of prices, quality, fair competition, choice and innovation in the digital sector. These gatekeepers control key channels of distribution, a strong power caused by the strong network effects, since users are more likely to value and choose platforms with a large user base; their role as intermediary between sellers and customers, and their ability and possibility to collect large amounts of data [66].

[57] The Digital Markets Act entered into force on 1 November 2022 and its rules started to apply on 2 May 2023. The European Commission will designate gatekeepers by 6 September 2023 at the latest and they will then have a maximum of six months to comply with the new obligations under the Digital Markets Act, so by March 2024.[74]

[58] Article 2 of the DMA, gatekeepers are undertakings that provide a "core platform service" and which are designated as gatekeepers under Article 3.

[59] In order for an undertaking that provides core platform services to be designated as a gatekeeper, three additional qualitative criteria have to be met as set out in Article 3(1). These are linked to a number of quantitative presumptions:
(1)The potential gatekeeper has to have a significant impact on the EU internal market. This criterion is presumed to be met when the undertaking (as a group) has achieved EU turnover of over €7.5 billion in the last three financial years. Or, alternatively, the undertaking has reached an equivalent fair market value of at least €75 billion in the last financial year, and it provides the same core platform service in at least three EU Member States.
(2)The core platform service provided by the undertaking has to serve as an important gateway for business users to reach end users. This is presumed to be the case where the relevant undertaking has more than 45 million monthly active end users established or located in the Union and more than 10.000 yearly active business users established in the Union in the last financial year. Monthly active end users means the average number of monthly active end users throughout the largest part of the last financial year.
(3)Third, the undertaking needs to enjoy an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future. This requirement is presumed to be met if the user number thresholds above have been met in each of the last three financial years.

If all of the quantitative presumptions are met, an undertaking has to notify the Commission within two months. In its notification the potential gatekeeper can provide arguments to demonstrate that in the specific circumstances in which the relevant core platform service operates, the qualitative requirements for being designated as a gatekeeper are not met.[75]

The scope of the regulation is defined in the second paragraph of Article 1, stating that *"This Regulation shall apply to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service."* According to Article 2(1) of the proposed legislation, a gatekeeper is defined as, *"an undertaking providing core platform services"*. Core platform services are subsequently listed in Article 2(2) and may consist of: *"(a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communications services; (f) operating systems; (g) web browsers; (h) virtual assistants; (i) cloud computing services; (j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i)."* [63]

With this regulation, Europe is setting standards for how the digital economy of the future will function; it is a new and innovative regulation, which has received much criticism for implementing appropriate improvements, but it is still a step toward safer and more efficient regulation. A specific regulation for gatekeepers is a novel approach. Since it has not been done before, no one knows how such a regulation will impact on the platforms, their users, and the wider economy [67]. The DMA can be intended as a asymmetric regulation [60], that targets the source of the problem, namely companies that enjoy an entrenched and durable position as a gateway for business users to reach end users [68].

The DMA also centralizes its enforcement through the Commission. The Commission is given strong investigative and enforcement powers which allow it to investigate, enforce and monitor the rules set out by the DMA. These powers include: assessing gatekeepers' compliance with rules and imposing appropriate measures on them in case of non compliance (Article 7); carrying out market investigations to designate a gatekeeper (Article 15); finding out possible systematic non-compliance (Article 16) or finding out if there are new services that need to be included on the list of core platforms services (Article 17). More importantly, as an outcome of these powers, the Commission is empowered to start proceedings as a result of the inves-

[60] Accordingly the regulation only applies to such companies, which, under the DMA, can be designated quantitatively or qualitatively as gatekeepers.[68]

tigations of non-compliance, etc. In the case of non-compliance with the obligations set out by Articles 5 and 6 (which will be explained below), the Commission could impose fines against a gatekeeper [61].

Articles 5 and 6 of the DMA are really important, as they include a list of 'dos and don'ts' for companies that fall under the scope of the regulation. Those companies must ensure openness of digital services and at the same time prevent unfair conditions on business and users alike [63]. In terms of the "do's": gatekeepers must allow third parties to operate with their services and allow businesses to access data generated in the gatekeeper platform. Regarding the "don'ts": the products or services of gatekeepers cannot be ranked higher than other third parties on their platforms, they cannot prefer business users that use their own ancillary services, they cannot stop users from easily uninstalling preloaded software applications and using third-party applications [63].
As addressed, the DMA considers gatekeepers providers of core services that fulfill the established quantitative and qualitative criteria. On the other hand, the DSA's focus is on the providers of internet services of different sizes and services. This does not mean that a service provider could not be subjected to the obligations of the DSA and the DMA at the same time. A very large online platform (which has more than 45 million recipients) may also be designated as a gatekeeper if it provides one of the core platform services specified in the DMA [66].

One characteristic of this regulation is that it introduces data sharing requirements to mitigate and reduce gatekeepers' exclusive control over the data that they collect. These obligations seek to eliminate market distortions inside the platform, including self-preferencing and information asymmetries between the platform and its business users, as well as distortions between competing platforms. Many aspects need to be clarified on this topic, as many criticisms have arisen even taking into consideration the GDPR [62].

[61] Due to the implementation of the DMA, the European Commission gains the authority to conduct market investigations and impose penalties on gatekeepers who engage in non-compliant behavior. In the event that a gatekeeper neglects its obligations or violates specific actions, it may face fines of up to 10% of its global revenue. For repeat offenders, the penalty can increase to 20%. Furthermore, if a gatekeeper demonstrates a pattern of systematic failure (occurring at least three times within an eight-year period), the Commission reserves the right to initiate a market investigation and enforce behavioral or structural remedies alongside the penalties.[63]

[62] The fundamental principles of the GDPR, such as transparency, data limitation, minimization, storage limitation, and integrity and confidentiality, pose challenges to the data-sharing obligations that may be required by the DSA and the DMA. Furthermore, the principles of purpose-limitation, data-minimization, and storage-limitation within the GDPR may potentially undermine the competitive value of data sharing.

Another critique stressed out by the European Parliamentary Research Service is that *" 'contestability' and 'fairness' are largely left undefined in the draft text, leaving the Commission and other regulators significant room to adjudicate what is 'fair' in commercial disputes, re-write agreements with suppliers, and protect favoured industries.[66]"*.Another one is that *"Some competition experts asked for more flexibility when it comes to imposing obligations on gatekeepers. They argued for a very limited black list (Article 5) of prohibited behaviours (with detailed obligations) and a grey list (Article 6) containing obligations that are more generally drafted and based on well-established theories of harm under competition law"[66].*

According to the European Commission, the DMA brings significant benefits to both business users and individuals. Smaller entrepreneurs and start-ups will have the opportunity to operate in a fairer environment, no longer solely reliant on gatekeepers to provide their services. This shift allows for increased innovation without the burden of unfair terms and conditions. For users, the DMA means a greater range of options to choose from and the ability to have greater control over the services they prefer. It will also be easier for users to explore alternative options beyond the confines of specific online platforms, leading to fairer competition and more competitive pricing, which in turn will stimulate the market [68].

Implementing a data-sharing scheme would not only involve innovation costs but also incur expenses related to operationalizing the process. To enable effective data sharing, new infrastructure would need to be established, including the development of agreements on standardized data formatting. These changes could introduce cybersecurity challenges since a significant amount of valuable user and business data would be consolidated and accessible to various entities.[66]

4 DATA SUBJECT & ORGANIZATIONS

In this section, the perspectives of the two main players in this new digital era will be examined: consumers and organizations. The implementation of these new regulations will have consequences for both parties involved. There are many uncertainties due to these changes, but there are also potential benefits that could arise from them. All three regulations under analysis, namely GDPR, DSA, and DMA, share the common objective of seeking balance and safeguarding all stakeholders in the digital market. Finding a middle ground is therefore crucial, addressing the needs of data subjects for control and protection of their data while enabling organizations to adapt to these new models, striving to maintain competitiveness for achieving international development and innovation.

4.1 Rights of the data subject from the GDPR implementation

One of the main goals of the GDPR is precisely to protect the data subject, in fact it provides tools that can give them more power and control regarding the processing of personal data. The regulation has a chapter dedicated to the rights of the data subject which will be listed and explained below. It is important to list and explain these rights, as many times, an ordinary consumer is not aware of their rights or has no idea how their data is processed and transferred.

Article 12 of GDPR generally gives several rules, in order to facilitate the exercise of those rights by data subjects and controllers. The rights that will be discussed below are the right to be informed, right of access, right to rectification, right to be forgotten, right to restriction of processing, right to data portability, right to object and the right to obtain human intervention (Article 22: Automated individual decision-making, including profiling).

Pursuant to Article 12 of the GDPR, the controller is obligated to communicate about the exercise of the rights of the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and understandable language. Those information given to the data subject should be given in a way to increase the transparency of data and processing activities for individuals, and also allows them to effectively exercise their rights. Any communication with the data subject must be governed by the principle of transparency [32]. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means (if requested by the data subject the information can even be transferred orally). Organizations must follow the principles of the GDPR when communicating with data subjects, including providing means for electronic requests, especially when personal data is processed by electronic means. These organizational requirements are crucial for data subjects to receive comprehensive information on how their data is being processed, which is essential for them to exercise their rights under the GDPR. To increase transparency and comprehensibility for the data subject, different requirements apply to the manner of providing information. Adhering to these principles promotes a more accountable and transparent approach to data processing, strengthening individuals' trust in the use of their personal data[32]. A controller is obligated to facilitate the exercise of the rights of the data subject, he must provide mechanisms that allow data subjects to exercise their rights more easily. This is an upgrade with regard to the Data Protection Directive [63], since the latter does not contain an obligation to facilitate the exercise of the rights of the data subject.

Time frames within which the request must be fulfilled are pronounced in the article, where the controller shall provide the information without undue delay and in any event within one month when receiving the request. However, that period may be extended by two further months where necessary, taking into account the complexity and number of the request (Article 12(3)). In this article the power of control of the data subject's data is enhanced, since the controller is actively forced to enable the data subject to exercise their rights. However, P.T.J. Wolters argues that the real effect of this obligation depends on its interpretation, since the article does not describe any concrete measures[35] [64].

The information should be provided according to two principles. Conciseness requires the information to be correct and comprehensive regarding its content. However, as it shall be presented in an intelligible and easily accessible form, unnecessary information should be avoided; accessibility requires an adaptation of the information to the specific needs of the data subjects in question. However, the level of adaptation should be limited by the practical efforts required in the specific case [32]. The means of communication do not provide specific requirements, however it must be made available to the data subject in this context in an easily accessible

[63] In comparison, the Data Protection Directive (which was in effect prior to the GDPR) also includes provisions regarding data subjects' rights. However, these rights were not as extensive or well-defined as those outlined in the GDPR. The Directive required member states to establish data protection laws that granted individuals certain rights, such as the right of access and the right to rectification. The Directive did not provide the same level of detail or specify the specific requirements for facilitating the exercise of these rights as comprehensively as the GDPR does.

[64] He says "Article 12(2) of the GDPR strengthens the control by the data subjects. It forces the controller to actively enable the data subject to exercise their rights. However, the real effect of this obligation depends on its interpretation. After all, Article 12(2) does not prescribe any concrete measures." [35]

form. The controller cannot refuse to act on the request of the data subject, unless the controller demonstrates that it is not in a position to identify the data subject (Article 12(2)) and may request the provision of additional information necessary to confirm the identity of the data subject (Article 12(6)). Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge [65] (Article 12(5)) and the information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing (Article 12(7)). This might be helpful for making important information easily recognisable. However, the sole use of icons for providing information is unlawful [66], moreover the commission shall be empowered to adopt delegated acts for the purpose of determining the information to be presented by the icons the procedures in giving those (Article 12(8)). The scope of Article 13 is to create a balance of information between the controller and the data subject. Indeed when the controller collects personal data from the data subject, he shall give, at the time the personal data are obtained, the following information to the data subject:

- Identity and contact details of the controller and, where applicable, the controller's representative;
- Contact details of the data protection officer;
- The purposes and legal basis of the processing of personal data;
- The legitimate interests pursued by the controller or y a third party;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, the controller's intention to transfer the personal data to a third country and the intended safeguards for such transfer.

The second paragraph of Article 13 has as objective the insurance of giving to the data subject fair and transparent processing, in fact the controller must give also information about:

[65] The provision "shall be provided free of charge" ensures that individuals can exercise these rights and receive the associated information and actions without incurring any monetary costs. It emphasizes that organizations should not charge individuals for fulfilling their data protection rights and obligations under these articles of the GDPR.

[66] It implies that organizations cannot solely rely on visual symbols without accompanying text or additional explanatory information to fulfill their obligations of providing information to data subjects under the GDPR.

- The period for which the personal data will be stored;
- The existence of the right to access, rectification, erasure of personal data as well as restriction of processing and the right of data portability;
- Information on the right to withdraw consent where processing is based on the data subject's consent;
- The right to lodge a complaint with the Supervisory Authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling.[32]

The provision of additional information is necessary to create a balance of information between the controller and the data subject. Given the typical imbalance [67]of information between these parties, providing additional information is necessary and must be carried out. This additional information empowers data subjects by providing them with a better understanding of how their personal data is being processed and by whom, allowing them to make informed decisions about how their personal information is used. By promoting a more balanced and informed approach to data processing, organizations can foster greater trust and transparency with data subjects, strengthening their relationship and compliance with the GDPR.

4.1.1 Right of access by the data subject (Article 15)

The content of the article goes beyond giving the data subject general information [68] on processing activities, instead it gives the possibility to demand more in-depth information on processing in order to guarantee further lawfulness of processing. The scope of this right is to increase fairness and transparency of data processing, since it gives the data subject the opportunity to verify the lawfulness of processing activities performed on their personal data and enforce their position on their data.

[67] "The rights are aimed at improving the control by and the position of the data subject. However, this disadvantaged position can prevent him from effectively exercising his rights. For example, a data subject will not benefit from his right of access if he does not know the parties that might process his personal data or if he cannot value the provided information." (Wolters, 2018) [35]

[68] Pursuant to Article 12(1), this information should be presented in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

The right of access [69] is organized in two steps. In a first step, the data subject has the right to obtain confirmation from the controller as to whether or not its personal data is being processed (Article 15(1)). If such processing happens, in a second step, the data subject can have access to its personal data being processed and the following information:

- The purpose of processing;
- The categories of personal data concerned;
- The recipients to whom the data has been or will be disclosed, in particular recipients in third countries or international organizations;
- The period of storage or the criteria used to determine that period;
- The existence of the data subject's rights to deletion, rectification, restriction of processing or the right to object;
- The right to lodge a complaint with the Supervisory Authority;
- Where the personal data is not collected from the data subject, any available information as to its source;
- The existence of automated decision-making and meaningful information about the logic involved and the envisaged consequences of such processing;
- Where personal data is transferred to third countries, information on the safeguards taken for such transfer.

The appropriate reaction of the controller to a request of the data subject will depend on the specific request in question [32]. The controller shall provide a copy of the personal data undergoing processing, to guarantee to the data subject access to their personal data and the first copy shall be provided to the data subject free of charge (Article 15(3)). The request for access can be done also by electronic means and the request should be provided in the electronic form, or the data subject can request otherwise. Where possible, the controller could give the data subject remote access to a secure system (web interfaces) that would provide it with direct access to its personal data. Since the object of the request is personal data, it is important to verify the identity of whoever is requesting access, in order to prevent abuse. Thus

[69] The right of access is also granted by Article 12(a) of the Data Protection Directive. However, a controller is obligated to provide more information under the GDPR.[35]

the controller should use all reasonable measures to carry out such verification, in particular in the context of online services and online identifiers [32].

4.1.2 Right to rectification (Article 16)

The objective of this right [70] is to correct or prevent negative effects on the rights and freedoms of the data subject. It is correlated with the principle of accuracy, according to which processed data, at any given time, should reflect reality. The data subject is responsible for demonstrating the inaccuracy or incompleteness of their personal data, and they should attach supporting documentation to their request. By doing so, data subjects can strengthen their case for the correction or erasure of their personal data, promoting a more efficient and effective process for exercising their GDPR rights.

To specify, inaccuracy exists where personal data do not reflect reality so that the information they disclose is untrue. The exercise of the right shall guarantee to have incomplete personal data completed [71].

The data subject can exercise this right for their personal data, but the article does not guarantee the same right to personal data of a third party. This might be a limitation of the right, where personal data do not only refer to the data subject but also to others, like the relationship with other individuals.

The rectification should happen without undue delay.

4.1.3 Right to erasure (Article 17)

The right to erasure, or the right to be forgotten, was brought to a greater attention of the public and of the legislator by the Court of Justice of the European Union's Google Spain decision and has now been strengthened in the GDPR. Pursuant to the article, the data subject has the right to demand from the controller the erasure of its personal data when:

- The personal data is no longer necessary in relation to the purposes for which they were processed. However, in case the data concerned is necessary for realizing another purpose of processing that partially overlaps with or is compatible with the eliminated purpose, erasure does not need to take place.

[70] The right to rectification is also granted by Article 12(b) and (c) of the Data Protection Directive.

[71] Article 19 obligates the controller to communicate the rectification or completion24 to the recipients to whom the personal data have been disclosed. This duty does not apply if the communication is impossible or would involve disproportionate effort.

- The data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;
- The data subject objects to the processing and there are no overriding legitimate grounds for processing;
- The personal data have been unlawfully processed;
- The personal data have to be erased for compliance with a legal obligation under EU or EU Member State Law to which the controller is subject;
- The personal data have been collected based on a child's consent in relation to the offer of information security services. This corresponds to the fact that a child might not be fully aware of the risks involved by data processing and later wants to remove such personal data, especially on the Internet[32].

According to the principle of accountability, the data controller [72] must be able to prove at any time that there is only one legal basis for processing the data, otherwise the processing must be stopped. The GDPR defines exceptions to the right to be forgotten, including cases where the processing of personal data is necessary to:

- The exercise of the right to freedom of expression and information;
- The performance of a legal obligation requiring the processing provided for by Union or Member State law to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- Reasons of public interest in the field of public health;
- archiving purposes in the public interest, scientific or historical research or statistical purposes;
- The establishment, exercise or defense of a legal claim.

The CJEU affirmed the importance of the right to erasure to ensure a high level of data protection, in fact this right improves the protection of the data subjects' privacy, especially when it comes to online publications of their personal data. In order to guarantee this right, the controller must have all the technical requirements

[72] Furthermore, Article 19 of the GDPR imposes a duty on the controller to communicate the erasure to the recipients to whom the personal data have been disclosed.

and should be able to adapt the most efficient measures to satisfy the request of the data subject.

One thing that is unclear about this right is the geographical scope: it is vague whether data stored on servers located outside the EU are affected by this obligation or whether it violates the erasure obligation if the data can still be accessed on websites that are targeted towards users located outside the EU [32].

4.1.4 Right to restriction of processing(Article (18)

This right has the objective to balance at the same time the interest of the data subject and the controller: the latter can continue processing the personal data, while the data subject's security is increased by allowing rectification or erasure of their data [32]. The first paragraph of the article provides four grounds that can establish the restriction of processing:

1. The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
2. The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
3. 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;
4. The data subject has objected to processing pursuant pending the verification whether the legitimate grounds of the controller override those of the data subject.

The restriction [73] of processing does not relate to the storage of the concerned personal data and where processing has been restricted, the concerned personal data may only be processed: with the data subject's consent; for the establishment, exercise or defense of legal claims; for the protection of the rights of another individual or legal person; or for reasons of important public interest of the EU/an EU Member State [32].

The controller must communicate [74]any rectification or erasure of personal data

[73] Article 12(b) and (c) of the Data Protection Directive also grants the right to "block" the data if the processing does not comply with the Data Protection Directive. The right to restriction of processing under the GDPR has a slightly broader scope.[35]

[74] Again, Article 19 of the GDPR imposes a duty on the controller to communicate the restriction to the recipients to whom the personal data have been disclosed.

or restriction of processing to each of the recipients to whom the personal data have been transmitted, unless this proves impossible or disproportionate. If the data subject requests information concerning those recipients, the controller must provide him with that information.

4.1.5 Right to data portability (Article 20)

This article introduces a new data subject right, whose objective is to strengthen the data subject's control over its data where processing is carried out by automated means, by giving it the possibility to transmit its personal data from one controller to another.

When the processing is carried out by automated means, any decision is made without any human involvement.

Data subjects have the right to data portability in situations where personal data they have provided to a data controller are processed by automated means on the basis of consent or where the processing of personal data is necessary for the performance of a contract and the data are processed by automated means. This means that this right does not apply if the processing of personal data is based on a legal ground other than consent or contract and if it is applicable, data subjects have the right to obtain the direct transmission of their personal data from one controller to another, if technically feasible. The article recollects four main elements:

1. The right to data portability 'aims to promote users' freedom of choice, their control over processing and their rights', with the objective of granting data subjects control over their personal data;

2. The right of data subjects to receive their personal data processed by the controller in a structured [75], commonly used [76], machine-readable and interoperable format;

3. The right to transmit personal data from one controller to another without hindrance where this is technically possible;

4. The exercise of the right to data portability does not affect any of the other rights; the same is true for all other rights recognised by the GDPR.

[75] "Structured" means that the personal data fit in a data model that can be used to define and interpret the data.[35]

[76] Wolters adds "The format should also be "commonly used". However, this does not obligate the controller to use a specific format. For this reason, the right to data portability does not guarantee that the recipient can actually use the data. This is only possible if the computer systems of the controller and the recipient are interoperable.[35]

The applicability of this right will enable data subject to switch service providers with ease, promoting greater economic flexibility and consumer empowerment. This right allows data subjects to move, copy, or transmit their personal data between different IT environments, making it easier to switch between providers. By promoting greater competition among service providers, the right to data portability can also stimulate the development of privacy-friendly technologies and interoperable data formats. As a result, this right helps to promote innovation in the field of data processing and can benefit both consumers and businesses alike. Overall, the right to data portability is an important aspect of the GDPR that helps to protect the rights of data subjects and foster a more competitive and innovative marketplace for data services [32].

4.1.6 Right to object (Article 21)

Pursuant to Article 21, data subjects may assert their right to object to the processing of personal data on grounds relating to their particular situation and to the processing of data for direct marketing purposes. The article [77] provides three situations that can be grounds for an objection to processing. The data subject can exercise this right at any time to processing which is based on prevailing legitimate interests of the controller/a third party; or is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, including profiling based on those legal permissions (Article 21(1)).
Pursuant to the second paragraph of the article, where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of its personal data for such marketing, which includes profiling, to the extent that the latter is related to such direct marketing (Article 21(2)).
Direct marketing includes text messages and emails that a customer receives from a product or service provider. The activities of direct marketing may include different steps such as collecting personal data from potential customers, creating profiles about those potential customers and their preferences, and then sending personalized communications to them. As a general rule for direct marketing, the company needs a consent from a customer.

[77] Wolters adds:"The right to object is also granted by Article 14 of the Data Protection Directive. This article does not make an explicit exception for the situation that the controller demonstrates compelling legitimate grounds for the processing that override the interests of the data subject. However, it does require that the data subject bases his objection on compelling legitimate grounds relating to his particular situation. Furthermore, the controller is only obligated to stop processing the data if the objection is "justified". Finally, Article 14 does not create a right to object to the processing for scientific or historical research purposes or statistical purposes." [35]

Pursuant to Article 21 paragraph 6, where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest. Under the GDPR, 'statistical purposes' means processing of personal data that is necessary for statistical surveys or for the production of statistical results that may further be used for different purposes. The controller will be obliged to prove such necessity [32].

Overall there are some general points and ground rules that must be applied to every right listed in the GDPR. Where the right is exercised, the controller should act without undue delay and within a month of the right being exercised; the period can be extended up to two months where necessary, but it is necessary to give notice to the data subject.
Any communication to the data subject must be done in a clear, concise and intelligible way and where a request is made electronically, information should be provided in the same manner where possible.
Any action should usually be taken free of charge. However, the controller is entitled either to charge a reasonable fee or refuse to act on a request where it is clearly unfounded or excessive (particularly if it is repetitive). In such a case, the burden will be on the latter to show that this is the case if, for example, the data subject complains to the supervisory authority.
The data subject must be notified of the possibility to complain to the supervisory authority or to take the matter to the court.
EU or national law may create further restrictions on the rights of data subjects on a number of public interest grounds.

4.2 Privacy Paradox

Despite the fact that the GDPR provides data subject the ability to have control over their data, or at least to verify their integrity and how it is processed, for the common issue of the invasion of privacy to be resolved, input is needed from all sides. When it comes to data, sensitive and otherwise, people often do not understand the value that this data has, particularly for companies that use it to target their campaigns, and they tend to "give it away" freely without worrying about the implications. In this era, each and every movement is monitored and tracked, exploited to achieve goals, and unfortunately, there is a general ignorance and lack of information among the common people. No one wants their most intimate and private information to be revealed, but at the same time there is often no effort made to ensure that this does not happen, quite the contrary. The contradiction between individual's stated concerns about privacy and their actual behaviors when it comes to sharing information online is a phenomenon known as the "Privacy Paradox". On the one hand, people express a desire for privacy and express concerns about data breaches and identity theft. On the other hand, they continue to engage in behaviors that compromise their privacy, such as sharing personal information on social media platforms and using weak passwords. Studies have been focused on comparing the constructs of privacy concerns and privacy attitudes, since they may seem closely related but are fundamentally different.Privacy concerns could be quite generic and, in most cases, are not bound to any specific context, whilst privacy attitudes refer to the appraisal of specific privacy behaviors.[36]

Although users are aware of privacy risks on the internet, they tend to share private information in exchange for retail value and personalized services.[37]. The earliest study of this theory (2001) highlighted that individuals expressed their concern about privacy being violated, yet they were still willing to give their personal details to online services as long as they had something to gain in return. Acquisti [78] claims that *"people may not be able to act as economically rational agents when it comes to personal privacy."* He argues that privacy-related decisions are affected by incomplete information, bounded rationality and psychological biases, such as confirmation bias, hyperbolic discounting and others.[36]

Different theories have been formulated as to why this behavior takes place. One of them is the Privacy Calculus [79], that suggest that consumers weight the risks associated with the loss of privacy and compare them to the benefits that they could gain[38]. In this perspective, privacy is seen as a commodity, whose value can be quantified[39].

A context-based perspective instead suggests that privacy concerns are situational, which makes them weak predictors of behavior [40]. In one study, consumers were

[78] In his paper, Kokolakis explains the arguments and the model proposed by Acquisti, writing that: "Acquisti built an economic model that partly explains privacy attitude – behaviour inconsistencies. This model incorporates the immediate gratification bias. Immediate gratification refers to the tendency to value present benefits more than future risks. Thus, in individuals' assessment, the present benefits of information disclosure outweigh the future privacy risks. Furthermore, he argued that sophisticated privacy advocates might realise that protecting themselves from any possible privacy intrusion is unrealistic. Thus, they might not be willing to adopt a strict privacy protection strategy, since they doubt it will eventually pay-off". [36]

[79] It is worth noting that while the Privacy Calculus provides a useful framework for understanding how individuals make privacy-related decisions, it does not capture the full complexity of privacy concerns and motivations. People's attitudes towards privacy can be influenced by cultural, social, and ethical factors that go beyond a simple cost-benefit analysis.

more likely to purchase products from Web sites that offered more privacy, even if the sites charged higher prices [41].

Consumers are subjected to thousands of stimuli every time they open their PC or smartphone. They are overwhelmed by requests for consent to collect data, and most of the time they don't even know what data they are providing while clicking a particular button. On the other hand, many people are trying to raise awareness of this problem, and often, as seen in studies, general laziness overwhelms the security of one's data. To solve this problem, there must be a commitment from consumers to understand the importance of these situations, as the drafting of regulations to protect data subjects would be useless if they do not believe in the value of their own information. Companies also have a significant job to do because they must allow consumers to understand what they are providing without trying to obtain their data through subterfuge, as unfortunately often happens.

4.3 Evaluating the Effects of DSA on User Rights and Protection

The DSA brings several changes for online platforms, but which can give benefits not only to online platforms, but also to the users themselves, as their protection and the protection of their rights is increased. These rules will in fact create a safer online experience for citizens to freely express their ideas, communicate and shop online, by reducing their exposure to illegal activities and dangerous goods and ensuring the protection of fundamental rights. These benefits include better services for consumers: online marketplaces will need to identify their business users and provide clear information regarding the sellers of products or services. This measure is useful to identify and combat fraudulent traders while safeguarding online shoppers from illegal and counterfeit products. Furthermore, online marketplaces will be obligated to inform consumers who purchased a product or service when they become aware of the illegality [80]of such products or services, about a) the illegality, b) the identity of the trader and c) any relevant means of redress [81] [64]. Regular checks on product documentation will be conducted by the marketplaces to ensure compliance, while an increasing reliance on advanced product traceability solutions will be encouraged

[80] Furthermore, the DSA will foster a co-regulatory framework for online harms, including codes of conduct such as a revised Code of Practice on disinformation, and crisis protocols.[64]

[81] If the marketplace becomes aware that a product or service is illegal, they must inform the consumer about the illegality, provide them with the identity of the trader who sold the product or service, and inform them about any relevant means of redress.

to minimize the availability of non-compliant goods to European consumers.

The introduction of this regulation grants users the acquisition of new rights, while also increasing their power of control. They will in fact be able to be a participant in the notification of illegal content and be informed the moment their content is removed, which decision they can challenge. Pursuant to Article 14 (Notice and action mechanisms), *"Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content."* To that end, the providers shall take the necessary measures to enable and facilitate the submission of notices containing the reasons, the location and a statement declaring the good faith of the action. Platforms are obliged to notify them of any decision taken, of the reason to take that decision and to provide for a mechanism to contest the decision [64]. Therefore transparency towards users will increase, allowed by a continuous exchange of information [82]. Users will also receive more information about ads they are seeing on online platforms, increasing the transparency of online advertising. For very large platforms, users and consumers will be able to have a better understanding of the ways these platforms impact our societies and will be obliged to mitigate those risks, including as regards freedom of expression [64]. Platforms will be prohibited from displaying behaviorally targeted advertisements to minors and from using profiling techniques that rely on special categories of personal data, such as ethnicity, political views, or sexual orientation, to present ads to their users. This measure aims to safeguard the privacy and protect the interests of individuals, particularly minors, by preventing the use of sensitive personal information for targeted advertising purposes [64]. In the event of a provider of intermediary services violating the DSA, users will have the right to seek compensation for any damages or losses they have incurred as a result of the infringement. Pursuant to Article 43 (Right to lodge a complaint) *"Recipients of the service shall have the right to lodge a complaint against providers of intermediary services alleging an infringement of this Regulation [...]"*. This provision ensures that users have recourse and can hold providers accountable for any harm they may have suffered due to non-compliance with the DSA regulations.

[82] The Digital Services Act will foster a co-regulatory framework, together with the updated Code of Practice on Disinformation and the new Commission Guidance, as announced in the European Democracy Action Plan. [64]

4.4 Assessing the impact of DMA on User Experience and Privacy

As the DMA proposal mentions, its scope is rather broad, dealing with practices generally "unfair" to the consumer. A report from the European Parliamentary Research Service stresses what said before about the influence of those gatekeepers: *"Businesses are increasingly dependent on these gatekeepers, which in many cases leads to gross imbalances in bargaining power and therefore results in unfair practices being imposed on business users, and small and medium-sized enterprises (SMEs) relying on the platforms to reach their customers[66]"*. A wide range of such practices have been identified: the imposition of anti-steering provisions (such as preventing business users from directing their customers to alternative offers other than the ones provided by the platform); lock-in strategies (such as imposition of identification services by the platform); self-preferencing practices (like favoring own products and services); mechanisms to limit or refuse access to data collected by gatekeepers and limit access or interoperability.

Several obligations for gatekeepers are listed in Article 5, regarding the collection and combination of personal data according to the users' consent. In particular, the second paragraph of the article imposes gatekeepers to not combine personal data collected from the relevant core platform service with personal data from any other services they offer though the core platform without the user's consent or outside of the core platform or with personal data from third parties. Additionally, a gatekeeper must not cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including core platform services and vice-versa, and must not, without the user's consent, sign in users to other services of the gatekeepers in order to combine personal data. The intention of the legislator was to limit a broad form of consent known as "single button consent" [83]. This type of consent would allow companies that control access to online platforms to merge user data collected from various services they offer, as well as data obtained from third parties through methods like cookies. As a result of the regulation, users of these platforms should have the freedom to decide whether

[83] The report from EIPA also introduces the concept of "consent fatigue", saying that " In the digital era, consent has become so tedious for individuals there is no guarantee that such consent is informed and represents an unambiguous indication of the user's wishes. In order to understand to what they are consenting, individuals must read the privacy policy. This has proved particularly difficult due to the lengthy and complex texts, but also due to the extreme pace of the digital era. The concept of 'consent fatigue' has influenced many data protection professionals to avoid using consent as a lawful basis as much as possible. " [63]

or not they want to participate in these business practices. However, this can only happen if individuals are provided with clear and explicit information about these practices and they explicitly agree to the collection and processing of their personal data [63].

However, a report from the European Institution of Public Administration (EIPA) argued that there are some concerns regarding Article 5(2) and its implication on the GDPR's purpose limitation principle. It was argued that *" the singular reference in 5(2)(a) to "process, for the purpose of providing online advertising services" implies that online advertising is based on a single data processing purpose, whilst realistically more than one processing activity takes place when a user is targeted with ads."* Therefore, this singular reference may not accurately reflect the complexity of data processing involved in online advertising. They also added that *"sub-paragraph 2 would create a loophole for gatekeepers and could still rely on an all-encompassing, single button consent, overriding the requirements within Article 6 GDPR to clearly identify and convey the purpose and legal basis for each processing activity from the controller to the user"*. The solution proposed is *"to remove this flaw from the text by adding the wording 'specific processing activities' so the text would read as follows: "unless the end user has been given a clear request for each processing purpose that states the specific processing purpose, and the sources of the data, and the result of the combination or cross-use of the personal data, in line with the requirements"*.

The EPRS states that DMA also seems to have a broader scope than the GDPR's right to data portability and would ensure additional forms of portability, including portability of non-personal data for business users and real-time and continuous portability. However, the implementation of data portability runs into a number of technical, legal and economic obstacles (like loss of context once data assets are ported from the original platform, need to obtain consent from natural persons to port personal data) [66]. Indeed the DMA requires gatekeepers to provide an end user and/or business user with access to data provided by the user; companies should comply with this obligation "in line with" the GDPR. Apostle et al. claim that *"Data subjects infrequently exercise the right to data portability under the GDPR, and it has not been subject to significant enforcement by data protection authorities"* [69] [84]. The clarification of this right can bring benefits for both data

[84] Apostole et. al claim that: "It remains to be seen how satisfaction of the portability obligation in relation to business users will align with the GDPR-imposed data subject right. Perhaps this obligation

subjects and businesses: on one side, the enforcement of the self-determination of the data subject has to be addressed, allowing him the possibility to decide who has and there his personal data are; on the other side, there is the reduction of transaction costs for users of changing platforms, enhancing the competition between companies.

The EPRS's opinion about the impact on customers and end-users: *"A report from the Centre for European Reform warned that although the DMA's approach of setting a single set of rules for a diverse set of companies is understandable, this approach risks unintended consequences. They called on EU lawmakers to empower the Commission with more flexibility to exempt tech firms from the rules in some cases and protect innovation. In the same vein, other experts argued that restricting collection or aggregation of user data could impair the viability of ad-funded platforms and have a significant potential to harm consumers."* [66]

4.5 Opportunities and Challenges of DSA compliance by organizations

The DSA is a regulation that will bring several benefits to all organizations, ensured by a more modern, clear and transparent framework, assuring that the rights are respected and the obligations are enforced [64].

The DSA aims at regulating the activities of intermediary services, and three different services are identified: a mere conduit service *"that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network"* (Article 3), a catching service *"that consists of the transmission in a communication network of information provided by a recipient of the service, the service provider shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request"* (Article 4), and a hosting service *"that consists of the storage of information provided by, and at the request of, a recipient of the service"* (Article 5) [70].

will also cover personal data of end users relevant to a business user, and business users will become "joint controllers" of personal data disclosed under the DMA's portability obligation, requiring a separate agreement with the gatekeeper.In addition, it is unclear how this portability requirement will interact with the data disclosure obligation set out in the DMA. The obligation of "portability" requires the disclosure of data in a format that is reusable and thus is not the same as mere "access," but both must be provided on a continuous and real-time basis."[69]

The DSA imposes certain key obligations [85] applicable to all intermediary services. The key areas for consideration are: transparency reporting, appointment of points of contact and legal representatives, updates to terms and conditions, content moderation policies and takedown orders and additional cumulative obligations for very large online platforms (VLOPs) and providers of hosting services and online platforms [70].
Regarding the principle of transparency, under Article 15, all providers are required to make publicly available annual reports on content moderation that they are engaged in. These reports must include information about the moderation initiative, including information relating to illegal content, use of automated tools, training measures, and complaints received under complaints-handling systems [70]; for VLOPs (very Large Online Platforms) only such reports must be published every six months under Article 42. In order to comply with the DSA as it becomes effective, providers need to evaluate whether their content moderation dashboards enable them to extract and report [86] the necessary information in an effective and efficient manner.

According to a report published by Latham Watkins, *"All providers are required to establish two points of contact: (i) under Article 11 for communication with the EU Member State Authorities, the Commission, and the European Board for Digital Services (the Board); and (ii) under Article 12 for rapid and direct communication with the recipients of their services. Under Article 13, providers not established in the EU but which provide services into the EU must designate a legal representative in an EU Member State in which it offers its services for the receipt of, compliance with, and enforcement of decisions issued under the DSA. Notably, such legal representatives can be held liable for non-compliance with the DSA, without prejudice to the liability that could be initiated against the provider."* [70].

Pursuant to Article 14, all providers must ensure that their terms of service use clear, plain, intelligible, user-friendly, and unambiguous language. Furthermore, these terms and conditions must be available in an easily accessible and machine-readable format. Providers are also obligated to inform the recipients of their services

[85] "In relation to the liability of intermediary service providers for content transmitted or hosted on their services, the DSA maintains the existing exemptions from liability or "safe harbours" under the e-Commerce Directive."[70]

[86] Designated online platforms and online search engines were required to publish their first transparency reports by 17 February 2023, and will be obliged to continue to do so once every six months thereafter.[70]

of any significant changes to such terms and conditions. To facilitate compliance with the DSA as a whole, providers should consider whether their terms and conditions need to be updated to reflect or to facilitate other applicable obligations arising under the DSA (e.g., their transparency or content moderation obligations) [70].

The majority of obligations concerning content moderation primarily applies to hosting services, online platforms, and very large online platforms. Nonetheless, according to Article 14(4), all intermediary service providers must ensure that any limitations imposed on content moderation should have due regard to the rights and legitimate interests of all parties. Furthermore, as stated in Articles 9 and 10, all intermediary services are required to comply with information orders and takedown orders from regulators and judicial authorities [70].

In addition to the obligations above, the DSA imposes further cumulative obligations on providers of hosting services.

Under Article 16, providers of hosting services are required to, in relation to the Article 15 transparency reporting obligations discussed above, implement mechanisms to allow recipients of their services to notify them of the presence of allegedly illegal content [70]. Under Article 17, providers of hosting services must include a statement of reasons to the affected users, with the decision taken, circumstances, information about the use of automated means and others. To prepare for the DSA coming into force, providers should appraise their notice and action mechanisms to ensure they meet the standards set under the DSA, and allow for sufficiently detailed and complex notices to be submitted, reviewed, judged, and transparently decided upon [70]. Under Article 18, providers of hosting services are obligated to inform the national law enforcement or judicial authorities of the relevant EU Member State of any information that gives rise to suspicions of criminal offenses involving a threat to the life or safety of persons [70].

In addition to the obligations listed above, providers of online platforms are subject to a number of additional cumulative obligations, as stated in Section 3 of the regulation; these obligations do not, however, apply to online platforms that qualify as micro or small enterprises [87]. Article 20 requires providers of online platforms to maintain an internal complaints-system that enables the recipients of their services to lodge complaints; Under Article 21, providers of online platforms are obligated to inform complainants of their reasoned decision and the options available to them

[87] as defined in Recommendation 2003/361/EC

[70]. Article 22 requires providers of online platforms to prioritize trusted flagger notices. Trusted flaggers are defined as an individual or entity which is considered by a hosting service provider to have particular expertise and responsibilities for the purposes of tackling illegal content online [71]. Under Article 23, providers shall take any measures against abusive notices. Under Article 26, providers of online platforms must supply users with information relating to any online advertisements on its platform so that the recipients of the services can clearly identify that such information constitutes an advertisement. Providers of online platforms are prohibited from presenting targeted advertisements based on profiling using either the personal data of minors or special category data (as defined in the GDPR) [70]. Article 24 imposes additional transparency reporting regarding disputes, suspensions.

Lastly, VLOPs are subject to the most robust obligations in the DSA, in addition to the cumulative obligations applicable to all online platforms as set out above. Under Article 34, they are required to conduct an annual assessment on any systemic risks stemming from the functioning and use of their services and mitigate risks identified in such risk assessment [70]. Under Article 37, they must submit annual independent audits to confirm their compliance with various obligations under the DSA. Under Article 40, they must provide access to data necessary to monitor their compliance with the DSA where requested by the relevant Digital Services Coordinator [70] [88]. Latham & Watkins write that *"To prepare for the DSA coming into force, they should assess whether their content moderation practices are sufficiently transparent and well documented so as to ensure they can meet the reporting standards set under Article 42, which requires them to include in their Article 15 transparency reports s the human resources dedicated to content moderation, the qualifications and linguistic expertise of the persons carrying out the activities, and the indicators of accuracy and related information referred to in such reports."* [70]

[88] According to the Digital Services Act (DSA), each Member State of the European Union is required to designate one or more competent authorities as responsible for the application and enforcement of the DSA. One of these authorities shall be appointed by the Member State as its Digital Services Coordinator1. The Digital Services Coordinator is responsible for supervising the implementation of the DSA within their respective Member State and for cooperating with other Digital Services Coordinators and the European Commission to ensure consistent application of the DSA across the EU [76]

4.6 Adapting to the Implications of DMA for Businesses and Innovation

The DMA requires gatekeepers to comply with a set of obligations and prohibitions within six months of their designation as gatekeepers. The report from European Parliamentary Research Service lists the set of requirements directly applicable to gatekeepers according to Article 5:

- Processing and use of end-users' personal data: prohibits a gatekeeper from processing endusers' personal data using third-party services for online advertising purposes without users' consent, from combining or cross-using personal data across CPS (Core Platform Services) or between CPS and other services without users' consent and from signing-in users to other services without their consent (Article 5(1)) [66].

- Parity clauses: requires a gatekeeper to allow its business users to offer their products or services at different prices or conditions on third-party intermediation services or their online sales channels (Article 5(3)) [66].

- Anti-steering: requires a gatekeeper to allow business users to promote their offers to end-users acquired through its CPS and to allow end-users to access services, content and subscriptions outside its CPS (Article 5(4) and 5(5) [66].

- Raising issues of non-compliance: prohibits a gatekeeper from preventing business users from raising issues of non-compliance with public authorities about its practices (Article 5(6)) [66].

- Tying: prohibits a gatekeeper from requiring business or end-users to use its web browser engine, identification or payment services (Article 5(7)) [66].

- Bundling: prohibits a gatekeeper from requiring business or end-users to subscribe to one of its CPS as a condition to access another of its CPS (Article 5(8)) [66].

- Transparency concerning online advertising practices: requires a gatekeeper to provide advertisers and publishers with transparent pricing and remuneration information regarding online advertising practices (Article 5(9) and 5(10)) [66].

Articles 6 and 7 impose on gatekeepers a list of requirements that may need to be specified,following a dialogue with the gatekeeper,as they potentially apply in different ways:

- Data silo[89]: prohibits a gatekeeper from using not-publicly available data generated by the business users to compete with them (Article 6(2)) [66].
- Uninstalling apps and changing default settings: requires a gatekeeper to allow end-users to easily uninstall apps on its operating system and to change default settings prompting end users towards its operating system, virtual assistant or web browser (Article 6(3)) [66].
- Sideloading: requires a gatekeeper to allow the installation of third-party apps and app stores using its operating system (Article 6(4)) [66].
- Self-preferencing: prohibits a gatekeeper from favouring its own products and services to the detriment to those of third parties (Article 6(5)) [66].
- Switching apps: prohibits a gatekeeper from restricting end-users to using its CPS to switch apps and services (Article 6(6)) [66].
- Interoperability: requires a gatekeeper to allow third-party providers and business users free of charge and effective interoperability to the same hardware and software features accessed or controlled via its operating system or virtual assistant (Article 6(7)) [66].
- Access to online advertisement performance measuring tools: requires a gatekeeper to provide online advertisers and publishers with access to its performance measuring tools (Article 6(8)) [66].
- Data portability: requires a gatekeeper to provide end-users with effective data portability upon their request and allow them real-time access to such data (Article 6(9)).
- Data access: requires a gatekeeper to provide business users with real-time access to data generated in the context of the use of the gatekeeper's CPS and of the users' interaction (Article 6(10))[66].
- Search data access: requires a gatekeeper to provide third-party search engines with access to fair, reasonable, and non-discriminatory (FRAND) terms for ranking, query, click and view data (Article 6(11))[66].

[89] A data silo is a repository of fixed data that remains under the control of one department and is isolated from the rest of an organization. This can result in a lack of transparency and cooperation between departments and can hinder the overall efficiency and effectiveness of an organization. Data silos can arise for a variety of reasons, including organizational structure, technological limitations, and a lack of data integration.

- Access to app stores, search engines and social networking services: requires a gatekeeper to provide fair and non-discriminatory (FRAND) access for business users to its app stores, search engines and social networks (Article 6(12))[66].

- Terminating provision of service: prohibits a gatekeeper from imposing disproportionate conditions for the termination of services (Article 6(13))[66].

- Interpersonal communications services' interoperability: requires a gatekeeper to make its interpersonal communications services interoperable with those of another provider (Article 7(1))[66].

- Basic functionalities' interoperability: requires a gatekeeper to ensure interoperability of the basic functionalities it provides to its own end users (Article 7(2) and 7(4))[66].

Furthermore, gatekeepers are subject to general obligations (Articles 13, 14 and 15):

- Anti-circumvention[90]: requires undertakings providing CPS (including gatekeepers) not to circumvent quantitative thresholds, engage in any behaviour undermining compliance, or alter CPS quality and conditions (Article 13(1), (4) and (6))[66].

- Concentrations: gatekeepers are required to inform the Commission of any intended concentration involving another provider of CPS or other services(Article 14(1))[66].

- Audit: gatekeepers have to submit an audit to the Commission describing customer profiling techniques (Article 15)[66] .

The DMA will affect gatekeepers as well as business users who rely on or use gatekeepers for their own services. In advance of the DMA coming into effect, business users should identify areas of their businesses that the DMA could impact and consider how to engage with large digital platforms to derive the advantages that the DMA could confer.

[90] Anti-circumvention refers to laws that prohibit the circumvention of technological barriers for using a digital good and/or service in a way that the rights-holder doesn't allow. The requirement for anti-circumvention laws was globalized in 1996 with the creation of the World Intellectual Property Organization's Copyright Treaty [77]

4.7 Organizations' compliance with GDPR, Impact and Adaptation

The introduction of the GDPR has compelled companies to restructure their business systems to comply with the imposed standards. It has been noted repeatedly that this era is defined by the emergence of increasingly advanced technologies, and how we humans strive to keep up with them and adjust to living with them. Thus far, we have emphasized the significance of privacy, safeguarding personal data, and the tools available to uphold these principles. Now, we need to shift our focus from the standpoint of individual data subjects to that of organizations.

The concept of privacy and data protection should be a priority for every business, large or small, regardless of industry or geographical location. At present, data has become a pivotal factor in making business decisions, defining and attaining goals. It is extensively utilized in various domains to gain a deeper understanding of customers' characteristics, establish certain strategies, streamline processes, and more. However, like any change, adhering to the GDPR regulation yields benefits for companies, as well as new obstacles to overcome and thus the goal of achieving these goals by adopting new solutions. A research conducted by Peter Lindgren (2016) highlighted that business had to face increasing costs due to more procedures to implement, such as *"more procedures – more value chain functions to be carried out, more technology and software necessary to be bought, more hours spend by HR to live up to the necessary GDPR requests, change in organizational procedures and structures together with implementation of new culture."* [42] In order to be able to demonstrate compliance with the GDPR, the data controller should implement measures, which meet the principles of data protection by design and data protection by default[91]. Pursuant to Article 25 of the GDPR, Privacy by Design and by Default, it is required that data protection measures are designed into the development of business value proposition processes for products, services and processes of product and services. It is the responsibility and liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing are carried out by a data processor on behalf of the controller (Recital 74). While according to Article 35, data protection impact assessments

[91] Data protection by design and by default is a concept that requires data controllers to implement appropriate technical and organizational measures and necessary safeguards to implement the data protection principles set out in Article 5 (1) of the GDPR and to protect the rights and freedoms of data subjects. This means that data protection by design and default must be considered throughout the life cycle of a processing activity: at development, design and at the point of processing [78]

have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities (DPA) is required for high risks[42].

Kiersten E. Todt in "Data Privacy and Protection: What Businesses Should Do" highlighted that one problem is that businesses do not know how to evolve their thinking on security to align with trends in technology and innovation[43]. Their approach to security is often based on traditional, outdated models that focused on physical components. However, in today's world, our economy and threat environment are defined by digital infrastructure and interdependencies, which pose new challenges, including privacy, that demand fresh thinking and innovative solutions. Ensuring robust privacy protection protocols for data is a crucial function for any organization that handles data, especially when sensitive data such as personal information is involved.
According to Kiersten E. Todt, there are three critical elements of a comprehensive business data protection plan:

1. Data inventory[92]. Its objective is to prioritize the business data according to the business mission and sensitivity of data. Organizational efficiency is crucial for businesses to safeguard and secure their data. To achieve this, businesses must conduct an inventory of all their data and prioritize it since it can be challenging and expensive to provide equal protection to all data. Certified contractual agreements should be in place with all third-party vendors, mandating adherence to a baseline of privacy and protection policies that align with the company's policies. [43]

2. Public projection of data privacy and protection policies. Businesses must thoughtfully consider the impact and understanding of their policies by the public, both in terms of how these policies are communicated and how the company engages with the public. For instance, what privacy options are offered on the business website, how much user engagement is present, and

[92] The author lists some critical questions such as "Who can access your data?How are you using your data? Do you know where your data is held along your value chain? Do you track your data appropriately and effectively? What security protocols do your partners, third-party vendors, and product and service providers have in place? Can you consolidate where your data are held? What data can you delete on a regular basis? Do any of your vendors present too much risk? Do you have the proper controls in place? Do these controls reflect your data and asset priorities? What are your consumers/clients asking/demanding of you regarding data privacy and protection? What can (and should) be told to your consumers/clients regarding your data privacy and protection safeguards?"[43]

how diligently are data requests fulfilled. These factors are crucial in ensuring policy effectiveness. Transparency and clarity regarding data usage and protection are imperative in earning the trust and confidence of customers and the public. Greater transparency leads to enhanced awareness, which, in turn, helps businesses better serve their customers. [43]

3. Incident response. In today's threat environment, most businesses have encountered some form of security breach. However, with the implementation of appropriate policies and the execution of a robust business security strategy, a breach does not necessarily indicate failure. Instead, success is often measured not by the incidents prevented but by how efficiently a business responds to an event. [43]. One problem is that many businesses lack the necessary expertise and knowledge in privacy protection and handling, which is compounded by the new requirements on private data protection. Consequently, a majority of the businesses examined had a significant need for education and training on data protection and privacy. However, many of them did not have extra resources to allocate to this critical issue, even though they recognized its importance in meeting the new GDPR demands. [42]

Colin Tankard in "What the GDPR means for business" highlights another problem: the increase of the cost in order to assure compliance with the GDPR. Due to this fact, many are worried about the impact of the regulation. According to the research, 52% of organizations believe that the GDPR will result in fines for their business and 68% feel that it will dramatically increase the costs of doing business in Europe, with some believing that their budgets will need to increase by some 10% to deal with its ramifications over the next two years [44]. Joe Garber adds that *"Becoming GDPR-compliant goes beyond avoiding fines. It means setting up processes and safeguards that enhance customers' trust and avoid business disruption."* [45] The worries about the fines are real, according to the regulation the following sanctions can be imposed: a warning in writing in cases of first and non-intentional non-compliance regular periodic data protection audits a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83(4)); a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83(5)).

One of the fundamental principles that companies must incorporate into their core values is transparency. They must be able to provide clear descriptions of how they collect data, why they do it, and how they intend to store and process it. This also includes providing information about third parties with whom data is shared and for how long.

Additionally, companies must provide more control to users regarding the actions taken on their data, such as by providing a copy of their data. The GDPR empowers users in this regard, allowing them to request the deletion or correction of their data, and to inquire about the specific purposes for which their data is shared with third parties. When data is collected, it rarely remains in one place. If we could visualize the journey data takes from one place to another, we would not be able to see the sun. Therefore, companies must ensure that any third parties involved in the data processing are in compliance with GDPR regulations to prevent violations.

Opinions on this new regulation are varied and divided. Some fear for businesses, especially small and medium-sized ones, due to the possible costs and difficulties in carrying out accurate targeting and segmentation operations with the new restrictions. However, many positives have also been identified.

The main advantage of complying with GDPR is the establishment of trust. By implementing various data security practices and designating a Data Protection Officer (DPO)[93] to ensure data privacy, companies can significantly increase their credibility in the eyes of their users. Adherence to GDPR will serve as a guarantee to users that the company's services will not compromise their privacy in any way. This, in turn, will enhance customer loyalty, resulting in positive brand recognition.

Another significant benefit is the improvement and refinement of decision-making practices. GDPR introduces new factors that require greater consideration and change the perception of risk. In short, the consequences of non-compliance are severe, and the stakes are higher. With increased responsibility and potential punishment, companies will adopt a more calculated and cautious approach to decision-making.

GDPR's greatest achievement is the clarification of key terms regarding the user/company relationship in terms of personal data use. This clarification has resulted in basic definitions of the rights and responsibilities of the involved parties, providing a proper map of what is permitted and prohibited. This, in turn, provides a set of tools to react to a variety of situations.

[93] "The Data Protection Officer (DPO) is a figure introduced by the GDPR to support and control data controllers and processors in preserving data and managing risks according to the principles and guidelines of the European Regulation. The DPO is a technical and legal consultant with executive power. Their role is twofold: they advise and supervise, but also act as a liaison between the organization and the authority"[79]

The adoption of GDPR has had a significant impact on risk assessment[94], making it one of the biggest winners. While it's considered part of standard operations, it often doesn't receive the attention and care it deserves. GDPR changes this by promoting a more thorough and responsible approach to risk assessment. The reason for this is simple: the risk of oversight and underestimation can result in significant monetary and reputational damage for the company. GDPR emphasizes the importance of a well-organized, impenetrable, and highly regulated security framework. Although this should be a reasonable requirement for any company, the prevalence of data breaches proves otherwise. However, GDPR provides clear and realistic guidelines on how to improve the security system and how to maintain it. A combination of regular system audits, monitoring, and a cautious employee culture is the key to effective improvement. [42]

4.8 Web Cookies

The amount of data collected on each individual every day is a tool that is being exploited in many economic and political environments in order to achieve predefined purposes, from advertising, using various forms of targeting, to electoral campaigns, being able to identify voters who are likely to switch or to turn out. The most prevalent technology to enable the collection and resale of individual-level information is based on cookies and related means of recording browsing data [46]. These tools are capable of recording user movements and histories, and organizations collect all this information. With the passage of time, concerns about this new technology, which has been known for just over two decades, have become increasingly acute regarding the security of personal data and the invasion of privacy. Later in the paragraph, definitions of these tools and their uses will be provided, and the different opinions on their potential risks and benefits will be analyzed.

Web cookies were invented in 1994 as a mechanism for enabling state to be maintained between clients and servers. A cookie is defined as *"a text string that is placed on a client browser when it accesses a given server."* [47][95].

Initially, they were not intended to be utilized as the type of surveillance tool they are known for today. Rather, their purpose was to notify the server of a website that

[94] the GDPR requires organizations to conduct various assessments and implement risk management measures to ensure compliance with its data protection principles and requirements. These assessments aim to identify and address potential risks related to the processing of personal data.

[95] The term cookie was derived from the term magic cookie, which is a packet of data a program receives and sends back unchanged, used by Unix programmers.

a user had revisited[96]. By accessing the data stored in the cookie file, the server can identify the user. This technique of monitoring user activity was originally intended to benefit the user, as saving user information could lead to more efficient and personalized visits in the future. Cookie uses have since grown far beyond their original intention and have become a very controversial issue. Users believe that their privacy is being violated, with the progression of cookie functions moving beyond basic user customization and personalization [48].
Cookies allow websites to store information on a user's machine and later retrieve it. Each cookie has several attributes:

- Name. The name attribute is the name given to a cookie sent by a particular server. This uniquely identifies cookies to a particular server. [47]

- Value. The value attribute contains the data the cookie is responsible for transmitting between the client and server. Value data may be clear text, but is generally encrypted, or obfuscated for security and privacy reasons [47]. It contains the information the server wants to save on the user's hard drive.

- Host. The host attribute identifies the cookie's origin server. This allows a browser to send cookies back to the proper server during subsequent communication. It also distinguishes 1st and 3rd party cookies [47].

- Path. The path attribute restricts when a browser sends a cookie back to a host. The value in the path attribute must exist in the URL of the website being requested by the browser [47]. It is potentially the most useful of the cookie settings because it sets the URL path the cookie is valid within and pages outside that path cannot read or use the cookie.

- Expires. The expiration attribute contains a datetime string announcing when the cookie should be invalidated. The value in the expires attribute distinguishes session and persistent cookies [47].

- Secure. It indicates if the cookie is secure; it is a flag indicating that a cookie should be used under a secure server condition.

- HttpOnly. The HttpOnly attribute is a flag which specifies whether a cookie can be accessed programmatically client side.

[96] They were originally designed to assist users in online shopping, by saving information about the items selected by the user.

- Domain. A partial or complete domain name indicates the cookie is valid. The browser will return the cookie to any host that matches the partial domain name. If no domain is specified, the cookie will be returned only to the web server that created it.

In addition to their attributes, cookies can be divided into several categories. First distinction is between functional and non functional cookies. Functional cookies are cookies that ensure the proper functioning of the website and their installation does not require permission. For example those are cookies enabled for the login or registration, or language preferences. Non-functional cookies are cookies that can be set for statistical, social, targeting and commercial purposes. They are not related to the mere technical support of the Website [49].

1. Strictly necessary cookies. These cookies are essential to browse the website and use its features, such as accessing secure areas of the site. An example of those cookies are the ones that permit the user to put in the shopping cart the desired items. These cookies will generally be first-party session cookies. While it is not required to obtain consent for these cookies, what they do and why they are necessary should be explained to the user.[97] [50]

2. Preferences cookies. Also known as "functionality cookies," these cookies allow a website to remember the choices the user has made in the past,like the preferred language, the geographical region, or the username and password to automatically log in.[50]

3. Statistics cookies. Also known as "performance cookies," these cookies collect information about how the user uses a website, for example which pages he visited and which links he clicked on. None of this information can be used to identify the single user. It is all aggregated and, therefore, anonymized. Their sole purpose is to improve website functions. This includes cookies from third-party analytics services as long as the cookies are for the exclusive use of the owner of the website visited.[50]

4. Marketing cookies. These cookies track the online activity to help advertisers deliver more relevant advertising or to limit how many times an ad is seen. These cookies can share that information with other organizations or

[97] An example of strictly necessary cookies are cookies that allow web shops to hold the items in the cart while shopping online

advertisers. These are persistent cookies and almost always of third-party provenance.[98][50]

For what concerns the provenance, cookies are divided between first-party cookies and third-party cookies. First-party cookies, as the name implies, are put on the user's device directly by the website he is visiting[99].[50] Third-party cookies are placed on the user's device, not by the website he is visiting, but by a third party like an advertiser or an analytic system.[50]
There is also a distinction between persistent and session cookies. Persistent cookies are stored on a users' device in between browser sessions which allow preferences or actions of the user to be remembered. The cookies are activated every time the user that set these cookies visits the Website; most non-functional cookies are persistent cookies[100] [49]. Session cookies allow websites to link the actions of a user only during a browser session. A browser session starts when a user opens the browser screen and ends when he closes the browser screen. Session cookies are only set temporarily. When you close the browser, the cookies will be removed. Most functional cookies are session cookies[101][49].

The tool used to allow users to accept [102] or reject the use of certain cookies on a site, or to inform them about the site's privacy policy is usually a popup, known as cookie banner. Across multiple web sites the user can see different types of banner, changing from their visual characteristics to the options shown. In the figure, from "Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web", three common types of banner are identified, ordered by an increasing amount of control provided to the user.
The Type 1 banner is also called "cookie walls" [51]. It only informs users that cookies are used, and enables them to click "Accept" to express consent. However it can be expected that cookies are set regardless, whether the user clicks on the Accept button or not. Since the user is not presented with an equal choice, web-

[98] Some examples of marketing cookies are Google Adwords cookie, DoubleClick, AddThis WordPress plugin, Remarketing pixels, and Social Media cookies.

[99] For example, first-party cookies can be used to remember a user's login credentials during a single browsing session.

[100] For example, session cookies can be used to store the items that a user has added to their shopping cart during a single browsing session

[101] For example, a shopping site can use persistent cookies to store the items users have placed in their basket.

[102] The Directive 2009/136/EC, also known as the "Cookie Directive," regulates the use of cookies and trackers by requiring websites to obtain prior consent from users when employing cookies to process personal data from individuals inside the European Union (EU).

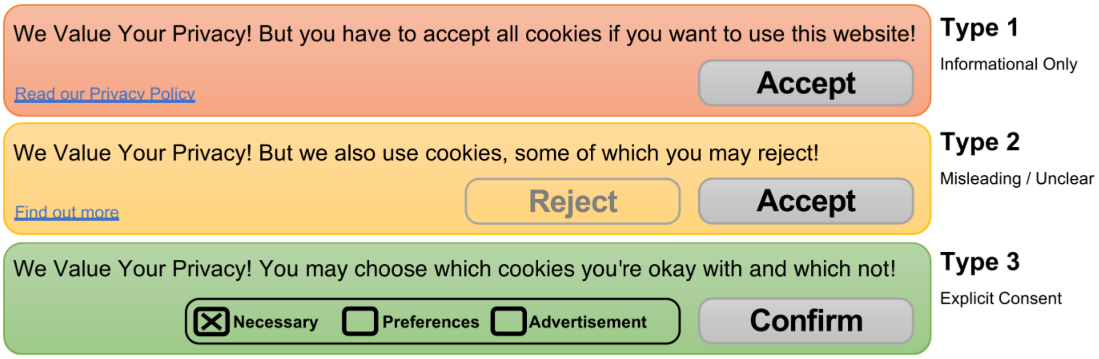

We Value Your Privacy! But you have to accept all cookies if you want to use this website!
Read our Privacy Policy
Accept
Type 1
Informational Only
We Value Your Privacy! But we also use cookies, some of which you may reject!
Find out more
Reject
Accept
Type 2
Misleading / Unclear
We Value Your Privacy! You may choose which cookies you're okay with and which not!
☒ Necessary
□ Preferences
□ Advertisement
Confirm
Type 3
Explicit Consent

Figure 1: Illustration of the three most common types of cookie banners ordered by an increasing amount of control provided to the user. (Source: [49])

sites with cookie walls cannot perform their data processing on the basis of explicit consent [49].

The second type of banner (Type 2) is the binary banner, and it offers users the possibility to reject cookies. Specifications about the use of cookies or how they are set may be formulated in the privacy policy. According to Article 7 of the GDPR, consent can only be provided in a comprehensible manner so the data subject knows what they consented to. According to the results obtained from the research of Kretschmer et al., after selecting “Reject”, usually some cookies are still being stored, and “Accept All” allows all possible cookies. The user needs to be able to know which cookies are necessary and cannot be rejected, and which constitute trackers that are only set upon consent. [49].

The third banner (Type 3) is the multiple-choice banner. It provides the user with more control about what kind of cookies he can reject or accept. Those type of banners can provide different levels of details, ranging from a couple of broad categories to listing every tracking party individually [49]. The categorization of cookies in multiple-choice banners varies and can be misleading, for example, by labeling cookies related to analytics used to personalize ads as necessary [52]. Thus, users cannot be certain that they are not being tracked even when selecting the most conservative cookie preferences [49].

Banners can also be set in a way that the user has to interact with them to fully access the website. Such banners are more difficult for the user to ignore, and the latter has to decide whether to give explicit consent or reject tracking. Another issue is that sometimes the choice of accepting all the cookies is made much easier for the user than rejecting cookies, which contradicts the GDPR’s notion of equal choice [49].

Many opinions have been collected concerning the use of cookies. It can be said that these are not exactly the evil of technologies, that they do not completely violate the privacy of the consumer, in fact their use has positive consequences. Some literature, however, rightly analyzes the negative sides of these tools, highlighting the dangerousness and immorality of their use.

When cookies were first developed, there were no intentions of using them as the type of spy mechanism they have the reputation of today. Cookies were developed only for the purpose of informing the Web site's server that a user had returned [48]. This process of user tracking was originally intended to be in the interest of the user. Saved information about the user results mean saved time and more personalized visits in the future for the user. Now the intention of this tool has grown broader, creating some controversial issues.

Cookies provide a variety of advantages for users, web developers, and marketers. It is really difficult today to use the internet without those [48]. The original function of cookies was the "shopping cart" feature, which has become very useful, both for consumers purchasing a variety of products and for companies that have an e-commerce market. Cookies allow users to save numerous items, as well as quantities, colors, and sizes in their shopping cart until they are ready for check-out. Cookies can also be used to store information about user interests. This enables the store to offer similar products that the user may like according to previous purchases. Advertisers and marketers also use the interests determined through cookie usage to select which advertisements will be most effective for a particular user [48]. Another function is to save the information with their ID and password so it is available when the user returns and is ready to make another purchase. The more information a user provides, the more cookies can assist the user in finding the information or products desired [48]. Marketers and advertisers use cookies to collect information about users. Upon encountering an advertisement for the first time from a particular server, a distinct ID is allocated to the browser and stored alongside the other cookie files. When visiting a Web site that contains an advertisement from that server, the cookie is employed to showcase the most suitable advertisement according to the user's interests that were inferred from the previously supplied information. Web developers use cookies for statistical purposes. They can track how many visitors arrive, how often a visitor returns, and how many are new visitors versus repeat visitors. This information can be used to plan future Web site updates, by keeping the data collected in a large database [48]. This is not done to spy on the users, but rather to provide information to Web site designers. By knowing where the users visit, designers can focus on those pages to present the information in the most user friendly way. Attention can also be given to the pages that have a low visitor count to determine any problems with the page content [48]. Overall the data obtained shows that since the introduction of GDPR, the amount of third-party tracking has declined, and transparency and user's control have improved. The prevalence of cookie banners and privacy policies and their volume has significantly increased across all datasets, leading to more consistent privacy levels on EU websites [49]. Hormozi et al, in "Cookies and Privacy", highlights also some disadvantages associated with the use of cookies. Firstly, the visitor counts can often be inaccurate or ineffective and that could influence statistical research. This can happen when users use more than one computer or share computers or a user accesses a website and has no intention to return. There is also a growing concern by users that perceive cookies as an invasion of privacy, since information is taken without their consent[103]. In the event that users do not review the privacy policy of a website, they may be unaware of the reasons behind the placement of cookies or how the collected data will be utilized. Typically, users do not know when a cookie stored on their hard drive is being accessed, as this process is carried out automatically by the web server. Fundamentally, cookies rely on user-specific data, which is transferred by the web server onto the user's computer for future use by itself or other servers [48]. Some issues that still remain [104], despite the introduction of GDPR, are the low ratio of multiple-choice cookie banners and the high complexity of privacy policies, since users prefer low-effort privacy-preserving choices [49].

The GDPR only mentions cookies directly once, in Recital 30 "Online Identifiers for Profiling and Identification": *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to*

[103] This is why private information such as credit card information, addresses, or phone numbers should not be stored in a cookie.[48]

[104] Hormozi et. al addressed the issue of cookie and privacy observing that: "The privacy controversy continues to grow with the number of lawsuits against Internet companies that do not disclose their use of cookies. In a June 2002 survey by Jupiter Research, 70 percent of E-commerce users said they were worried about their privacy online. In another survey conducted by Jupiter Research, 93 percent of Ecommerce users said it was very important that sites disclose their privacy practices. Goldman13 also believes that users attempting to protect their privacy are a small percentage of the Internet community. Many users who are concerned about their privacy do little or nothing to protect their privacy. Many do not even know how to configure a browser to stop cookies from being recorded, or read the privacy policies of the Web sites to learn what information cookies collect and how it is used."[48]

create profiles of the natural persons and identify them." This means that if it is possible to identify the user from cookies, those may be intended as personal data and therefore subject to the regulation. Companies can process their users' data as long as they receive consent or if they have a legitimate interest.

The ePrivacy Directive has become known as the "cookie law" and in some cases overrider the GDPR, addressing crucial aspects about the confidentiality of electronic communications and the tracking of Internet users more broadly. [50]

In order to be compliant with the GDPR and ePrivacy Directive while governing cookies, it is necessary to receive the users' consent before the use of any cookies (except the strictly necessary ones) and provide accurate and specific informations about which data the cookie tracks and its purpose, it all must be done in a clear and plain language. It should also be easy for the users to withdraw their consent as it was for them to give their consent in the first place. [50]

5 Enhancing Compliance with Bot Technology

5.1 Robotic Process Automation

The objective of this work is to provide a tool that can help companies comply with the principles of the GDPR. The creation of a bot would in fact bring various benefits, from saving time and costs to reducing errors. It is important to note that this tool is not intended to replace human involvement, as an understanding of the law and the rights guaranteed by regulations is necessary. Instead, it is designed to facilitate the compliance process. The primary focus of this thesis project is to create a bot capable of collecting cookies generated by various websites, simulating the actions of an ordinary user. The bot has been programmed using UiPath, a platform which is part of the technologies used for Robotic Process Automation (RPA) technologies.

Robotic Process Automation (RPA) is a cutting-edge technology that uses software robots to automate repetitive, rules-based tasks by emulating human actions. This technology is revolutionizing the way businesses operate, as it enables automation of tasks that were previously performed by humans, freeing them up to focus on more complex and higher-value tasks. Just like people, software robots can do things like understand what's on a screen, complete the right keystrokes, navigate systems, identify and extract data, and perform a wide range of defined actions [53]. The main difference between RPA and other forms of automation[105] is that RPA software robots mimic human actions to complete tasks, rather than simply automating the underlying processes, this allows RPA to be used to automate a wide range of jobs that would otherwise be performed by humans. One of the key advantages of RPA is that it is non-intrusive and can be integrated with existing systems without requiring any changes to the infrastructure, making it adaptable to legacy systems. This allows RPA to be used to automate tasks across a wide range of systems, including legacy systems that may not be easily integrated with other forms of automation [54].

Adopting these types of technologies gives organizations several benefits to exploit their resources better. By doing so, organizations can automate a wide range of tasks across different departments and functions, leading to significant cost savings and

[105] Those may include: AI and Machine Learning, Business Process Management (BPM), Intelligent Document Processing (IDP), Internet of Things (IoT), Cognitive Automation, DevOps Automation and many more.

increased efficiency. Moreover, an important characteristic is the ability to gather and analyze data in real-time. Robots can collect data from various sources, process it and make decisions in real time, providing organizations with real-time insights into their operations. RPA also has great flexibility, it can be easily integrated with other technologies, such as AI, Machine Learning, and Natural Language Processing, to improve the automation capabilities and to perform more complex tasks[54]. The adoption of RPA technology provides organizations with numerous benefits, including increased efficiency and accuracy, reduced costs, improved compliance, improved customer service, data gathering and analysis, scalability, process consistency, and increased flexibility. With robots capable of working 24/7 with little or no human supervision, automations can run more frequently and with higher accuracy, providing significant cost savings, improved quality of products or services and the reduction of human errors. Furthermore, RPA robots can work with sensitive data without the risk of human error, enhancing data security and regulatory compliance. In summary, RPA is a game-changing technology that enables organizations to optimize their resources and improve their operations in numerous ways[54].

UiPath[106] is one of the most popular software platforms, providing a wide range of automation tools and capabilities for businesses to automate their processes. The platform enables organizations to automate tasks such as data entry, document processing, and customer service, which leads to increased efficiency and cost savings. UiPath's powerful automation software is designed to work seamlessly with a variety of systems, including legacy systems, web, and desktop applications. This means that organizations can automate tasks across all areas of their business, from front-office functions to back-office operations[54]. The platform is made up of several components, including UiPath Studio, UiPath Robot, and UiPath Orchestrator. UiPath Studio is the development environment that facilitates the creation of automation projects, UiPath Robot runs the automations, and UiPath Orchestrator is the management and monitoring platform that enables organizations to manage and deploy their automation projects[54].
The UiPath platform is user-friendly, with a drag-and-drop interface that simplifies the process of creating and deploying automations. UiPath also offers a broad range of pre-built activities and templates, making it easy for users to begin automation projects.

[106] UiPath was launched for the first time in 2005 in Bucharest, Romania.

5.2 Introduction of the project

The project arose from the need to have a tool that would allow for continuous monitoring of cookies on all websites in the domain, facilitating the compliance with the regulations. As seen in previous chapters, compliance in the GDPR regulations is a fundamental requirement for companies to respect the privacy and rights of data subjects. Cookies, according to different opinions, may be a tool for violating consumer privacy, and are therefore covered by the regulations, which the company must comply with. The bot's programming focused on mimicking the behaviors of the normal individual when browsing a website. Given the vast amount of material to be verified (150 sites with all the sub-links for each site), the adoption of a technological robotics tool seemed an excellent solution, since repetitive and mechanical actions have to be carried out, and even a small human error can lead to serious consequences. Therefore, given a list of 150 websites as input, all cases of cookie acceptance were considered: the decision to click on "accept all cookies," "reject all cookies," and the selection of statistical, analytical, marketing cookies etc. For each type of cookie selected, the latter is collected from the Chrome console and saved in a database, so that the company can complete the verification, and check that there are no "misplaced" cookies, which would result in a very high administrative penalty, as required by the GDPR. The application of robotics, for this project, ensures the reduction of human error, high quality assurance, saves time and optimizes the effort of resources in time-consuming activities, and increases the frequency of inspections. Specifically, this paper aims to explain the individual process steps in question, identified and involved in Robotic Process Automation (RPA), using the "UIPATH" technology solution, which allows the automation of the entire process and the management of any failures, notifying the operator specifically if an error occurred or if the process was successful. During the analysis phase, the Working Group did not limit itself only to the collection of requirements, but also hypothesized the application solutions currently considered most suitable, which are also given in the document.

5.3 Methodology

The first step was to confront the company operator and understand what actions he usually carried out. To program a robot that mimics human behavior, it is necessary to fully understand this behavior. Every step taken is recorded so that it can be taught to the robot later on. There is a difference between the AS-IS and TO-BE processes, which were both carried out. The AS-IS analysis is based on the definition, documentation, and measurement of a situation before a planned change. In this case, it is how the operator carried out cookie verification without the use of the bot [107]. The definition of the TO-BE process, on the other hand, is the planning of the steps and objectives that the bot must achieve. Although the bot imitates human behavior, the tools it uses are obviously different (a human cannot be programmed to do things). Therefore, in this phase, the various activities and schedules that the bot must execute are defined. The final output will be the same, but the methods and execution speed will be different compared to before.

Further steps require methods for organizing the process, defining the activities to be performed, and handling any errors. UiPath provides various templates to select from, making the process arrangement easier and more effective. For this project, the Robotic Enterprise Framework was used [108]. This framework is designed to fit all the practices related to logging, exception handling, application initialization, and others, making it ready to handle complex business scenarios. It is a state machine-based template, containing default state containers for various stages or blocks. Different transitions are defined to jump from one state to another, with three different blocks being used in this case: Initialization, Process Transaction, and End Process.
This framework has several features that make it useful, including efficient reuse since the logic code is separated from other aspects of ReFramework and it can work for any type of process and business. It has the ability to retry a failed transaction multiple times and send exception notifications, provides an effective logging mechanism to monitor the process and error handling, takes a screenshot of the screen at the point of failure, making unattended automation easier to manage, and has the functionality to take action when an exception occurs, with code standards allowing for easy handover to a different developer [55].

[107] In this case the work consisted in updating the file with all the cookies in a specialized server, One Trust, which will be explained later. The bot adds a double verification to the process.

[108] Despite being the most used framework, the UiPath platfrom offers a long list of other framwroks that caan be used according to the specific needs such as: the Simple Process Framework (SPF) suitable for smaller automation projects with less complexity; the State Machine Framework; the Transactional Business Process Framework (TBF) which is designed for automating transactional processes that involve interactions with multiple systems or applications; the Page Object Model (POM) Framework which is particularly relevant for automating web-based applications; the Hybrid Framework combines multiple frameworks and methodologies to address the specific needs of a complex automation project; and many more alternatives.

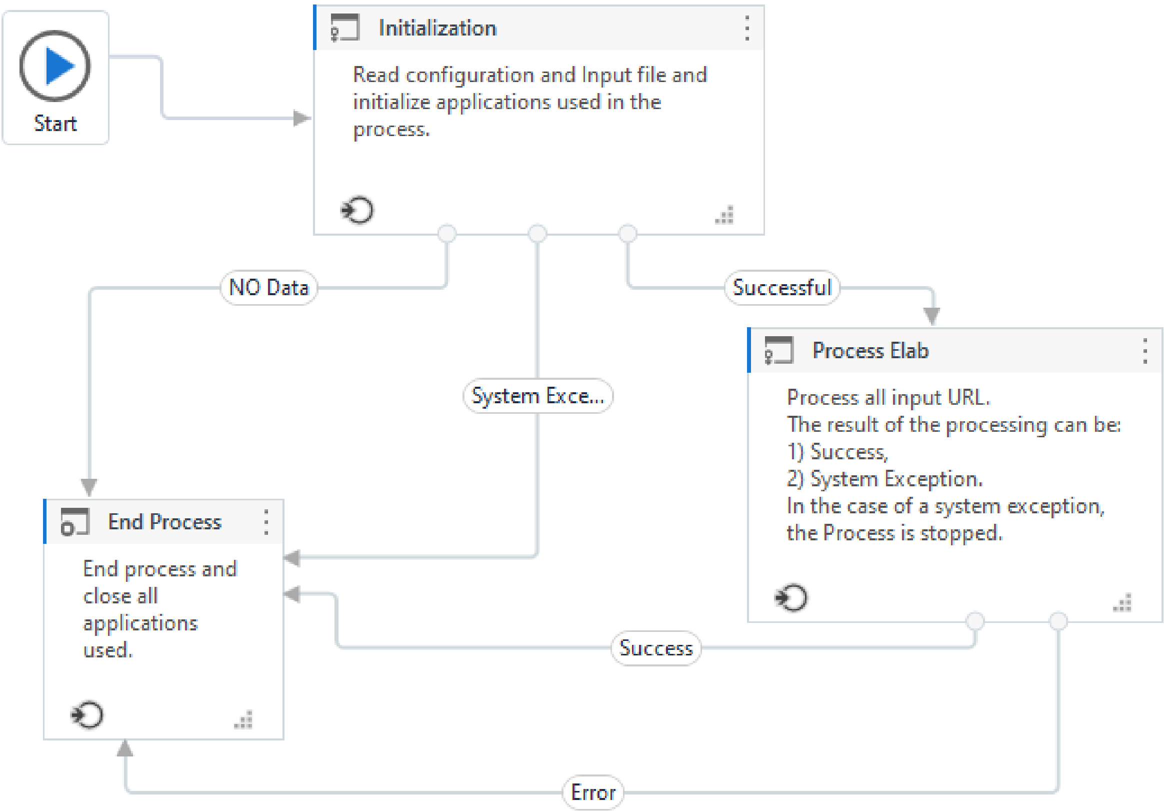

Start
Initialization
Read configuration and Input file and initialize applications used in the process.
NO Data
System Exce...
Successful
Process Elab
Process all input URL.
The result of the processing can be:
1) Success,
2) System Exception.
In the case of a system exception, the Process is stopped.
End Process
End process and close all applications used.
Success
Error

Figure 2: Illustration of the General Process in the UiPath Platform.

The first block used is the Initialization Process, a state that reads and stores configuration data, closes all unnecessary applications, and opens the required ones. In case of an error (System Exception) or absence of data, the flow moves to the End Process state. If the initialization is successful, the flow moves to the Process Elaboration state, where the actual processing takes place. Multiple sequences and workflows are included to support the execution. Regardless of success or error, the flow moves to the End Process state[109], which is the final state of the ReFramework, where all used applications are closed, and the project is stopped.

Different activities are utilized in the workflow for the robot to perform the desired functions. Some of these are Try Catch, Click, Check App State, Use Application/Browser, Keyboard Shortcuts, Connection to DataBase among others. The Try Catch Activity is used for managing exceptions, it allows to determine how to respond if an exception is thrown so it can be handled appropriately; it is useful to prevent the robot from breaking in the event of an exception. There are three main

[109] Sometimes it can happen that in case of an error, instead of going direclty to the End Process, the bot stops.

sections: the Try holds the activities that could throw an exception, the Catches indicate the exception type and the Finally section holds an activity that will always be executed. The Click Activity is used to click a particular element; there is the possibility to choose between a double click, right or left click according to the specific requirements. For this project it is used for various tasks, such as clicking on the different benner's buttons on the webpages or selecting different tabs on the Chrome console. The Check App State checks the state of an application or web browser by verifying if an element appears in or disappears from the user interface, and can execute one set of activities if the element is found and a different set of activities if the element is not found. It was used to check the different versions of banners from different Websites that appeared on the screen or to wait the end of loading of sites while they were being scanned. The Use Application/Browser Activity allows to automate the web application process and it is used where there is the need to select a browser or any other application to perform an automation; in the process it is used to run on Chrome or ScreamingFrog, a website crawler used to obtain all the sub-links of the major sites which was use to scan all the urls belonging to a single site. Keyboard Shortcuts Activity allows to perform some of the keyboard functions without using the actual keyboard, for example it was used Ctrl + Shift + Del to delete the cache from Chrome navigation. Other useful activities were the Connect Activity, which gives the possibility to connect to a database by using a standard connection string, and the activities that allows to execute queries in order to modify or to get some data from the database. The Extract Table Data Activity allows to extract data from a specified web page or application, which is used to get data from the Chrome's console and put it in the database, obtaining values in terms of columns and rows. Many more activities were used to program the robot that will be discussed later on this paper.
A fundamental tool used during the automation is the Selector, used to interact with the Graphical User Interface elements by identifying their tags and attributes in UiPath Studio [57]. A selector is composed of several nodes and each node has one or more attributes associated with it. Modifications to the attributes can be done as required [58]. It has been a very useful tool for detecting banners and buttons, as they are nonconstant elements since their value changes according to their type. The selector is still able to identify them according to their "id", "class", "parentid" etc.

The SQL Database was used for storing and retrieving data. This type of database consists of highly structured tables, where each row reflects a data entity, and every column defines a specific information field. Relational databases are built using SQL to create, store, update, and retrieve data [56].

5.4 General Process Description

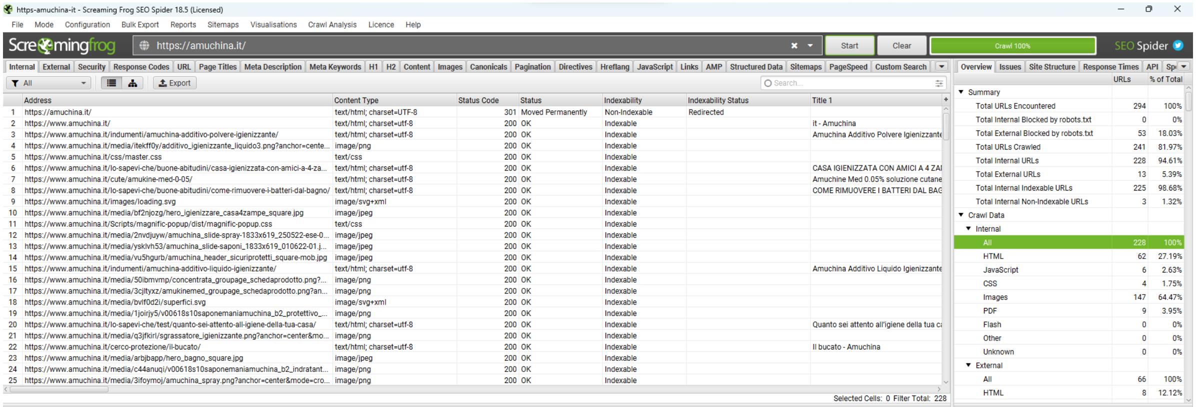
The general process starts with the "Initialization" block, where the configurations and input files are read, and the applications that will be used in the process are initialized. Within a Try Catch Activity, variables representing System Exceptions and the current date are assigned using the DateTime format in Italian. The CultureInfo variable type in Italian is also assigned, which provides culture-specific information such as the language, sublanguage, country/region, calendar, and conventions associated with the Italian culture. Next, the RCODE of the specific operation is defined, which includes a datetime string in the format "yyyyMMddHHmmss" to generate a unique code associated with a specific date and time. This allows for diversification of the operations since no two will be executed at the same time. The referenced code is then saved in the SQL database via an INSERT query in the "RCODE" column to serve as a reference point for all operations. Other columns, such as "TIMESTAMP" for the execution date, "FEEDBACK" for the status code of the URLs obtained after the scan, "SITO_URL" for the domain site, "SOTTO_LINK" for the sub-links derived from it, and "TIPO_COOKIE" for the detected cookies by the Chrome console, are also created for later use in the process.

The client provides a list of all the sites to be browsed by the bot, which is saved in an Excel file. The bot can read this file via the Read Range Activity and saves all the sites in a dictionary variable type. To avoid possible errors due to missing sites in the Excel file, a second check is performed. The bot checks the string to ensure it is not empty or null using a For Loop.

After all initial configurations and settings are set, the process begins[110]. The result of the processing can either be Success or System Exception, and in the latter case, the process stops. The process starts with a For Loop, as the same process must be done for all the sites in the list (stored in a DataTable). The bot cycles through each site and performs the desired actions. In case of an error, a BusinessRuleException[111] is thrown, indicating that the link is not being elaborated due to an exception. A Business Exception describes an error caused by incomplete or

[110] The process is launched by the Orchestrator in UiPath.

[111] Other types of exception are System.Exception, System.ApplicationException, System.ArgumentException, System.NullReferenceException, System.TimeoutException, System.Security.SecurityException, UiPath.Core.ElementNotFoundException, UiPath.Core.SelectorNotFoundException, and many more which depend on the project and the specific activities used.


https-amuchina-it - Screaming Frog SEO Spider 18.5 (Licensed)
File Mode Configuration Bulk Export Reports Sitemaps Visualisations Crawl Analysis Licence Help
Screamingfrog
https://amuchina.it/
Start
Clear
Crawl 100%
SEO Spider
Internal External Security Response Codes URL Page Titles Meta Description Meta Keywords H1 H2 Content Images Canonicals Pagination Directives Hreflang JavaScript Links AMP Structured Data Sitemaps PageSpeed Custom Search
All
Export
Search...
Overview Issues Site Structure Response Times API Spe

	Address	Content Type	Status Code	Status	Indexability	Indexability Status	Title 1
1	https://amuchina.it/	text/html; charset=UTF-8	301	Moved Permanently	Non-Indexable	Redirected	
2	https://www.amuchina.it/	text/html; charset=utf-8	200	OK	Indexable		it - Amuchina
3	https://www.amuchina.it/indumenti/amuchina-additivo-polvere-igienizzante/	text/html; charset=utf-8	200	OK	Indexable		Amuchina Additivo Polvere Igienizzante
4	https://www.amuchina.it/media/itekff0y/additivo_igienizzante_liquido3.png?anchor=cente...	image/png	200	OK	Indexable		
5	https://www.amuchina.it/css/master.css	text/css	200	OK	Indexable		
6	https://www.amuchina.it/lo-sapevi-che/buone-abitudini/casa-igienizzata-con-amici-a-4-za...	text/html; charset=utf-8	200	OK	Indexable		CASA IGIENIZZATA CON AMICI A 4 ZA
7	https://www.amuchina.it/cute/amukine-med-0-05/	text/html; charset=utf-8	200	OK	Indexable		Amuchine Med 0.05% soluzione cutane
8	https://www.amuchina.it/lo-sapevi-che/buone-abitudini/come-rimuovere-i-batteri-dal-bagno/	text/html; charset=utf-8	200	OK	Indexable		COME RIMUOVERE I BATTERI DAL BAG
9	https://www.amuchina.it/images/loading.svg	image/svg+xml	200	OK	Indexable		
10	https://www.amuchina.it/media/bf2njozg/hero_igienizzare_casa4zampe_square.jpg	image/jpeg	200	OK	Indexable		
11	https://www.amuchina.it/Scripts/magnific-popup/dist/magnific-popup.css	text/css	200	OK	Indexable		
12	https://www.amuchina.it/media/2nvdjuyw/amuchina_slide-spray-1833x619_250522-ese-0...	image/jpeg	200	OK	Indexable		
13	https://www.amuchina.it/media/ysklvh53/amuchina_slide-saponi_1833x619_010622-01.j...	image/jpeg	200	OK	Indexable		
14	https://www.amuchina.it/media/vu5hgurb/amuchina_header_sicuriprotetti_square-mob.jpg	image/jpeg	200	OK	Indexable		
15	https://www.amuchina.it/indumenti/amuchina-additivo-liquido-igienizzante/	text/html; charset=utf-8	200	OK	Indexable		Amuchina Additivo Liquido Igienizzante
16	https://www.amuchina.it/media/50ibmvmp/concentrata_groupage_schedaprodotto.png?...	image/png	200	OK	Indexable		
17	https://www.amuchina.it/media/3cjltyxz/amukinemed_groupage_schedaprodotto.png?an...	image/png	200	OK	Indexable		
18	https://www.amuchina.it/media/bvlf0d2i/superfici.svg	image/svg+xml	200	OK	Indexable		
19	https://www.amuchina.it/media/1joirjy5/v00618s10saponemaniamuchina_b2_protettivo_...	image/png	200	OK	Indexable		
20	https://www.amuchina.it/lo-sapevi-che/test/quanto-sei-attento-all-igiene-della-tua-casa/	text/html; charset=utf-8	200	OK	Indexable		Quanto sei attento all'igiene della tua c
21	https://www.amuchina.it/media/q3jfkirl/sgrassatore_igienizzante.png?anchor=center&mo...	image/png	200	OK	Indexable		
22	https://www.amuchina.it/cerco-protezione/il-bucato/	text/html; charset=utf-8	200	OK	Indexable		Il bucato - Amuchina
23	https://www.amuchina.it/media/arbjbapp/hero_bagno_square.jpg	image/jpeg	200	OK	Indexable		
24	https://www.amuchina.it/media/c44anuqi/v00618s10saponemaniamuchina_b2_indratant...	image/png	200	OK	Indexable		
25	https://www.amuchina.it/media/3ifoymoj/amuchina_spray.png?anchor=center&mode=cro...	image/png	200	OK	Indexable		

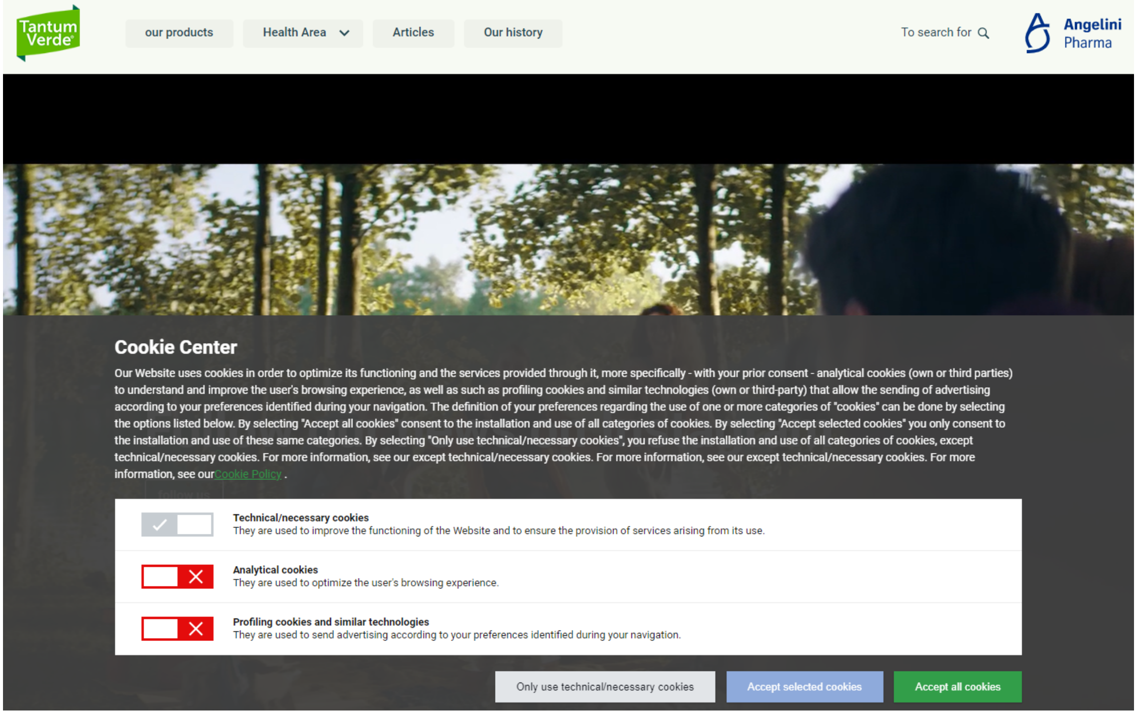
Selected Cells: 0 Filter Total: 228

	URLs	% of Total
▼ Summary		
Total URLs Encountered	294	100%
Total Internal Blocked by robots.txt	0	0%
Total External Blocked by robots.txt	53	18.03%
Total URLs Crawled	241	81.97%
Total Internal URLs	228	94.61%
Total External URLs	13	5.39%
Total Internal Indexable URLs	225	98.68%
Total Internal Non-Indexable URLs	3	1.32%
▼ Crawl Data		
▼ Internal		
All	228	100%
HTML	62	27.19%
JavaScript	6	2.63%
CSS	4	1.75%
Images	147	64.47%
PDF	9	3.95%
Flash	0	0%
Other	0	0%
Unknown	0	0%
▼ External		
All	66	100%
HTML	8	12.12%

Figure 3: Illustration of the ScreamingFrog application after the scan.

missing data, in this case, the link of the website. If the link has an appropriate value, the process starts. First, the ScreamingFrog application is opened using the Use Application/Browser Activity, the bot writes the current URL in the search bar using the TypeInto Activity, and it begins to scan all the sub-links [59].
The application provides all the data related to a site, so the bot clicks on "Page Titles" because it represents all the sub-links of the main site and is the data needed for navigation. Before starting the export, the bot checks that the status code of the site is equal to "200" using the Get Text Activity. The 200 response means that the page exists, so the site is valid and browsable. In other cases, the status code of the site might be the same as 301, 302, 404, or others, which means that the site might have been moved permanently or temporarily, or it no longer exists. The status code is then entered into the database, so that if there are problems on the site, the client can easily identify them. Once it is verified that the status code is valid, the URL is considered "imported". The bot cliks on the buttom "Export" and types the desired path, with a Type Into Activity, where the data should be stored. The whole list of sub-links is exported to an Excel file and then to a CSV File. Some sites are saved as "original," indicating that they are the ones being scanned from.

After performing the scan and saving all URLs, navigation for each site on Google Chrome begins. Cookies are collected according to three categories, with an array defined to contain the values "ALL," "Selected," and "DEFAULT." This is done to make browsing more efficient in terms of timing and to better classify the cookies found. The loop starts with the value "ALL," referring to the selection and acceptance of all cookies without preference management. Before browsing begins, the cache is cleared because browsers such as Chrome store some information about websites in their cache and cookies. This ensures that all detected cookies will be



Cookie Center

Our Website uses cookies in order to optimize its functioning and the services provided through it, more specifically - with your prior consent - analytical cookies (own or third parties) to understand and improve the user's browsing experience, as well as such as profiling cookies and similar technologies (own or third-party) that allow the sending of advertising according to your preferences identified during your navigation. The definition of your preferences regarding the use of one or more categories of "cookies" can be done by selecting the options listed below. By selecting "Accept all cookies" consent to the installation and use of all categories of cookies. By selecting "Accept selected cookies" you only consent to the installation and use of these same categories. By selecting "Only use technical/necessary cookies", you refuse the installation and use of all categories of cookies, except technical/necessary cookies. For more information, see our except technical/necessary cookies. For more information, see our except technical/necessary cookies. For more information, see ourCookie Policy .

☑ **Technical/necessary cookies**
They are used to improve the functioning of the Website and to ensure the provision of services arising from its use.

☒ **Analytical cookies**
They are used to optimize the user's browsing experience.

☒ **Profiling cookies and similar technologies**
They are used to send advertising according to your preferences identified during your navigation.

Figure 4: Example of type of banner

"cleaned." This task is performed thanks to the Keyboard Shortcuts and Click Activity, where the bot simulates the keyboard's option to delete the cache, Ctrl + Shift + Del and then clicks on "Clear Data".

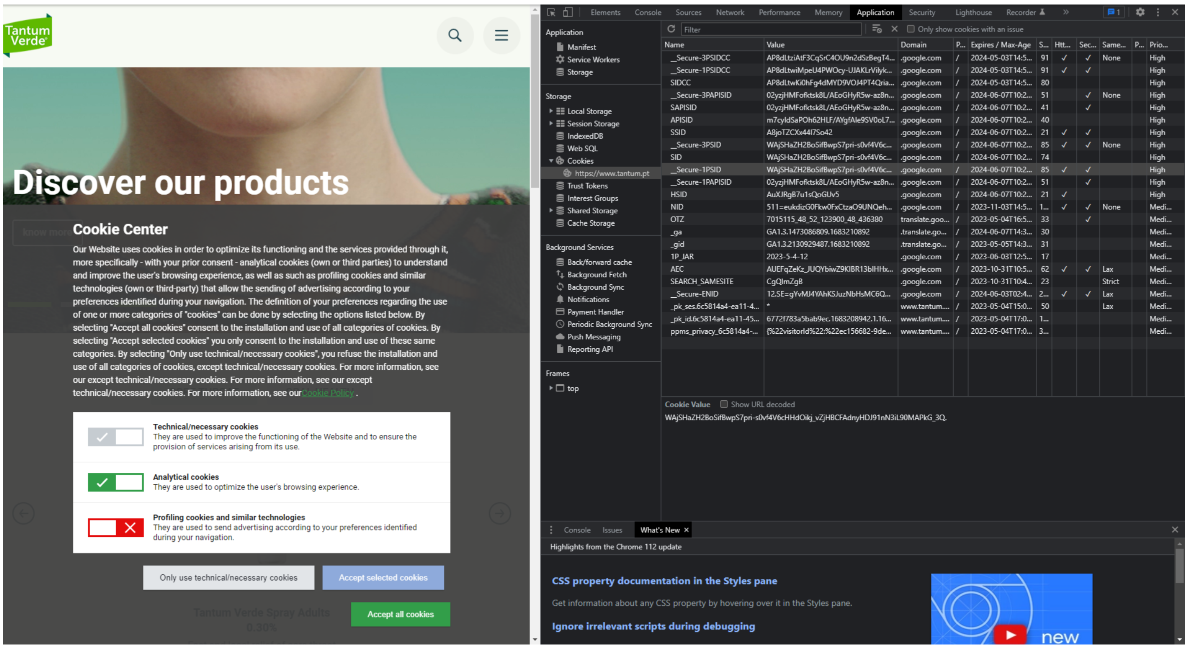
At this point, an If statement is inserted with a critical condition: the process takes a different direction if the link is the first in the domain or not. If it is the first, all information regarding the site will be collected, from the type of banner to the type of cookies present. This information will be recorded only once for the site, whereas for others it will be remembered to make the process more efficient and faster. Navigation of the first URL then takes place. When the website is opened, the bot must identify the version of the banner present. In a previous analysis, eleven [112] different banner versions were discovered, each with unique button types, graphics and html code. The bot was programmed with this information, and through a Check App State activity, it is able to recognize the banners. To begin, the variable "ExistBanner" is set to False using an Assign Activity, which changes when the bot finds a match with the referenced banner. In some cases, the banner may be present in the website's console, but not immediately visible. Therefore, a second check was

[112] Banner diversity comes from the fact that the company assigns the management of the sites to different agencies, which then apply their own graphics and codes to manage them.

added to determine if the ”relativeVisibility” attribute is present and set to True. Identifying the banner is crucial, as each version has unique buttons that require different approaches to navigate. Once identified, the bot creates a datatable to store all selectable buttons (switches) present on the screen. This datatable will be used in a second round to select buttons and save detected cookies. However, some banners do not have these options, and the bot will adjust its approach accordingly. For example, some banners require the user to click ”manage options” to view all existing buttons, while others only allow acceptance or refusal of cookies. To prevent errors and save time during navigation, the bot will change the initial array used in the cycle based on the banner and existing buttons. Some sites will only have the ”ALL” option, in this case a Break Actitivty will stop the loop since there is no need to go further with the navigation and will continue extracting data from the other sub/links; while others will have ”ALL” and ”Default”, meaning that the ”user”'s choices are either to accept all cookies or just the necessary ones, without having to choose between specific ones.
After identifying the banner, the bot uses a Switch Activity to determine the next actions based on the input value. If the value is ”ALL”, the bot creates a datatable to store all IDs of the buttons detected while scanning the banner. This allows the bot to determine how many options the user has, such as the ability to choose between analytical, profiling, or marketing cookies. The information is then saved in a variable, which is used to click on the desired button. This variable is inserted in the dynamic selector, allowing the bot to click on the specific button, according to its Button ID. Afterward, the bot accepts the cookies by clicking on the ”accept” button.
If the banner is not identified, so no match occurs, then the ExistBanner variable will remain equal to False, indicating that no banner is present in the current site being scanned. This information will be saved in the database, with the attribute ”NO BANNER”.

Next, the bot opens the console using the Keyboard Shortcuts Activity, which simulates the combination of Ctrl+Shift+l buttons to open the console. Once the console is opened, the bot can identify the section where the various cookies are listed, which is located under the ”Storage” section. The bot is able to identify the correct index to manage the cookies accordingly.

To further enhance the accuracy of the process, an additional check is added to ensure that sites listed under the ”Cookies” heading actually contain entries. This is achieved through a Check App State activity, which verifies whether the ”Name”



Cookie Center

Our Website uses cookies in order to optimize its functioning and the services provided through it, more specifically - with your prior consent - analytical cookies (own or third parties) to understand and improve the user's browsing experience, as well as such as profiling cookies and similar technologies (own or third-party) that allow the sending of advertising according to your preferences identified during your navigation. The definition of your preferences regarding the use of one or more categories of "cookies" can be done by selecting the options listed below. By selecting "Accept all cookies" consent to the installation and use of all categories of cookies. By selecting "Accept selected cookies" you only consent to the installation and use of these same categories. By selecting "Only use technical/necessary cookies", you refuse the installation and use of all categories of cookies, except technical/necessary cookies. For more information, see our except technical/necessary cookies. For more information, see our except technical/necessary cookies. For more information, see ourCookie Policy .

☑ **Technical/necessary cookies**
They are used to improve the functioning of the Website and to ensure the provision of services arising from its use.

☑ **Analytical cookies**
They are used to optimize the user's browsing experience.

☒ **Profiling cookies and similar technologies**
They are used to send advertising according to your preferences identified during your navigation.

Only use technical/necessary cookies | Accept selected cookies | Accept all cookies

Name	Value	Domain	P...	Expires / Max-Age	S...	Htt...	Sec...	Same...	P...	Prio...
__Secure-3PSIDCC	AP8dLtziAtF3CqSrC4OU9n2dSzBegT4...	.google.com	/	2024-05-03T14:5...	91	✓	✓	None		High
__Secure-1PSIDCC	AP8dLtwiMpeU4PWOcy-UJAKLrVilyk...	.google.com	/	2024-05-03T14:5...	91	✓	✓			High
SIDCC	AP8dLtwKi0hFg4dMYD9VOJ4PT4Qria...	.google.com	/	2024-05-03T14:5...	80					High
__Secure-3PAPISID	02yzjHMFofktsk8L/AEoGHyR5w-az8n...	.google.com	/	2024-06-07T10:2...	51		✓	None		High
SAPISID	02yzjHMFofktsk8L/AEoGHyR5w-az8n...	.google.com	/	2024-06-07T10:2...	41		✓			High
APISID	m7cyldSaPOh62HLF/AYgfAIe9SV0oL7...	.google.com	/	2024-06-07T10:2...	40					High
SSID	A8joTZCXx44I7So42	.google.com	/	2024-06-07T10:2...	21	✓	✓			High
__Secure-3PSID	WAjSHaZH2BoSifBwpS7pri-s0vf4V6c...	.google.com	/	2024-06-07T10:2...	85	✓	✓	None		High
SID	WAjSHaZH2BoSifBwpS7pri-s0vf4V6c...	.google.com	/	2024-06-07T10:2...	74					High
__Secure-1PSID	WAjSHaZH2BoSifBwpS7pri-s0vf4V6c...	.google.com	/	2024-06-07T10:2...	85	✓	✓			High
__Secure-1PAPISID	02yzjHMFofktsk8L/AEoGHyR5w-az8n...	.google.com	/	2024-06-07T10:2...	51		✓			High
HSID	AuXJRgB7u1sQoGUv5	.google.com	/	2024-06-07T10:2...	21	✓				High
NID	511=eukdizG0Fkw0FxCtzaO9UNQeh...	.google.com	/	2023-11-03T14:5...	1...	✓	✓	None		Medi...
OTZ	7015115_48_52_123900_48_436380	translate.goo...	/	2023-05-04T16:5...	33		✓			Medi...
_ga	GA1.3.1473086809.1683210892	.translate.go...	/	2024-06-07T14:3...	30					Medi...
_gid	GA1.3.2130929487.1683210892	.translate.go...	/	2023-05-05T14:3...	31					Medi...
1P_JAR	2023-5-4-12	.google.com	/	2023-06-03T12:5...	17					Medi...
AEC	AUEFqZeKz_JUQYbiwZ9KIBR13bIHHx...	.google.com	/	2023-10-31T10:5...	62	✓	✓	Lax		Medi...
SEARCH_SAMESITE	CgQImZgB	.google.com	/	2023-10-31T10:4...	23			Strict		Medi...
__Secure-ENID	12.SE=gYvMJ4YAhKSJuzNbHsMC6Q...	.google.com	/	2024-06-03T02:4...	2...	✓	✓	Lax		Medi...
_pk_ses.6c5814a4-ea11-4...	*	www.tantum....	/	2023-05-04T15:0...	50			Lax		Medi...
_pk_id.6c5814a4-ea11-45...	6772f783a5bab9ec.1683208942.1.16...	www.tantum....	/	2023-05-04T17:0...	1...					Medi...
ppms_privacy_6c5814a4-...	{%22visitorId%22:%22ec156682-9de...	www.tantum....	/	2023-05-04T17:0...	3...					Medi...

Cookie Value □ Show URL decoded
WAjSHaZH2BoSifBwpS7pri-s0vf4V6cHHdOikj_vZjHBCFAdnyHDJ91nN3iL90MAPkG_3Q.

Highlights from the Chrome 112 update

CSS property documentation in the Styles pane

Get information about any CSS property by hovering over it in the Styles pane.

Ignore irrelevant scripts during debugging

Figure 5: Image of the Chrome Console

and "Value" entries have actual values, and excludes them from consideration if they do not. The console data is then captured and written to a database table using the Extract Table Data Activity.

As discussed in chapter two, cookies have various attributes and characteristics, including Name, Value, Domain, Path, Expires, Secure, HttpOnly, Size, SameSite, Partition Key, and Priority[113]. These values are all recorded in the table, enabling the client to easily access the information as needed.

All the extracted cookies are then saved in the database. A difference is made between cookies that are saved as "Original" and those that are saved as "Console", in the FEEDBACK column.

As mentioned earlier, the "Original" sites are the ones from which the scanning and sub-link detection starts. In a first phase of experimentation, the plan was to run button click simulation and cookie extraction for each sub-link, each time reopening the browser and performing a new navigation. However, this operation was very time-consuming. A discussion with the client led to a much more effective solution. There is no need for the bot to start the navigation and button selection for each sub-link each time: once the choice is made on which cookies to consider and accept on the main site, this will be remembered for all other sub-links, making

[113] Not all of this properties will be useful for the current analysis, but are collected anyways to facilitate further implementations.

the navigation faster and the process easier because the bot does not have to reopen the browser and console each time. Indeed, once the cookies are extracted from one site, through a Type Into Activity the bot types the next site in the search bar and it continues the extraction on the other sub-links, while the cookie settings are still enabled.

One important step, however, is to have the bot click on the "Clear all cookies" button to avoid that while browsing, cookies belonging to the previous site are also detected in the next, making the analysis incorrect. The "Original" designation thus belongs to the cookies extracted from the main site, while the "Console" designation belongs to those found later.

In case of an error, a System Exception is thrown specifying that the data could not be loaded to the database.

Once the loading of the first link's information is finished, the bot knows that it will next go on to analyze the sub-links (thanks to a variable called "FirstLink" which is given the value of True at first, and False after that), so it remembers all the initialization settings previously set and continues browsing and extracting data from the console.

Once the first navigation cycle for the extraction of cookies, in which they are accepted all and are saved as "ALL", it continues with the other options. Next it will be selected the button "accept only necessary" and then "accept selected ones", in which depending on the options in the banners, the distinction between analytical cookies, marketing, profiling etc. will be made. As mentioned above, if the banners do not have all the buttons (as in the Figure 5), cookies are still managed and registered on the database.

Finally, the bot, via the FTP Scope activity, which manages the connection with the FTP server and provides scope for all the FTP activities, uploads the file created, with all the cookies' information in it, in CSV format.

Then the process ends; and depending on the customer's request, it will be restarted, or it will work uninterruptedly if it is given continuous input data flows.

5.5 Verification of Cookies' Compliance

Once all the data has been provided to the customer, the RPA project can be said to be completed, but not the cookie verification project in general. The data is extracted from the database and the bot finally sends the final document in the form of FTP (File Transfer Protocol). To verify cookie compliance, the company uses a software platform called OneTrust. OneTrust provides tools for website and

cookie compliance management. One of the features it offers is a cookie compliance scanner, which checks websites for cookies and other tracking technologies to help ensure that the site is compliant with GDPR requirements [60].
Consequently, the client uploads the files containing all the information with cookies to the platform. OneTrust is in fact able to scan all sites and identify which cookies are in use. A comparison is then made between the list of cookies and those identified during the scan; any discrepancies between the two lists may indicate cookies that are not compliant with GDPR.
For large organizations, the bot proves to be a very useful tool. It is common for website management to be assigned to multiple agencies (in this case, almost ten), each with different ways of handling the sites. Therefore, a tool that can handle this decentralization is crucial. Many agencies have different cookie policies that should be harmonized, as well as various software houses. The bot is a tool that would help reduce maintenance and monitoring costs. In this way, the agency is also able to identify where the problem occurs: the bot uploads each cookie and its corresponding URL into a table, making it possible to understand the origin of that cookie and the reason for its placement. Another benefit is the availability of continuous reports on each individual site, making the checks more accessible and comprehensible. They can also be used as historical evidence in case of comparison with the privacy authority[114].

5.6 Discussion of the results

Before discussing the results, it is important to clarify that at the time of writing this document, the project is still in the development phase and has not yet entered the production phase. This means that future changes and adjustments may be made to implement the results and improve efficiency.

One of the baselines used to measure results is the comparison between the activity performed by the human operator and that performed by the bot, in terms of time and efficiency. During the development phase, tests were conducted on a sample of 10 sites to improve monitoring. The bot took an average of 1.6 minutes per site to detect the different cookies, and processing times for the 10 sites averaged 4 hours per site (including sub-links, which on average are 200 per site), totaling 40 hours

[114] All of those information were obtained from an interview with one of the agencies that handle the websites of the organization.

(on average) or slightly over a day to complete the process (1,667 days). These results can be achieved when the robot is able to work unattended, without human supervision, and can work 24/7. This gives the robot a significant advantage over a human operator, who cannot work continuously every day, and allows it to complete the process in much shorter execution times.

The main objective of the project was to correctly detect cookies within the sites, and the bot was tested on two specific websites where the client had purposely added cookies that were not supposed to be there. During the testing phase, the bot successfully detected the additional cookies, including their attributes, types, and the sites they belonged to. This was a crucial success, as in the real world, the company could have faced severe penalties for failing to comply with GDPR regulations.

The project results can be evaluated based on its efficiency, timing, and error reduction. Compared to humans, robots have a lower error rate, in part because bot errors often result from human programming mistakes. Human errors can therefore reduce the efficiency of work. In terms of flexibility, the project has achieved excellent results, as modifications can be easily made to meet specific needs and accommodate changes. Furthermore, implementing process automation can lead to better results in terms of cost reduction and return on investment, with costs being relatively low compared to the significant penalties imposed by the GDPR. By investing in automation, companies can become more innovative and free up workers from repetitive and automatic tasks, allowing them to focus on tasks that require human reasoning skills. This can lead to increased job satisfaction and a more engaged workforce.

5.7 Further Implementation

This section will explore potential improvements that can be made to both the technical aspects of the process and the broader context and environment in which GDPR and privacy issues arise.

Regarding the technical component, it should be remainded that this thesis work is still in an experimental stage, as the project has not yet been put into production. Therefore, there is still time for the team to make necessary improvements to make the process even more efficient.

The first adjustment that needs to be made pertains to the project's theme, which is improving security. This involves adding controls to the process flow to manage passwords and user application access to ensure greater security. All utilities will be placed on an asset, which typically represents shared variables or credentials and allows for specific information to be stored so that robots can easily access it.
They can be invoked by RPA developers when designing a process, but their values can be hidden from them. The values will then go into a configuration file, so the bot will query it when it needs to save credentials to make various accesses to the applications, the database, or online. The Assets page simplifies this operation, allowing for the creation of new assets. It also displays all previously created assets, which can be edited or deleted. The Get Asset and Get Credential Activities used in Studio request information from Orchestrator about a specific asset, according to a provided AssetName. If the AssetName provided in Studio coincides with the name of an asset stored in the Orchestrator database, and the Robot has the required permissions, the asset information is retrieved and used by the Robot when executing the automation project. [61] This step would significantly enhance the security of the robot, as it accesses and processes credentials that are considered sensitive data and must be safeguarded in the event of any vulnerabilities in the system.

Numerous actions performed by the bot necessitate the recognition of specific elements such as the type of banner or the detection of the button pad, hence there is a need to add more control activities to ensure that these actions are correctly executed. The detection of individual cookies is indeed critical, since missing even one of them can lead to serious consequences for the business; therefore, it is possible to decide to make a trade-off between speed and accuracy for certain situations in order for the bot to correctly recognize all elements, even if it takes slightly longer.
A multiple check is fundamental also to increase consistency, as it can ensure that the output produced will be the same, and facilitate the debugging phase, whereas it can easily help developers themself to quickly diagnose and fix eventual issues.
In order to allow it to function properly and not make the bot go wrong, there is also the need to add processing steps, for instance, have the bot verify that the Chrome console is actually open in the desired location, so that the click and data extraction activities can always be accurate.
The correct definition of variables is fundamental to guarantee greater accuracy, because they are not always written by the bot, and NullReferenceException could occur the moment the value of the variable is null. This check must be inserted

because sometimes the bot does not go into error, but then continues the process while using incomplete data, which could compromise the final result [115]. Application shutdowns must also be handled well in this context, which should happen only if the process has not encountered any errors, and if not, at the EndProcess level the different errors must be handled differently from the current state.

Another objective is to leverage the functions of the Dispatcher and the Performer. The Dispatcher extracts data from a particular source, such as an excel sheet or a database, and adds it to a queue that the bot can access. This model helps the bot handle large amounts of data in an organized and efficient manner, which is particularly useful when dealing with larger quantities of websites. The Performer is responsible for processing the data added by the Dispatcher into the queue. By separating the data retrieval and processing tasks, the Performer can focus solely on executing the bot's core tasks, which results in increased efficiency and productivity. Implementing this model improves the process in terms of scalability, enabling the bot to handle large volumes of data without compromising its performance. Additionally, this model improves flexibility and the ability to handle errors since it gives the ability to perform multiple functions simultaneously and better vulnerabilities detection. In summary, leveraging the Dispatcher and the Performer functions will improve the bot's process, increasing efficiency and productivity while ensuring scalability and error handling.

A trade-off between accuracy and execution time was mentioned earlier, and many activities within the process require high execution times. Therefore, there is a twofold necessity to have an optimal result and in the shortest possible time. To improve timing and make the process run faster, one can reduce the wait time on certain activities, such as Retry Activity or ElementExist Activity, which usually take a few seconds, without compromising the final result.

UiPath Studio integrates with Microsoft Outlook, meaning there are integrated activities that aid in email automation when using the Outlook application. By using the "SendOutlookMailMessages" Activity, the bot can send an email from UiPath Studio. The introduction of these activities can allow reports with the results for each site to be sent to the desired recipient. The robot generates these

[115] As mentioned above, the bot goes directly to EndProcess in case of an Excpetion, but according to spefici requirements it can be programmed to stop.

reports at the end of the process and sends emails if any errors occur so that the client is immediately informed, thus improving the reporting phase. Currently, the bot creates a document named with the RCODE of the site it analyzed, and it may send an email once it has finished working on a particular site, keeping the client continuously updated on the progress of the analysis, impriving monitoring and error handling.

One solution that can balance the trade-off between accuracy and execution time and lead to maximum results in both areas is to have multiple robots working on the same process. Currently, only one robot executes the process. Inserting multiple bots requires more coordination between them, but it would lead to exponential improvements in execution times as there would be more users parsing the same input. Starting with an input file with the different sites to be analyzed, the first bot would start extracting the various sub-links and related cookies from the first one, assigning the row the value of "working." The second bot, seeing that the first site is already being processed, would go directly to the analysis of the second one, and so on. This approach would be like hiring more people to speed up the whole process. The level of accuracy would remain the same, but the execution time would improve because more data can be handled in less time.
To accomplish this, an efficient organization must be established, leveraging all bots (otherwise, the bot license would be paid unnecessarily) and assigning the Orchestrator to handle the functions. The UiPath Orchestrator is a centralized platform that manages and monitors all the different bots within an organization. It provides a single point of control and visibility for all bots, enabling users to manage and monitor them in a unified way. When multiple bots work on the same process, the Orchestrator ensures that they work together in a coordinated manner by providing functionalities such as queue management, resource allocation, load balancing, error handling, reporting, and analytics. These functionalities ensure that the bots work together in a coordinated and efficient manner, improving the overall performance of the process.

This project offers only a material tool with the objective of helping companies to act in compliance with the correct values and principles regarding privacy. It has been seen in previous chapters how this is a very broad, nuanced topic, characterized by an era of change and innovation, which leave little room for reasoning and at the same time multiply the stimuli and areas in which work needs to be done. Hopefully in the future there will be more and more regulations to protect this. Governments must continue to create and enforce data protection regulations so that companies are responsible for collecting, processing, and sharing user data. Another approach to privacy protection is the principle of ”privacy by design,” which involves incorporating privacy considerations into the design of digital systems and products from the outset. Education of the individual concerned, regarding privacy and data protection topics, also becomes crucial. Many people are unaware of the extent to which their personal data is collected and used, and do not understand the risks involved. By providing consumers with clear information about their rights and options, and by promoting greater awareness of privacy issues, we can help to create a more informed and privacy-conscious society. New technologies will need to be harnessed to protect the consumer, for example by creating a decentralized, tamper-proof ledger of data transactions, blockchain and other technologies could provide a more secure and private way to store and share sensitive information.

Overall, progress is being made in the digital area about privacy, but there is still a long way to go. Continued efforts in the areas mentioned above will help to ensure that users’ privacy is protected in the digital space.

6 Conclusions

The objective of this work is to provide an overview of the world of privacy and its current regulations, and how it is evolving alongside Western society, including the adaptations, changes found in the literature, and new provisions to be implemented. The concept of privacy is broad, filled with uncertainties in providing definitions and establishing boundaries. The literature has sought to establish principles and concepts that can be linked to the concept of privacy, determining what is included and what is not. The difficulty lies in framing privacy in this new digital era, characterized by continuous and rapid changes imposed by technology or humans themselves, situations in which it is challenging to establish limits on what can be shared and what cannot. It is a hybrid concept, full of nuances, but it is important to analyze because it is part of human rights and forms the basis for their drafting, in order to respect personal sphere and inviolability.

Large institutions are working to provide tools that can solve various problems, trying to set limits and specific rules to ensure that the rights of all parties involved, from individuals to large organizations, are respected, while also guaranteeing development and innovation without excessive limitations.

Therefore, three different regulations have been analyzed, which are part of the European strategy aimed at protecting the fundamental rights of data subjects while allowing the development of markets and exchanges. The GDPR establishes rules and guarantees for the processing of personal data by public and private entities in order to protect privacy and individuals' rights. The Digital Services Act aims to create a safer, fairer, and more transparent online environment, protecting users from illegal or harmful content, defining the responsibilities and obligations of online platforms that offer intermediary services, promoting freedom of expression and content diversity, and ensuring cooperation between national authorities. The Digital Markets Act addresses abuses of dominant position by large online platforms acting as "gatekeepers" between businesses and users. The Digital Markets Act establishes a set of clear rules for platforms, prohibiting unfair or anti-competitive practices. These three measures represent an important step towards creating a competitive, innovative, and respectful European single digital market that respects the fundamental rights of users and businesses.

These regulations have been analyzed, describing the applicable principles and rules, the benefits they can bring, but also their limitations. Special attention has been given to the two sides of the coin: consumers and organizations. These regulations must ensure the balance of interests between these two parties, aiming to promote protection and sharing, in order to foster collaboration instead of creating competition.

Most of the obstacles have been raised by the advent of these new technologies that collect data and influence the way of life. However, it is important not to see these new tools as enemies but rather to harness them to achieve better goals and objectives. For this reason, this work proposes a bot, a tool that belongs to robotics, which can help large companies comply with the new rules they must adhere to. The bot successfully collects all cookies from various websites, allowing the human operator to verify which ones are GDPR compliant and which are not, avoiding penalties and, above all, respecting the rights of the data subject, their privacy, and personal data. If more tools of this kind were implemented, enabling technology to assist humans, it would be much easier for companies to adapt to new regulations, which may initially appear rigid and difficult to comply with.

There are still many objectives to be achieved, and it is crucial to involve everyone by disseminating current and up-to-date information, in order to avoid information asymmetry that only leads to confusion. These regulations must also be implemented, and there must be a commitment on the part of institutions to expedite processes and set aside personal interests. Progress has been made; for example, recently the European Parliament adopted its negotiating position on a proposed law, the Data Act, which harmonizes rules on fair access to and use of data generated in the EU across all economic sectors. Its aim is to facilitate data sharing and valorization in line with EU norms and values, and introduce rules on the use of data generated by devices connected to the Internet of Things.

European regulations such as the GDPR, the Digital Services Act, the Digital Market Act, and others are significant steps towards creating a secure, fair, and transparent digital space for citizens and businesses. However, these rules must be constantly updated and effectively enforced to address the challenges and opportunities of technological transformation. Only in this way can Europe ensure digital sovereignty based on its values and respectful of human rights.

References

[1] Solove, D. J. (2002). Conceptualizing privacy. *California law review*, 1087-1155.

[2] Smith, R. E., & Site, B. F. S. W. (2000). Privacy and Curiosity from Plymouth Rock to the Internet. *Privacy Journal.*

[3] Barbas, S. (2015). *When Privacy Almost Won: Time*, Inc. v. Hill. U. Pa. J. Const. L., 18, 505.

[4] Godkin, E. L. (1880). *Libel and its legal remedy.* J. Soc. Sci., 12, 69-80.

[5] Posner, R. A. (1983). The economics of justice. *Harvard University Press.*

[6] Posner, R. A. (2014). *Economic analysis of law.* Aspen Publishing

[7] Lehman, B. A. (1995). Intellectual property and the national information infrastructure: The report of the working group on intellectual property rights. *Washington, DC: Information Infrastructure Task Force.*

[8] United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989)

[9] Locke, J. (1980). John Locke Second Treatise of Government (1690). Edited and introduced by CB McPherson. Indianapolis, IN: Hackett.)

[10] Paul Freund, AMERICAN LAW INSTITUTE, 52ND ANNUAL MEETING

[11] Inness, J. C. (1992). *Privacy, intimacy, and isolation.* Oxford University Press, USA.

[12] Smith, H. J., Dinev, T., & Xu, H. (2011). *Information privacy research: an interdisciplinary review.* MIS quarterly, 989-1015.

[13] Warren, C., & Laslett, B. (1977). *Privacy and secrecy: A conceptual comparison.* Journal of Social Issues, 33(3), 43-51.

[14] Zwick, D., & Dholakia, N. (2004). *Whose identity is it anyway? Consumer representation in the age of database marketing.* Journal of Macromarketing, 24(1), 31-43.

[15] Chellappa, R. K. (2008). *Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security.* under submission, 13.

[16] Camp, L. J. (1999). *Web security and privacy: An American perspective.* The Information Society, 15(4), 249-256.

[17] Belanger, F., Hiller, J. S., & Smith, W. J. (2002). *Trustworthiness in electronic commerce: the role of privacy, security, and site attributes.* The journal of strategic Information Systems, 11(3-4), 245-270.

[18] DeVries, W. (2003). *Protecting privacy in the digital age.* Berkeley Technology Law Journal, 18(1), 283-312.

[19] Romansky, R. (2019). *A survey of informatization and privacy in the digital age and basic principles of the new regulation.* International Journal on Information Technologies and Security, 1(11), 95-106.

[20] Bélanger, F., & Crossler, R. E. (2011). *Privacy in the digital age: a review of information privacy research in information systems.* MIS quarterly, 1017-1041.

[21] Berman, J., & Mulligan, D. (1998). *Privacy in the digital age: Work in progress.* Nova L. Rev., 23, 551

[22] Bansal, G., & Gefen, D. (2010). *The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online.* Decision support systems, 49(2), 138-150.

[23] Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, M. H. C. (2017). *Cross-Cultural Privacy Prediction.* Proc. Priv. Enhancing Technol., 2017(2), 113-132.

[24] Milberg, S. J., Smith, H. J., Burke, S. J. (2000). *Information privacy: Corporate management and national regulation.* Organization science, 11(1), 35-57.

[25] Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). *Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities.* European journal of information systems, 19, 181-195.

[26] Miltgen, C. L., & Peyrat-Guillard, D. (2014). *Cultural and generational influences on privacy concerns: a qualitative study in seven European countries.* European journal of information systems, 23(2), 103-125

[27] Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). *A multinational study on online privacy: global concerns and local responses.* New media society, 11(3), 395-416.

[28] Tzanou, M. (2013). *Data protection as a fundamental right next to privacy? 'Reconstructing'a not so new right.* International Data Privacy Law, 3(2), 88-99

[29] Lynskey, O. (2014). *DECONSTRUCTING DATA PROTECTION: THE 'ADDED-VALUE' OF A RIGHT TO DATA PROTECTION IN THE EU LEGAL ORDER.* International Comparative Law Quarterly, 63(3), 569-597

[30] Gellert, R., & Gutwirth, S. (2013). *The legal construction of privacy and data protection.* Computer Law Security Review, 29(5), 522-530.

[31] Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). *The critical success factors of GDPR implementation: a systematic literature review.* Digital Policy, Regulation and Governance, 21(4), 402-418.

[32] Voigt, P., & Von dem Bussche, A. (2017). *The eu general data protection regulation (gdpr).* A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10(3152676), 10-5555.

[33] Mondschein, C. F., & Monda, C. (2019). *The EU's General Data Protection Regulation (GDPR) in a research context.* Fundamentals of clinical data science, 55-71.

[34] Voss, W. G. (2016). *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting.* The Business Lawyer, 72(1), 221–234.

[35] Wolters, P. T. J. (2018). *The control by and rights of the data subject under the GDPR.*

[36] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers security*, 64, 122-134.

[37] A. Acquisti, J. Grossklags *Privacy and rationality in individual decision making IEEE Secur. Priv.*, 3 (1) (2005), pp. 26-33.

[38] Sultan, F., Rohm, A.J. and Gao, T. (2009), *"Factors influencing consumer acceptance of mobile marketing: a two-country study of youth markets"*, Journal of Interactive Marketing, Vol. 23 No. 4, pp. 308-320.

[39] Hann, I., Hui, K., Lee, S.T. and Png, I.P.L. (2007), *"Overcoming online information privacy concern: an information-processing theory approach"*, Journal of Management Information Systems, Vol. 24 No. 2, pp. 13-42.

[40] Peltier, J.W., Milne, G.R. and Phelps, J.E. (2009), *"Information privacy research: framework for integrating multiple publics, information channels, and responses"*, Journal of Interactive Marketing, Vol. 23 No. 2, pp. 191-205.

[41] Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. (2011), *"The effect of online privacy information on purchasing behavior: an experimental study"*, Information Systems Research, Vol. 22 No. 2, pp. 254-268.

[42] Lindgren, P. (2016). *GDPR regulation impact on different business models and businesses.* Journal of Multi Business Model Innovation and Technology, 4(3), 241-254.

[43] Todt, K. E. (2019). *Data Privacy and Protection: What Businesses Should Do.* The Cyber Defense Review, 4(2), 39–46.

[44] Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8.

[45] Garber, J. (2018). GDPR–compliance nightmare or business opportunity?. *Computer Fraud Security*, 2018(6), 14-15.

[46] Bergemann, D., Bonatti, A. (2015). Selling cookies. *American Economic Journal: Microeconomics*, 7(3), 259-294.

[47] Cahn, A., Alfeld, S., Barford, P., Muthukrishnan, S. (2016, April). *An empirical study of web cookies.* In Proceedings of the 25th international conference on world wide web (pp. 891-901).

[48] Hormozi, A. M. (2005). Cookies and privacy. *Information Security Journal*, 13(6), 51.

[49] Kretschmer, M., Pennekamp, J., Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)*, 15(4), 1-42.

[50] Cookies, the GDPR, and the ePrivacy Directive - GDPR.eu. (s.d.). GDPR.eu. `https://gdpr.eu/cookies/`

[51] Cookie walls — EDPB guidelines on cookie walls and valid consent. Retrieved from https://www.cookiebot.com/en/cookie-walls/.

[52] Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). *We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy.* arXiv preprint arXiv:1808.05096..

[53] What is Robotic Process Automation - RPA Software — UiPath. (s.d.). AI-powered UiPath Business Automation Platform™ - Leader in RPA automation — UiPath. https://www.uipath.com/rpa/robotic-process-automation

[54] Chary, Y., RPA with UiPath: A Practical Guide.

[55] Technologies, H. (2022, 21 March). A Complete Guide To Uipath ReFramework. Medium. https://hashstudioz.medium.com/a-complete-guide-to-uipath-reframework-f76bbac04f86

[56] What Is SQL Database? - IT Glossary — SolarWinds. (s.d.). IT Management Software and Observability Platform — SolarWinds. https://www.solarwinds.com/resources/it-glossary/sql-database#:~:text=SQL%20database%20or%20relational%20database,%2C%20update%2C%20and%20retrieve%20data.

[57] UiPath Selectors: Best Practices For UiPath Automation 2023. (s.d.). RPA Tutorial. https://rpatutorials.com/uipath-selectors-best-practices-for-automation/

[58] How many types of selectors are in UiPath? (s.d.). SOAIS. https://www.soais.com/what-are-selectors-in-uipath/#:~:text=What%20is%20a%20selector%3F,wnd%2Dcls

[59] (s.d.) https://docs.uipath.com/orchestrator/standalone/2023.4/user-guide/business-exception-vs-application-exception

[60] How to Comply with Cookie Laws using OneTrust Cookie Consent Module. (s.d.). Specbee. https://www.specbee.com/blogs/how-comply-cookie-laws-using-onetrust-cookie-consent-module

[61] (s.d.) https://docs.uipath.com/orchestrator/standalone/2023.4/user-guide/about-assets

[62] Error handling with UIPath try-catch and retry scopesF-PenIT blog. (s.d.). F-PenIT blog. https://penrako.com/eng/uipatherrorhandling/#:~:text=If%20an%20exception%20occurs%20during,is%20located%20in%20Workflow%20%3E%20Control.&text=The%20retry%20scope%20consists%20of,and%20(2)%20condition%20blocks.

[63] *The Digital Markets Act: more choice and improved data protection for users?* Eipa. https://www.eipa.eu/blog/the-digital-markets-act-more-choice-and-improved-data-protection-for-users/

[64] *Press corner* . European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

[65] Cauffman, C., Goanta, C. (2021). A new order: the digital services act and consumer protection. *European Journal of Risk Regulation*, 12(4), 758-774.

[66] Madiega, T. (2021). Digital markets act.

[67] Bauer, M., Erixon, F., Guinea, O., Van der Marel, E., Sharma, V. (2022). The EU Digital Markets Act: Assessing the Quality of Regulation. *Europan Centre For International Political Economy*

[68] The Digital Markets Act – Key Enforcement Principles . *Competition Policy International.* https://www.competitionpolicyinternational.com/the-digital-markets-act-key-enforcement-principles/

[69] *The EU's Digital Markets Act: What Does It Mean for Businesses and Data Privacy?* Orrick - Homepage. https://www.orrick.com/en/Insights/2022/11/The-EUs-Digital-Markets-Act-What-Does-It-Mean-for-Businesses-and-Data-Privacy

[70] Crawford, G., Juhan, J., Kempe-Muller, S., Kirk, D., Kjolbye, L., Righini, E., Volcker, S., Leigh, B., Wan, V., Smyth, A., The Digital Services Act: Practical Implications for Online Services and Platforms, (2023), Lathman & Watkins

[71] trusted flagger Definition — Law Insider. Law Insider. https://www.lawinsider.com/dictionary/trusted-flagger#:~:text=Let's%20do%20it!,Sample%201Sample%202

[72] Senftleben, M., & Angelopoulos, C. (2020). The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act:

Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market. Amsterdam/Cambridge, October.

[73] What is a Recommendation System?. NVIDIA Data Science Glossary . URL: https://www.nvidia.com/en-us/glossary/data-science/recommendation-system/

[74] EU Digital Markets Act and Digital Services Act explained — News — European Parliament. URL: https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained

[75] Who are the gatekeepers under the EU's Digital Markets Act?. Taylor Wessing . URL: https://www.taylorwessing.com/en/interface/2022/the-eus-digital-markets-act/who-are-the-gatekeepers-under-the-eus-digital-markets-act

[76] Digital Services Act: Questions and Answers — Shaping Europe's digital future. Shaping Europe's digital future — Shaping Europe's digital future . URL: https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers

[77] Contributors to Wikimedia projects. Anti-circumvention - Wikipedia. Wikipedia, the free encyclopedia . URL: https://en.wikipedia.org/wiki/Anti-circumvention

[78] Data protection by design and by default: new guidelines . (b. d.). UK and International Law Firm — Penningtons Manches Cooper. https://www.penningtonslaw.com/news-publications/latest-news/2020/data-protection-by-design-and-by-default-new-guidelines

[79] La Figura del DPO: Chi e Cosa Fa . (b. d.). PrivacyLab. https://www.privacylab.it/IT/163/Cosa-fa-il-Data-Protection-Officer-%28DPO%29%3F/

7 Summary

7.1 Introduction

The digital age encompasses a broad range of technological advancements, which include virtual environments, digital services, intelligent applications, machine learning, and knowledge-based systems. These innovations shape the distinctive characteristics of our contemporary world, such as globalization, e-communications, information sharing, and virtualization.

This paper aims to inform on the current privacy literature by providing general definitions and analyzing dissenting opinions, regulations to be adopted, and stakeholders, to the point of providing a technological tool that can help balance the technological and privacy worlds.

The goal of this project is therefore to provide an overview of privacy, analyzing, as much as possible given the vastness of the topic, its nuances. Finally, to provide a tool that can ease the technological transition toward respecting the rights of the individual.

In the first chapter, the literature of privacy is studied, its history and various definitions, interpretations and influences are reported while also examining privacy within the context of technology and innovation. The General Data Protection Regulation, Digital Services Act and Digital Markets Act are then introduced and explained.

In the second chapter, the point of view of the two key players in today's landscape is presented: consumers and businesses in relation to the advent of those new regulations. An overview of the cookies technology is then given.

Finally, in the third chapter, the robot is described, how it works, how it was designed, results achieved, and minutiae for improvement while verifying cookies compliance with the GDPR.

7.2 Privacy and Regulations

Privacy is a concept that has been studied for many years, well before the advent of new technologies in this digital age. It is a broad concept that encompasses several subjects and areas, which many scholars have not yet been able to define.

Daniel J.Solove defines privacy as a "sweeping concept", an all-encompassing concept that includes various aspects, such as: the freedom of thought, autonomy over one's body, seclusion within one's dwelling, authority over personal information, freedom from monitoring, safeguarding one's reputation, and shielding oneself from

invasive searches and interrogations. Arthur Miller has expressed his opinion that privacy is a challenging notion to define because it is remarkably ambiguous and elusive. In his paper, Daniel J. Solove summarizes the concept of privacy under six headings: (1) the right to be let alone (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy [1].
To establish a more precise framework for the concept of privacy, it is essential to consider the historical reference period and socio-cultural context. Jeff Smith et al. write about four periods of privacy development: (1) Privacy Baseline (1945-1960); (2) First Era of Contemporary Privacy Development (1961-1979); (3) Second Era of Privacy Development (1980-1989) and (4)Third Era of Privacy Development (1990-present).[12]

Despite the many definitions of privacy, it is worth clarifying what Smith et al. define "What Privacy Is Not": (1) Anonymity, (2) Secrecy, (3) Confidentiality, and (4) Security.[12]

In this framework, it is worth mentioning the concept of information privacy, which is a subset of the overall concept of privacy. Clarke defined information privacy specifically as *"the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves"*[20]. The issue about redefining privacy in the digital age is fundamental to all policy, legal and cultural discussions, because the new growth of data we are facing needs to be addressed. Jerry Berman and Deirdre Mulligan highlight three significant digital advancements that significantly impact privacy. These include: (1) the increase of data generation and the consequential accumulation of extensive amounts of personal data, caused by the recording of nearly every modern interaction; (2) the globalization of the data market and its accessibility for anyone to compile and scrutinize this data; and (3) the inadequacy of control mechanisms for digital data that previously safeguarded analog data[21].

Smith et. al highlight other factors that shape the view of privacy: experience, awareness, personality differences (such as extroversion, agreeableness, emotional instability, conscientiousness, and intellect[22]) and demographic differences. There are also behavioral factors to be taken into account, depending on the individual's actions during browsing on the Internet. In reference to that, trust has been playing an important role as a variable between privacy concerns and disclosure[12].

This work will mainly focus on the regulations and tools that protect data privacy within the European Union. However, it is important to note that there is not only a Western perspective. On the contrary, the concept of privacy and its implications can vary depending on where we are in the world. Although privacy regulation exists in almost every culture, the specific behavioral and psychological mechanisms that people use to regulate privacy boundaries are unique to each culture. For instance, users in Western countries tend to have a different perspective about how to classify personal data in respect to Eastern countries[23]. Li et al.suggest that specific design recommendations for privacy systems, data collection strategies, and privacy regulations should be developed in response to the international context[23]. Posey et al. and Miltgen et al. revealed that participants in focus groups from individualistic societies exhibited greater reluctance to reveal information compared to those from collectivistic societies. Likewise, Cho et al. found that Internet users from highly individualistic cultures exhibited greater concerns about online privacy and give more importance to privacy protection and customization than collectivistic countries[23].

Data protection appeared as an offspring of privacy and the two rights still seem inextricably tied up together. However data protection is trying to mark its own way in life. It is a relatively new concept that emerged with the rise of digital technologies and the collection and processing of personal data. The EU Data Protection Directive (DPD) sees data protection as the protection of *"the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"*. (Article 1 (1).) The ultimate goal of data protection is to promote fairness in the processing of personal data and, to some extent, fairness in the outcomes of such processing. To ensure this fairness, a set of principles, commonly referred to as 'fair information principles' or 'data protection principles', have been developed. These principles include collection and purpose limitation, data quality, data security, openness and transparency of processing, accountability, and individual participation.

There are ongoing debates regarding whether the right to privacy and the right to data protection should be considered as distinct and autonomous or whether the right to data protection is simply a subset of the right to privacy. Most literature tells us that these two rights are not identical; the right to privacy is considered by some to be a much broader concept. These two rights can be found in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The EU secondary legislation currently in place does not fully consider the fundamental right to data protection. Article 8 of the Charter establishes a distinction between data protection and privacy and outlines particular safeguards in paragraphs 2 and 3 [32]. These guarantees include processing personal data in a fair and specified manner based on consent or other lawful grounds; providing individuals with the right to access and correct data collected about them; and ensuring independent oversight of compliance with these regulations by an impartial authority. To the purpose of distinction of the rights, the Court differentiates between two types of data processing: those that pertain to an individual's private life and those that do not. This distinction is based on two criteria: the nature of the data being processed and the scope of the processing. Different opinions have also been formed regarding the scope of the two rights. Data protection is considered both narrower and broader than privacy.Similarly, privacy is both narrower and broader at the same time: it might apply to a processing of data which are not personal but nevertheless affects one's privacy, while it will not apply upon a processing of personal data which is not considered to infringe upon one's privacy. It can also be argued that the processing of personal data may have implications beyond privacy and affect other constitutional rights. [30][29] [19]

The European Union has introduced three new legislative measures aimed at regulating the digital market and services: the General Data Protection Regulation, the Digital Services Act, and the Digital Markets Act.
The General Data Protection Regulation (GDPR) is a comprehensive privacy law that came into effect in the European Union (EU) in May 2018. The GDPR replaces the outdated Data Protection Directive of 1995 and provides a modern and more robust framework for protecting personal data in the digital age. The GDPR is said to introduce a higher level of harmonization of data protection law throughout the European Union[31]; indeed the GDPR is applicable in every member state without the need for a national legislation implementation, unifying the European Union rules and laws. The objective of this regulation by the EU is to empower citizens with greater control over their personal data, strengthen their rights, change the way organizations handle and govern such information, and eliminate barriers to cross-border trade. As not only data protection duties but also the impending fines have been significantly increased, companies should carefully reorganize their internal data protection procedures in order to reach compliance with the GDPR. This regulation applies to anyone processing or controlling the processing of personal data. Given the exponential growth of data and its importance for business processes and objectives, companies will be affected. It gives several definitions, including the controller, processor, personal and sensitive data. The literature iden-

tifies the material and territorial scope of the regulation. With regard to the material scope, the GDPR applies to both public bodies as well as private organizations[32]. For what concerns the territorial scope, despite being a European Regulation, the GDPR's reach extends beyond the borders of Europe. Article 5 GDPR lays down the principles allowing for lawful processing of personal data. These principles are: (1) Lawfulness, Fairness and Transparency; (2) Purpose Limitation; (3) Data Minimisation; (4) Accuracy; (5) Storage Limitation; (6) Integrity and Confidentiality; (7) Accountability. There are legal bases of GDPR in order to be able to process personal data in a lawful manner, the two most important are: consent, legitimate interest of the controller or by a third party and compliance[33].

The Digital Services Act and Digital Markets Act aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. The digital package was created by the Commission to regulate and harmonize landmark rules concerning online platforms in the European Union[63].

The Digital Services Act is a policy document setting the policy goals to achieve in order to have an European strategy for data economy. The DSA introduces a new regulatory framework for online platforms. Its goal is to encourage them to fight objectionable content while respecting users' fundamental rights. It will indeed give better protection to users and to fundamental rights online, respecting the principles of accountability and transparency for online platforms, providing a unified framework across the EU. The key features of the Digital Services Act can be summarized in five points: (1) it is an asymmetrical regulation; (2) it preserves the exemption from liability established by the E-Commerce Directive in 2000, with additional clarifications; (3) it introduces new obligations for content moderation; (4) it incorporates provisions aimed at safeguarding users of online services and (5) it contains specific implementations and enforcement procedures[64]. The regulation is directly applicable and does not require a transposition law to be adopted by each Member State. The DSA introduces new measures that empower users to report unlawful online content, while enabling platforms to collaborate with designated "trusted flaggers" in order to detect and eliminate such content. This enables effective safeguards for users, as it includes a provision that grants users the right to contest content moderation decisions made by platforms. This is facilitated through mandatory disclosure of information to users when their content is removed or restricted, thereby providing them with an opportunity to challenge such decisions. Users will indeed have new rights, including the right to complain to the platform or their national authority. New rules are set to trace sellers on online marketplaces, to help build trust and go after scammers more easily. New measures for transparency for online platforms are set, including better information on terms and conditions, as well as transparency on the algorithms used for recommending content or products to users and many more implementations[64].

The purpose of the Digital Markets is to ensure equal opportunities for all digital companies, regardless their size. As stated in Article 1(1) of the regulation *"The purpose of this Regulation is to contribute to the proper functioning of the internal market by laying down harmonized rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users."* Particular attention is given to large platforms, the so-called "gatekeepers", whose specific definition is given in Articles 3 and 4 of the regulation. The reasons behind the stipulation of this document is to ensure a fair equilibrium in the digital market[66]. The DMA can be intended as an asymmetric regulation that targets the source of the problem, namely companies that enjoy an entrenched and durable position as a gateway for business users to reach end users; while also centralizing its enforcement through the Commission. Articles 5 and 6 of the DMA are really important, as they include a list of 'dos and don'ts' for companies that fall under the scope of the regulation[63]. Those companies must ensure openness of digital services and at the same time prevent unfair conditions on business and users alike. According to the European Commission, the DMA brings significant benefits to both business users and individuals. Smaller entrepreneurs and start-ups will have the opportunity to operate in a fairer environment, no longer solely reliant on gatekeepers to provide their services. This shift allows for increased innovation without the burden of unfair terms and conditions. For users, the DMA means a greater range of options to choose from and the ability to have greater control over the services they prefer. It will also be easier for users to explore alternative options beyond the confines of specific online platforms, leading to fairer competition and more competitive pricing, which in turn will stimulate the market[68].

7.3 Data Subjects & Organizations

One of the main goals of the GDPR is precisely to protect the data subject, in fact it provides tools that can give them more power and control regarding the processing of personal data.The regulation has a chapter dedicated to the rights of the data subject which will be listed below. Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) of

GDPR generally gives several rules, in order to facilitate the exercise of those rights by data subjects and controllers. The scope of Article 13 (Information to be provided where personal data are collected from the data subject) is to create a balance of information between the controller and the data subject. The scope of Article 15 (Right of access by the data subject) is to increase fairness and transparency of data processing, since it gives the data subject the opportunity to verify the lawfulness of processing activities performed on their personal data and enforce their position on their data. The scope of Article 16 (Right to rectification) is to correct or prevent negative effects on the rights and freedoms of the data subject. It is correlated with the principle of accuracy, according to which processed data, at any given time, should reflect reality. Article 17 of the GDPR establishes the right to erasure or right to be forgotten, which means that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her in certain circumstances. The Right to restriction of processing (Article 18) has the objective to balance at the same time the interest of the data subject and the controller: the latter can continue processing the personal data, while the data subject's security is increased by allowing rectification or erasure of their data. Article 20 introduces a new data subject right, the right to data portability, whose objective is to strengthen the data subject's control over its data where processing is carried out by automated means, by giving it the possibility to transmit its personal data from one controller to another. Pursuant to Article 21 (Right to object), data subjects may assert their right to object to the processing of personal data on grounds relating to their particular situation and to the processing of data for direct marketing purposes. The article provides three situations that can be grounds for an objection to processing. Overall there are some general points and ground rules that must be applied to every right listed in the GDPR. Where the right is exercised, the controller should act without undue delay and within a month of the right being exercised; the period can be extended up to two months where necessary, but it is necessary to give notice to the data subject[32].

When it comes to data, sensitive and otherwise, people often do not understand the value that this data has, particularly for companies that use it to target their campaigns, and they tend to "give it away" freely without worrying about the implications. The contradiction between individual's stated concerns about privacy and their actual behaviors when it comes to sharing information online is a phenomenon known as the "Privacy Paradox". On the one hand, people express a desire for privacy and express concerns about data breaches and identity theft. On the other hand, they continue to engage in behaviors that compromise their privacy[36][37].

The DSA brings several changes for online platforms, but which can give benefits not only to online platforms, but also to the users themselves, as their protection and the protection of their rights is increased. These rules will in fact create a safer online experience for citizens to freely express their ideas, communicate and shop online, by reducing their exposure to illegal activities and dangerous goods and ensuring the protection of fundamental rights. The introduction of this regulation grants users the acquisition of new rights, while also increasing their power of control. They will in fact be able to be a participant in the notification of illegal content and be informed the moment their content is removed, which decision they can challenge. Transparency towards users will increase, allowed by a continuous exchange of information.

While, as the DMA proposal mentions, its scope is rather broad, dealing with practices generally "unfair" to the consumer. Several obligations for gatekeepers are listed in Article 5, regarding the collection and combination of personal data according to the users' consent. Some concerns have been brought up regarding the implications on the GDPR's purpose limitation principle [66]. Also, the EPRS states that DMA also seems to have a broader scope than the GDPR's right to data portability and would ensure additional forms of portability, including portability of non-personal data for business users and real-time and continuous portability[69]. However, the implementation of data portability runs into a number of technical, legal and economic obstacles.

From the organizations' point of view, the DSA aims at regulating the activities of intermediary services, and three different services are identified: a mere conduit service, a catching service and a hosting service. The DSA imposes certain key obligations applicable to all intermediary services[70]. The key areas for consideration are: transparency reporting, appointment of points of contact and legal representatives, updates to terms and conditions, content moderation policies and takedown orders and additional cumulative obligations for very large online platforms (VLOPs) and providers of hosting services and online platforms. Article 14 ensures that providers enhance transparency towards users in their terms and conditions. DSA also imposes further cumulative obligations for providers of hosting services listed in Article 15, Article 16, Article 17, Article 18. In addition to the obligations listed above, providers of online platforms are subject to a number of additional cumulative obligations, as stated in Section 3 of the regulation which can be found in Article 20, Article 21, Article 22, Article 23, Article 24 and Article 26. Very large online platforms are also subject to additional obligations[70].

The DMA requires gatekeepers to comply with a set of obligations and prohibitions within six months of their designation as gatekeepers. According to Article 5, there is a list of requirements directly applicable to gatekeepers, regarding parity clauses, processing and use of end-users' personal data, anti-steering, transparency and issues of non compliance; Articles 6 and 7 impose on gatekeepers a list of requirements that may need to be specified [66].

The introduction of the GDPR has compelled companies to restructure their business systems to comply with the imposed standards. However, like any change, adhering to the GDPR regulation yields benefits for companies, as well as new obstacles to overcome and thus the goal of achieving these goals by adopting new solutions. A research conducted by Peter Lindgren (2016) highlighted that business had to face increasing costs due to more procedures to implement, such as *"more procedures – more value chain functions to be carried out, more technology and software necessary to be bought, more hours spend by HR to live up to the necessary GDPR requests, change in organizational procedures and structures together with implementation of new culture."*[42] In order to be able to demonstrate compliance with the GDPR, the data controller should implement measures, which meet the principles of data protection by design and data protection by default. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities (DPA) is required for high risks. Ensuring robust privacy protection protocols for data is a crucial function for any organization that handles data, especially when sensitive data such as personal information is involved. According to Kiersten E. Todt, there are three critical elements of a comprehensive business data protection plan: (1) Data inventory; (2) Public projection of data privacy and protection policies; and (3) Incident response. Colin Tankard highlights another problem: the increase of the cost in order to assure compliance with the GDPR. Due to this fact, many are worried about the impact of the regulation[43]. One of the fundamental principles that companies must incorporate into their core values is transparency. They must be able to provide clear descriptions of how they collect data, why they do it, and how they intend to store and process it. This also includes providing information about third parties with whom data is shared and for how long. Additionally, companies must provide more control to users regarding the actions taken on their data, such as by providing a copy of their data. The GDPR empowers users in this regard. Opinions on this new regulation are varied and divided. Some fear for businesses, especially small and medium-sized ones, due to the possible costs and difficulties in carrying out accurate targeting and segmentation operations with the new restrictions. However, many positives have also been identified. The main advantage of complying with GDPR is the establishment of trust. Another significant benefit is the improvement and refinement of decision-making practices. GDPR's greatest achievement is the clarification of key terms regarding the user/company relationship in terms of personal data use. This clarification has resulted in basic definitions of the rights and responsibilities of the involved parties, providing a proper map of what is permitted and prohibited. GDPR emphasizes the importance of a well-organized, impenetrable, and highly regulated security framework.; it provides clear and realistic guidelines on how to improve the security system and how to maintain it. [42]

The most prevalent technology to enable the collection and resale of individual-level information is based on cookies and related means of recording browsing data. These tools are capable of recording user movements and histories, and organizations collect all this information. Web cookies were invented in 1994 as a mechanism for enabling state to be maintained between clients and servers. A cookie is defined as "a text string that is placed on a client browser when it accesses a given server."[47] By accessing the data stored in the cookie file, the server can identify the user. This technique of monitoring user activity was originally intended to benefit the user, as saving user information could lead to more efficient and personalized visits in the future. Cookie uses have since grown far beyond their original intention and have become a very controversial issue. Users believe that their privacy is being violated, with the progression of cookie functions moving beyond basic user customization and personalization. Each cookie has several attributes: Name, Value, Host, Path, Expires, Secure, HttpOnly and the Domain[47]. In addition to their attributes, cookies can be divided into several categories. First distinction is between functional and non functional cookies[49]. Then different types of cookies can be categorized: Strictly necessary cookies, Preferences cookies, Statistics cookies and Marketing cookies[50]. For what concerns the provenance, cookies are divided between first-party cookies and third-party cookies[50]. There is also a distinction between persistent and session cookies[49].
The tool used to allow users to accept or reject the use of certain cookies on a site, or to inform them about the site's privacy policy is usually a popup, known as cookie banner. Three common types of banner are identified, ordered by an increasing

amount of control provided to the user. The Type 1 banner is also called "cookie walls". It only informs users that cookies are used, and enables them to click "Accept" to express consent. The second type of banner (Type 2) is the binary banner, and it offers users the possibility to reject cookies. The third banner (Type 3) is the multiple-choice banner[49].
When cookies were first developed, there were no intentions of using them as the type of spy mechanism they have the reputation of today. Cookies provide a variety of advantages for users, web developers, and marketers. Cookies allow users to save numerous items, as well as quantities, colors, and sizes in their shopping cart until they are ready for check-out. Cookies can also be used to store information about user interests. This enables the store to offer similar products that the user may like according to previous purchases. Advertisers and marketers also use the interests determined through cookie usage to select which advertisements will be most effective for a particular user. The more information a user provides, the more cookies can assist the user in finding the information or products desired. Web developers use cookies for statistical purposes. They can track how many visitors arrive, how often a visitor returns, and how many are new visitors versus repeat visitors. Some disadvantages highlighted in the literature are: the visitor counts can often be inaccurate or ineffective and that could influence statistical research; there is also a growing concern by users that perceive cookies as an invasion of privacy, since information is taken without their consent[48][49].

7.4 Enhancing Compliance with Bot Technology

The objective of this work is to provide a tool that can help companies comply with the principles of the GDPR. The creation of a bot would in fact bring various benefits, from saving time and costs to reducing errors. It is important to note that this tool is not intended to replace human involvement, as an understanding of the law and the rights guaranteed by regulations is necessary. Instead, it is designed to facilitate the compliance process. The bot has been programmed using UiPath, a platform which is part of the technologies used for Robotic Process Automation (RPA) technologies.

Robotic Process Automation (RPA) is a cutting-edge technology that uses software robots to automate repetitive, rules-based tasks by emulating human actions[53]. This technology is revolutionizing the way businesses operate, as it enables automation of tasks that were previously performed by humans, freeing them up to focus on more complex and higher-value tasks. The adoption of RPA technology provides organizations with numerous benefits, including increased efficiency and accuracy, reduced costs, improved compliance, improved customer service, data gathering and analysis, scalability, process consistency, and increased flexibility. With robots capable of working 24/7 with little or no human supervision, automations can run more frequently and with higher accuracy, providing significant cost savings, improved quality of products or services and the reduction of human errors. Furthermore, RPA robots can work with sensitive data without the risk of human error, enhancing data security and regulatory compliance[54].

UiPath is one of the most popular software platforms, providing a wide range of automation tools and capabilities for businesses to automate their processes. The platform is made up of several components, including UiPath Studio, UiPath Robot, and UiPath Orchestrator. The UiPath platform is user-friendly, with a drag-and-drop interface that simplifies the process of creating and deploying automations. UiPath also offers a broad range of pre-built activities and templates, making it easy for users to begin automation projects[54].

The project arose from the need to have a tool that would allow for continuous monitoring of cookies on all websites in the domain, facilitating the compliance with the regulations. The bot's programming focused on mimicking the behaviors of the normal individual when browsing a website. Given the vast amount of material to be verified (150 sites with all the sub-links for each site), the adoption of a technological robotics tool seemed an excellent solution, since repetitive and mechanical actions have to be carried out, and even a small human error can lead to serious consequences. Therefore, given a list of 150 websites as input, all cases of cookie acceptance were considered: the decision to click on "accept all cookies," "reject all cookies," and the selection of statistical, analytical, marketing cookies etc. For each type of cookie selected, the latter is collected from the Chrome console and saved in a database, so that the company can complete the verification, and check that there are no "misplaced" cookies, which would result in a very high administrative penalty, as required by the GDPR.
The first step was to confront the company operator and understand what actions he usually carried out. Therefore, an AS-Is and TO-BE analysis has been carried out. For this project, the Robotic Enterprise Framework was used. Different activities are utilized in the workflow for the robot to perform the desired functions. Some of these are Try Catch, Click, Check App State, Use Application/Browser, Keyboard Shortcuts, Connection to DataBase among others. The SQL Database was used

for storing and retrieving data. The general process starts with the "Initialization" block, where the configurations and input files are read, and the applications that will be used in the process are initialized. Next, the RCODE of the specific operation is defined, which includes a datetime string in the format “yyyyMMddHHmmss” to generate a unique code associated with a specific date and time. This allows for diversification of the operations since no two will be executed at the same time. The referenced code is then saved in the SQL database via an INSERT query in the column, and other columns used later in the analysis are created too. The client provides a list of all the sites to be browsed by the bot, which is saved in an Excel file. The bot reads this file and saves all the sites in a variable and checks if there are no missing values. After all initial configurations and settings are set, the process begins. The bot cycles through each site and performs the desired actions. First, the ScreamingFrog application is opened using the Use Application/Browser Activity, the bot writes the current URL in the search bar, and it begins to scan all the sub-links. Once it is verified that the status code is valid, the URL is considered "imported" and the list of sub-links is exported to an Excel file and then to a CSV File. After performing the scan and saving all URLs, navigation for each site on Google Chrome begins. Cookies are collected according to three categories, with an array defined to contain the values "ALL," "Selected," and "DEFAULT." Before browsing begins, the cache is cleared because browsers such as Chrome store some information about websites in their cache and cookies. Navigation of the first URL then takes place. When the website is opened, the bot must identify the version of the banner present. Identifying the banner is crucial, as each version has unique buttons that require different approaches to navigate. Once identified, the bot creates a datatable to store all selectable buttons (switches) present on the screen. This datatable will be used in a second round to select buttons and save detected cookies; the bot indeed creates a datatable to store all IDs of the buttons detected while scanning the banner. Afterward, the bot accepts the cookies by clicking on the "accept" button. If the banner is not identified, the information will be saved in the database, with the attribute "NO BANNER". Next, the bot opens the Chrome Console and saves all the cookies and its information; then it continues the extraction on the other sub.links, navigating the web. One important step, however, is to have the bot click on the "Clear all cookies" button to avoid that while browsing, cookies belonging to the previous site are also detected in the next, making the analysis incorrect. The bot is able to collect all combinations of cookies, selecting each time the different buttons (Accept all, Reject all, only analytical cookies, both preferences cookies and marketing cookies etc.), storing all the information in the database. Then the process ends; and depending on the customer's request, it will be restarted, or it will work uninterruptedly if it is given continuous input data flows. To verify cookies compliance, a software platform called OneTrust is used. OneTrust is in fact able to scan all sites and identify which cookies are in use. A comparison is then made between the list of cookies and those identified during the scan; any discrepancies between the two lists may indicate cookies that are not compliant with GDPR. For large organizations, the bot proves to be a very useful tool, as it can handle decentralized organizations, harmonizing the processes. The bot is a tool that would help reduce maintenance and monitoring costs and the data stored can also be used as historical evidence in case of comparison with the privacy authority.

The bot took an average of 1.6 minutes per site to detect the different cookies, and processing times for the 10 sites averaged 4 hours per site (including sub-links, which on average are 200 per site), totaling 40 hours (on average) or slightly over a day to complete the process (1,667 days). These results can be achieved when the robot is able to work unattended, without human supervision, and can work 24/7. The project results can be evaluated based on its efficiency, timing, and error reduction. Some adjustments can still be made to implement the bot's performance, such as: improving security in storing personal informations and credentials; a multiple check on the recognition of the elements to increase consistency; implement the correct definition of variables to guarantee greater accuracy; handle application shutdown; o leverage the functions of the Dispatcher and the Performer; send an email once the process finishes or if an error occurs, increasing the flow of information exchanged and bring the project to another level by dividing the work between different bots, all managed by the orchestrator, with the objective to increase accuracy while at the same time reduce the execution times.

7.5 Conclusions

The objective of this work was to provide an overview of the world of privacy and its current regulations, and how it is evolving alongside Western society, including the adaptations, changes found in the literature, and new provisions to be implemented. The literature has sought to establish principles and concepts that can be linked to the concept of privacy, determining what is included and what is not. Large institutions are working to provide tools that can solve various problems, trying to set limits and specific rules to ensure that the rights of all parties involved, from individuals to large organizations, are respected, while also guaranteeing development and innovation without excessive limitations. Therefore, three different regulations have been analyzed, which are part of the European strategy aimed at protecting the fundamental rights of data subjects while allowing the development of markets and exchanges: the General Data Protection Regulation, the Digital Services Act and the Digital Markets Act. These regulations have been analyzed, describing the applicable principles and rules, the benefits they can bring, but also their limitations. Special attention has been given to the two sides of the coin: consumers and organizations. These regulations must ensure the balance of interests between these two parties, aiming to promote protection and sharing, in order to foster collaboration instead of creating competition.

The work proposes a robot which can help large companies comply with the new rules they must adhere to. The bot successfully collects all cookies from various websites, allowing the human operator to verify which ones are GDPR compliant and which are not, avoiding penalties and, above all, respecting the rights of the data subject, their privacy, and personal data. There are still many objectives to be achieved, but progress has been made; these rules must be constantly updated and effectively enforced to address the challenges and opportunities of technological transformation. Only in this way can Europe ensure digital sovereignty based on its values and respect for human rights.