Sociology and Social Work Review
Volume 7 (Issue 1)/2023 | pp. 35-60


DOI: 10.58179/SSWR7103
https://globalresearchpublishing.com/sswr/


Evolution of Concepts of Privacy and Personal Data Protection under the Influence of Information Technology Development

Gianmarco, Cifaldi[a*]
[a] *University of Chieti-Pescara, Chieti, Italy*

Abstract
The preservation of privacy is inextricably linked to technical advancement: nowadays, modern science and technology make it quite simple to invade someone's privacy. The basic right to data privacy and the growing need for personal information collide as a result. The legislation must change to reflect these advances in order to guarantee the protection of privacy under the law. However, it is crucial to identify the underlying concepts pertaining to the concept of privacy.
In order to better comprehend the notion of privacy and discover a solution for how privacy may be properly safeguarded in the information society, the study's goal is to outline the historical evolution of privacy. In addition to providing a thorough explanation of the GDPR, the study makes an analysis of literature on the evolution of data protection and the effect of technological advancements on the evolution and emergence of the personal data protection.

Keywords*: personal data protection; GDPR; privacy; data processing; data storage.*

1. Introduction

Although it has always existed, privacy has not always been a legally recognized right. What is seen as private and what is protected as private by law might differ. In the past, privacy was mostly concerned with one's physical surroundings, such as their home or possessions. With the introduction of new technology and easier access to information, privacy concerns have expanded to encompass problems with the gathering, storing, and utilization of personal data.
According to a number of privacy scholars and the European Court of Human Rights, one of the biggest issues with legal privacy protection is that it is hard to offer a complete legal

[*]Corresponding author: Gianmarco Cifaldi. *E-mail: cifaldi@unich.it*

definition of the idea of privacy protection. The significance of privacy may be explained by the fact that it is increasingly threatened in an era of quick technological advancement in the information society. Privacy also has a very tight relationship to human dignity, freedom, and independence of the person.

The concept of privacy has been changing and developing throughout history. But what is seen as private varies depending on the time period, the community, and the person. There may also be a difference between what is regarded as private and what is legally protected as private (Solove, 2011). From a legal perspective, the Code of Hammurabi featured a section prohibiting entering someone's house, and Roman law also addressed the issue (Konvitz, 1966). The dichotomy between "private" and "public," which derives from the individual's innate to draw a boundary between himself and the outside world, is where the concept of privacy usually originates from. The boundaries between private and public vary depending on the era and culture at the time, which results in ongoing changes in what individuals regard to be private throughout time (Westin, 2003).

Because the person existed as a member of a community and privacy was not valued in the same way it is now, other community members constantly "monitored" the individual's private life. The transition of these rural areas into cities is related to the appearance of "genuine" privacy (Bratman, 2002). The way people lived throughout the 19th century underwent a metamorphosis. “As a result of new economic and social developments, and these changes also had an impact on privacy as physical and mental privacy began to diverge and develop in distinct directions” (Solove, 2011). As a result of urbanization, cities' populations began to increase, forcing residents to live in more crowded conditions. However, as they were no longer subject to the continual moral supervision of their village neighbors and their constant watchful eyes, citizens were able to experience a new kind of privacy. The emergence and expansion of (tabloid) newspapers, which provided a “fertile ground for rumors and photography” (Solove, 2011), was another significant shift (Bratman, 2002).

1. The evolution of the concept of privacy

1.1 Concept of privacy in its inception

The famous paper "The Right to Privacy," written by Louis Brandeis and Samuel Warren in 1890, is credited as being the first to introduce the modern notion of privacy. This development marked a significant turning point (Konvitz, 1966). The Right to Privacy by Warren and Brandeis, which was published in the Harvard Law Review in 1890, quickly gained recognition among legal historians as one of the "undisputed classics" and "most significant law review articles of all time" (Bratman, 2002). The authors of the research concluded that in order for the law to "meet the demand of society" and provide the complete protection of the person and the property, the law must adapt as political, social, and economic developments take place in society. They saw two developments as threats to privacy: technical advancement (namely, instantaneous photos) and newspaper gossip, which turned into a business (Bratman, 2002). In light of these developments, they were the first to call for “the recognition of the right to privacy as a distinct and universal right, one that offered protection against not the infringement of property rights but rather the sheer infliction of emotional anguish” (Konvitz, 1966). The right to privacy is described by the writers of this publication as "the right to be left alone" (Konvitz, 1966). Warren and Brandeis described an already-existing common law right as a "stepping stone to the right to be left alone" because it “allows people to choose how much of their thoughts, feelings, and emotions they want to share with others” (Bratman, 2002). The "inviolate personality"

served as this right's guiding premise (Bratman, 2002). The right to privacy essentially provided protection against the illegal disclosure of personal information, including "facts, feelings, and ideas" (Konvitz, 1966).

The right to privacy is described by the writers of this publication as "the right to be left alone" (Konvitz, 1966). Since that era, "the right to privacy had achieved universal acceptance, started to take shape, and in western nations, it had established itself as a fundamental human right" (Konvitz, 1966). Despite the fact that laws ensure privacy protection, there is disagreement on what really needs to be safeguarded and what privacy is. Many famous jurists have attempted to define privacy, but most of these definitions only focus on one part of it owing to its unfathomability and the ongoing evolution of the components that make up an individual's private sphere.

It is extremely challenging to identify the philosophical and sociological arguments for the right to privacy (and data protection), because they are always evolving in line with social and legal developments. The value of privacy, according to Post, "is so complicated, so intertwined in conflicting and contradicting aspects, so engorged with diverse and unique meanings, that I often despair whether it can be successfully handled at all" (Post, 2001). These fundamentally unclear understandings and definitions have an impact on how the public is seen. They are most likely reflected in uncertainty regarding the framework's applicability and operation in general, the relationship between privacy and a rapidly changing environment, the assessment of the relationship between privacy and other rights, with individual action, and its applicability in light of other social goals (Post, 2001).

1.2 Privacy and its philosophical ontology

For several reasons, people choose to expose their personal information. We occasionally divulge information about our identities, residences, social security numbers, job histories, and net worth in order to apply for loans, mortgages, or credit cards. Other causes include the need for comfort (confessions), or while conversing with medical professionals and legal professionals. Another important factor is that individuals accept or allow monitoring in order to preserve social order (for instance, it is considered absolutely normal to have cameras in governmental buildings, airports or banks to deter criminals).

In a court case, photography - a new technology at that time - had been employed to gather data and information about a person without their consent. Warren and Brandeis were writing about this case being first lawyers to analyze the case of data processing using methods that appeared due to rapid technological advancement (Bratman, 2002). Although technology, especially information and ICT, has advanced significantly, the fundamental idea of privacy changed not in a such radical manner. With a few exceptions, ideally a person should be able to choose between being open or remaining in "solitude, intimacy, anonymity, reserve," as stated by Professor Alan Westin (Westin, 2003). Others, like Solove, have pointed out the difficulty in defining privacy, admitting that it is a "conceptual jungle," and have suggested a more nuanced definition that decouples privacy from a fundamental human rights approach based on how privacy is viewed in the context of resolving particular issues (Solove, 2011).

According to Alan Westin three levels: political, sociocultural, and personal were identified by as having an impact on privacy standards (Westin, 2003). An important part of privacy is played by the individual: it may be thought of as a kind of "aura" that surrounds the person and serves as the boundary between them and the outer world (Westin, 2003). The boundaries of this aura differ from context to context and from individual to individual, thus an average standard needs to be derived from all of this

customized and shifting context and this standard can be legally protected (Westin, 2003). In addition to this dynamic environment, there have been many attempts over the past centuries to define privacy.

All of these definitions, though, have a flaw, as Daniel Solove noted in one of his articles: either their breadth is too limited or too broad (Solove, 2011). He emphasizes that this does not imply that the concepts are flawed; rather, the issue is that these authors conceptualize privacy in a traditional way, which leads to definitions that either only highlight a few aspects of privacy or are overly general and do not provide a precise understanding of its components (Solove, 2011). According to his six categories for these definitions, privacy is the right to be left alone, to have only limited access to oneself, to secrecy, to have control over one's personal information, to be considered a person, and to intimacy (Solove, 2011).

Our interest in privacy, says Israeli law scholar Ruth Gavison, "is tied to our worry over our accessibility to others: the amount to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the focus of others' attention (Gavison, 1980)." The withholding or suppression of information is one component of privacy, according to American lawyer and economist Richard Posner (Posner, Alan Westin and American professor Charles Fried must be recognized among the authors who view privacy as a control over personal information) (Posner, 1978).

While Fried said that "privacy [...] is the control we have over information about ourselves," (Fried, 1968), Westin described privacy as "the claim of a person to select whether information about himself or herself should be revealed to others (Westin, 2003)." According to American lawyer Edward Bloustein, privacy invasion is closely related to personhood, individuality, and human dignity (Bloustein, 1964). Privacy, according to American scholar Tom Gerety, is "the control over or the autonomy of the intimacies of human identification" (Gerety, 1977). The claim that "privacy is the right of the person to determine about themselves" was made by Hungarian jurist Mate Daniel Szabo (Szabo, 2005). Adding the requirement that privacy must be understood in light of contemporary society and economic institutions makes it appear difficult to develop a complete legal definition of privacy. Despite these ambiguities, the right to privacy is recognized in a number of international legal texts. However, it is “unclear how or even if effective legal protection can be provided when the target of the protection cannot be identified with certainty” (Post, 2001).

1.3 Right to Privacy and its recognition

A large number of international statutory provisions from the second half of the 20th century recognized the right to privacy as a first generation fundamental human right, and protection for this right eventually emerged in the national laws of the countries that ratified these articles. The case law of the courts protecting these rules establishes the precise nature of privacy and the facets of life that can be deemed private (De Hert, 2004). These texts do not provide more information on what privacy is. The right to privacy is covered by a number of international human rights agreements, both at the global and regional levels.

“The right to privacy is a fundamental human right, and everyone has the right to their private and family life, home, and correspondence”, according to “Articles 12 of the Universal Declaration of Human Rights (United Nations, 1948), Article 17 of the International Covenant on Civil and Political Rights (United Nations, 1966), Article 8 of the European Convention of Human Rights (Council of Europe, 1950), and Article 7 of the Charter of Fundamental Rights of the European Union” (Gellert, Gutwirth ,2013)

(European Court of Human Rights, 2018). These dispositions, however, are relatively brief and "don't give detailed instructions on what privacy is or what aspects of privacy need to be protected by law" (Solove 2011). The case law and judicial decisions that govern how these rules are applied contain the answers to these questions. Due to their intricate procedures and rules, it is important to mention the influence of the Council of Europe (CoE), The European Court of Human Rights (ECtHR), and the Court of Justice of the European Union (CJEU). These institutions have created a comprehensive corpus of case law pertaining to protection of individual's private life.

The right to respect for one's private and family life is stated in Article 8 of the European Convention on Human Rights (ECHR). 1. "Everyone has a right to respect for their home, their communications, and their private and family lives" (European Court of Human Rights, 2018). 2. "Public authorities may not impede the exercise of this right unless doing so is legal, necessary for a democratic society, and serves the interests of national security, public safety, the country's economic well-being, the prevention of disorder or crime, the protection of health or morals, or the preservation of the rights and freedoms of others" (European Court of Human Rights, 2018).

Since Article 8 protects such a wide range of aspects of life, the ECtHR declared that "there is no complete definition of what constitutes private life" (Gellert, Gutwirth, 2013). Additionally, the ECtHR was prompted to build a flexible definition of private life under the contemporary conditions by the technical and scientific advancements that surfaced following the ratification of the ECHR. In its case law, the ECtHR stated that interference with the following aspects of life fell under the purview of Article 8 (and further examined whether the interference was legitimate or not as it is not an absolute right): "access to personal data, telephone tapping, choice or change of name, sexual life, profession or domicile, protection from environmental annoyances, and the right to form and maintain relationships with others" (European Court of Human Rights, 2018). Additionally, the ECHR's preamble emphasizes that these essential rights will be maintained and expanded (De Hert, 2004). It suggests that what is covered by Article 8 fluctuates along with the constantly shifting socioeconomic circumstances.

The ECtHR has a significant impact on the decision of the European Court of Justice for a number of reasons. "The language of Article 7 of the Charter of Fundamental Rights was modeled after Article 8 of the ECHR, and Article 52.3 of the Charter stipulates that for rights that also occur in the ECHR, the meaning and extent of the right also apply to them in the Charter" (Gerety, 1977). As a result, "the ECtHR's case law can be used to infer information about privacy" (Gellert, Gutwirth, 2013).

It is important to notice when we are looking at the concept of privacy throughout the history that technological advancements are inextricably linked to its evolution. It was clear that the ECHR had significant limits by the 1970s thanks to modern technology (De Hert, 2004). These drawbacks included the application's ambiguous scope (because privacy was not defined), the fact that it only protected individuals from state meddling and offered little protection for "personal data in the modern sense" (De Hert, 2004). The right to data protection, which seeks to safeguard the person in the age of the information society, emerged as a result of this.

Convention 108 or "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" was adopted in 1981 after addressing the issue of data protection under Article 8 of the ECHR on multiple occasions (European Court of Human Rights, 2018). Not all data processing involves an individual's private life.

However, "…its regulation does not apply to all data processing, since it does not apply to processing which does not infringe on the privacy of the individual" (Gellert, Gutwirth, 2013). Privacy is also more broad and specific, as it "may apply to the processing of non-personal data while still impacting privacy" (De Hert, 2004). Another significant distinction is that, "in contrast to the right to privacy, which is more abstract, the right to data protection is subject to a complex set of laws that include definitions, guiding principles, and other provisions" (Gellert, Gutwirth, 2013).

2. Personal data protection concept and privacy protection challenges

2.1 Challenges of privacy protection

Privacy protection remains a challenge despite present statutory constraints and the creation of a right to data protection. In his 1967 book "Privacy and Freedom", Professor Alan Westin claimed that there existed "a serious anxiety over the protection of privacy under the increasing constraints from monitoring technologies" (Reynolds, 1969). It is important to consider Internet usage, cellphones, social media, drones, biometric identification, and the Internet of Things (IoT). According to Solove, it is essentially impossible to exist today without having some sort of record made of you (Solove, 2011).

As a socially recognized phenomena that has always existed, "monitoring was evident in tiny communities when individuals constantly observed their neighbors, exerting moral pressure and upholding the values of the neighborhood" (Westin, 2003). Today's monitoring is significantly different since in addition to being seen, information about us is also captured, saved, and an increasing number of elements of our lives are being documented in this manner (e.g. security cameras, paying with credit cards, buying airplane tickets, etc.) (Solove, 2011). The advancement of computer technology also makes it feasible to store data without restrictions on quantity, volume, or duration of storage. The gathered data may be promptly transferred, sorted in a methodical fashion, and stored in large volume databases.

However, some lawyers argue that despite what individuals claim, their behavior shows that they do not truly value privacy. According to Jonathan Franzen "The fear about privacy has all the finger-pointing and hysteria of a good old American scare, but it's lacking one key ingredient: a really worried population" (Gonzalez, 2015). Americans are generally interested in privacy in the abstract. Despite surveys showing that individuals value their privacy greatly, many people habitually divulge personal information and openly share sensitive details about their life online. The claimed and actual privacy concerns of people differ. Calvin Gotlieb asserts that "the majority of individuals do not care enough about privacy to respect it when other interests are at stake" (Cohen, Gotlieb, 1989).

When weighing the significance of their personal privacy, people typically don't systematically analyze how their rights and what is acceptable should be balanced (West, 2008) (ENISA, 2016). On a practical level, people could decide to give up their personal information or be compelled to do so in order to receive benefits in return, such when making an online purchase (ENISA, 2016). "For law enforcement or national security purposes, such as during criminal investigations or intelligence operations to prevent further harm to society from public security dangers, society may also determine through particular rules that some persons within specified settings may have portions of their right to privacy annulled" (West, 2008).

Privacy and its implications especially regarding the breach of privacy depend much on context. When taken out of context, "even personal information that could be thought to be

harmless could become harmful if paired with other personal or non-personal information" (West, 2008). Consequently, managing this is not a task that a person can complete on their own; rather, they must collaborate with and rely on other third parties (such as regulators or organizations utilizing their personal data) "in order to fulfill expectations on the use of personal data and prevent its misuse, if possible" (ENISA, 2016). However, value assessment of personal data is challenging and "context-specific" (Solove, 2011).

Consumers' attitudes and behaviors are complicated when it comes to assessing risk and harm (West, 2008). According to research, people value losses twice as highly as profits, but they are also more willing to gamble when losses are possible rather than certain (West, 2008). This same reasoning would suggest that data subjects may be less likely to take safeguards while managing their own personal data if they are unsure about the likelihood of data misuse or security breaches. If these threats are truly impossible to predict in advance, it follows that an appropriate legislative strategy should not only define data subjects' rights but also provide people with practical instruments to take action when such instances occur (ENISA, 2016). If precautions are taken to mitigate dangers, people may in fact alter their behavior (West, 2008). There are several intriguing concepts in this regard from the research on behavioral economics. One is that "human decision-making demonstrates constrained rationality, meaning that individuals rely on techniques like rules of thumb and anchor points because they are unable to completely appreciate how their personal information could be utilized" (West, 2008).

The information society in which we currently live has a significant influence on our daily lives. There are numerous ways in which this issue affects privacy (Szabo, 2005). On the one hand, a "person's private sphere grows more open as new advancements intrude more and more into it" (Szabo, 2005). Increasingly, private areas of life may be accessed or influenced by technologies. On the other side, when more activities in life are done online, individuals tend to retreat, their connections become "less intimate, and the individual becomes more private in the offline world" (Szabo, 2005). It is even feasible to live a whole life online thanks to technology advancement and the many opportunities it has opened up, including the ability to work, have friends, shop, and so on (Solove, 2011). Because of this, each person in society is defined not by himself or herself but rather by the information that has been gathered on him or her. Since many of personal relations online do not allow to know the person in their true physical form, the person becomes virtual and is instead recognized by the recipient as a collection of data (Szabo, 2005). The person remains a genuine human being despite this virtualization, but is only known to the outside world as a collection of data (Solove, 2011). As a result, the outside world has a preconceived notion that the online person they are interacting with is also a real person in the offline world.

There are several in which poor privacy safeguards may cause harm. One of classification is proposed by Hoven:

1. Information inequality which refers to price discrimination without the individual's knowledge or ability to affect it, in which information about purchases and preferences is exploited for marketing purposes (Hoven, 2008). The use of behavioral monitoring and analysis tools is a case in point in this situation, where the same goods and services may be offered at various rates based on knowledge about prior purchases or habits. Additionally, this could result in discrimination, when people or particular social groups are picked out for unfavorable treatment based on false or inaccurate beliefs (Hoven, 2008).

2. “Restriction of moral autonomy which occurs when people's alternatives for self-representation are constrained or limited as a result of the ubiquitous and widespread nature of personal information” (Hoven, 2008). This might also be referred to as “a limitation on the freedoms guaranteed by the right to privacy” (Hoven, 2008). This may be seen, for instance, in behavioral profiling and advertising, where persistent profiles may exist across several distinct domains, or in the development of “numerous online personas in response to the requirement to clearly distinguish personal data settings” (for instance, profiles specifically created for different purposes: social networking, work and professional use, creativity etc.) (Hoven, 2008).
3. Information damage which includes harm to the individual, which are only conceivable after the acquisition of data or information about the person, and includes apparent examples like identity theft (Hoven, 2008). Identity theft is one of the most prominent examples in the information age.
People may be harmed directly or indirectly by each of these sorts of damage. As a result of the exposure of personal information, they may unintentionally exacerbate conflicts or ruin relationships (Hoven, 2008). People may constantly worry that someone may use their personal information against them, such as in stalking or personal surveillance situations. There could also be immediate effects, such as theft of credit cards, bodily injury, or lost property.
When privacy safeguards are withdrawn or violated, it is difficult to determine the damage or the harm that may ensue (Fogarty, 2009). Damage may come in both direct and indirect forms, and it can affect a person in a number of different ways, from financial to social, emotional, and physical. Types of injury might be hard to predict in advance. Finally, the erosion of trust and confidence in individuals exploiting personal data may have an impact on society as a whole.
Furthermore, it is important to think about how the usage of personal data may have wider effect. While it may be feasible to pinpoint specific instances of a person's physical or financial damage, there are also potential social repercussions from the ongoing, systemic drive to collect and exploit personal data (Dyson, 2008). The development of a culture of mistrust or dread, as well as a decline in confidence in the organizations collecting personal data, are examples of indirect social effects.
However, defining social damages consistently across national borders is far more difficult since what is considered acceptable in one country could not be in another (Dyson, 2008). An excellent illustration of this is how privacy is seen differently in different countries and cultures throughout the world, where physical rather than informational factors are more important (Hoven, 2008).

2.2 Evolution and emergence of personal data protection

The field of EU legislation governing data protection is relatively new. However, there was legislation in Europe governing data protection prior to the creation of the European Union. From the 1960s onward, “a number of country states started to legislate on data protection concerns, developing the fundamental ideas that later became a component of the European data protection legislation regime” (Craig, Búrca, 2021). The OECD's data protection recommendations and the Council of Europe's data protection convention, in particular, put forth significant foundational elements that affected the framework as it took shape under and as EU legislation.
As a result of advancements in computing technology, data protection law was created in the 1970s. The first data protection legislation in history was passed in 1970 in the German state of Hesse, which is typically credited for it (Schwartz, 1995). Over the course of the

1970s, some Member States, including Sweden, Germany, Austria, Denmark, France, and Luxembourg, created their own, distinctive domestic data protection rules as a result of this precedent. The US started debating the social effects of computerization as well. Fundamental guidelines for fair information practices were put forward in the important 1973 study Records, Computers, and the Rights of Citizens, which was anticipatory for the future development of data protection law in Europe and internationally. Since the 1974 Privacy Act only applies to data processing by federal agencies, the legislative outcome in the US, however, remained largely constrained (Schwartz, 1995) (Craig, Búrca, 2021). With the exception of a few sectoral initiatives, the private sector continued to be essentially unregulated. The consequent gap in transatlantic data protection regulation has often resulted in controversies between the EU and US legislation in the sphere of personal data protection (Craig, Búrca, 2021).

Despite repeated requests from the European Parliament, which has consistently pushed for European data protection law, the European Communities refrained from legislative attempts during this initial period of data protection regulation (Craig, Búrca, 2021). The Commission declined to propose such legislation for a number of reasons. It first asserted that it had no plans to create any data banks, which reflected an early, limited perception of data protection. The Commission overlooked the corresponding need for European data protection regulation for a very long time in favor of concentrating almost exclusively on the economic possibilities of digitization, computerization, and telecommunication (Fogarty, 2009). As a result, the EU originally failed to influence this developing area both inside and outside of Europe.

Other global institutions started to help fill the gap as the demand for global coordination increased. The OECD released recommendations "On the protection of privacy and transborder flows of personal data" in 1980, expanding on the fair information practices principles the US had established (Fogarty, 2009). These guidelines covered crucial data protection ideas such as "the limiting of data collection and use, data quality and security, and purpose definition standards" (Convention 108, 1981) (Fogarty, 2009). Convention No. 108 for the "Protection of Individuals with Regard to Automatic Processing of Personal Data", established fundamental rights to access and correct personal data and laid forth important data protection concepts including "fairness, lawfulness, proportionality, and purpose restriction, building on precedents from domestic law" (Convention 108, 1981) (Fogarty, 2009). These principles and rights had an impact on how data protection law was later developed in Europe and beyond (Fogarty, 2009).

A European data protection regulation was ultimately presented by the European Commission in 1990. It was possible largely due to requests for action made by the Member States' commissioners for data protection. It cited the internal market competence and declared that the free flow of personal data within the internal market was threatened by the fragmented national data protection regimes. Since each Member State had enacted data protection legislation, harmonization was achieved by a directive. The lengthy legislative process made clear that Member States were more interested in preserving the data protection ideas they had developed than in coming up with new ones. The Data Protection Directive of 1995 was "the end outcome, combining elements from several national data protection laws" (Craig, Burca, 2021).

Additionally, the Directive of 1995 developed into a concrete representation of some fundamental aspects of EU law. The EU data protection regulation's reach is constrained to EU law, according to the theory of conferral. The Member States insisted on their versions,

which resulted in wide (in any case) carve outs on matters of public and national security, defense, and criminal law. These exclusions split the internal structure of EU data protection law while illuminating the unique constitutional context of the EU. Furthermore, it was obvious that member nations couldn't constantly maintain their favored strategy. A fragile compromise produced the resulting regulations on personal data transfers from the EEA to third nations. Such transfers were frequently prohibited by existing national data protection systems, but these restrictions varied widely in terms of their underlying justifications, actual requirements, and institutional evaluation.

2.3 Privacy and societal drivers

Numerous socioeconomic forces are relevant regarding the societal demand for privacy and achievement of balance between privacy and security. The state is increasingly resorting to the use of personal data to supply societal "goods," which are regarded valuable and acceptable as a privacy invasion by either governments (unilaterally) or society at large (Lieshout et al.,2007). This is due to changing social necessities for social security, healthcare, national security, and law enforcement.

The shifting social attitudes toward privacy, including individuals' growing willingness to divulge personal information in exchange for modest benefits like joining a trusted group of people who share similar interests or sharing content more frequently on user-friendly and accessible platforms like YouTube (Lieshout et al.,2007). “A changing understanding of the integrity of the human body and what it is to be human is attested to by an increasing familiarity and comfort with technology that blurs the barrier between the human and the artificial” (Fogarty, 2009). Ideas of personal space and privacy are starting to “change as a result of trends toward cosmetic procedures and body alteration” (Fogarty, 2009). It is also important to mention development of technologies related to DNA manipulations (Fogarty, 2009).

The appropriate implementation of personal data processing can be advantageous to society as a whole. Processing of personal data is being used more and more by the public sector to enhance public services like social security and tax administration. To integrate various government services and improve the citizen's "service," managing personal data is viewed as essential. These may be made simpler by "one stop shops," which “compile personal information from several sources to make it easier for the citizen to access” (Fogarty, 2009). The growing demand and the possibility to use large volumes of data in such areas and healthcare, sociology and economics also boosts the necessity for an improved data protection landscape.

To “combat organized crime, identity fraud, illegal immigration, and terrorism” in response to recent geopolitical events, the processing of personal data has risen (Fogarty, 2009). One example of this is the Data Retention Directive (Directive 2006/24/EC, 2006). Information is frequently gathered from databases created by governments or private parties for various reasons, which has raised worries about civil rights, not least because “the borders between stewardship and accountability for personal data can become unclear when the private sector is deemed an agent of the state” (Lieshout et al.,2007). Two prominent instances of this are the conflict between Europe and the US over obtaining information on financial transfers employing the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and Passenger Name Record (PNR) data collected from airlines. (Fogarty, 2009).

This might bolster the already existing mistrust towards private services and public security

This might bolster the already existing mistrust towards private services and public security. Finding the "ideal balance between security and privacy" is a topic of intense policy discussion, which frequently "downplays the importance of human rights and the fact that, in a democratic society, actions that are detrimental to an individual's privacy may only be adopted when required" (Lieshout et al.,2007). Methods to tackle such issues differ throughout Europe, with some nations emphasizing data exchange between administrations to reduce duplication and the chance of discrepancies while others adopting a sector-specific strategy to minimize privacy issues. In that regard, the Directive's harmonizing impact is similarly constrained in scope due to its restricted applicability to first pillar Internal Market concerns (Fogarty, 2009). The establishment of large databases of fingerprints planned for the near future, despite privacy concerns voiced by civil society organizations, data protection commissioners, and regulatory agencies is another discussion revolving around the debate between privacy and security (Lieshout et al.,2007). Data sharing and biometrics, which are more and more recognized as effective weapons for combatting severe crime and international terrorism are used increasingly to identify threats and combat crime.

When evaluating the social value of personal data and personal data protection, it is important to keep in mind that "protecting personal data has inherent value to society on its own" (Fogarty, 2009). To effectively enjoy such freedoms as the freedom of expression, the freedom of association, and the right to practice religion, a person must have a "suitable personal environment in which to develop his or her views and choose how to express them" (Fogarty, 2009). Thus, the exercise of privacy rights can be a means of achieving other rights. Therefore, privacy protection is crucial not just as a guarantee for individual well-being but also to allow the necessary freedom and creativity that can be advantageous to society as a whole. Therefore, the discussion cannot be only framed in terms of "sacrificing personal freedom for societal gain in order to define more or less strict data protection standards" (Lieshout et al.,2007). It's important to remember that data protection and privacy are not a zero-sum game where one person's gain is another's loss, or the other way around. (Solove, 2011).

2.4. European data protection directive

The European Data Protection Directive (officially Directive 95/46/EC) is a directive adopted by the European Union in 1995 which "regulates the processing of personal data within the EU" (Directive 95/46/EC). By regulating the "collection, use, and sharing of individuals' personal data", it seeks to safeguard their privacy and basic rights. The regulation, known as Directive 95/46/EC, is applicable to "all EU member states and specifies obligations for data controllers, who are in charge of ensuring that personal data is handled in compliance with the directive's rules" (Directive 95/46/EC). In 2018, the EU replaced the directive with the General Data Protection Regulation (GDPR) which has more strict rules and also applies to non-EU companies that target or collect data from EU citizens.

The Directive consists of 34 articles, and its requirements include topics including data quality, specific categories of processing, data subject rights, confidentiality, security, responsibility, and sanctions, as well as codes of behavior and supervisory agencies. It shares several fundamental ideas with other legal documents, including the Asia Pacific Economic Forum (APEC) Privacy Framework and the 1980 OECD Privacy Guidelines.

Despite the Directive's focus on regulation, it indirectly supports the protection of privacy through technology, most notably in Article 17. “Data controllers must use the required technological and organizational measures to secure personal data” in accordance with Article 17 of the Directive. The addition of Recital 46 to Article 17 emphasizes the need for these safeguards to be part of both the processing system's and the processing itself. As a result, security cannot simply be added to data systems; it must be built in; this concept is now known as "privacy-by-design."

Following the introduction and widespread use of ICT in the 1970s, the private sector started using personal data extensively. This increased the risk of “improper use of personal information and highlighted questions about the need for laws to maintain the degree of security for individuals” (Bennett, Raab, 2006) (Directive 95/46/EC). These regulations at the EU level were not very uniform at the time. While some Member States had very tight guidelines and processes, others had none at all. The Directive was developed as “an internal market tool to facilitate cross-border commerce by harmonizing data protection laws since this variability posed a barrier to the growth of the internal market” (Bennett, Raab, 2006).

The Directive's reference to the concept of personal data, rather than the idea of privacy, is one of its key features. Indeed, data processing activities that are not seen as being particularly sensitive to personal privacy in and of themselves may be subject to the Directive's restrictions. As a result, the Directive has several uses, privacy protection being only one of them. In actuality, its regulations serve a variety of purposes, such as promoting freedom of expression, combating discrimination, and enhancing effectiveness (Bennett, Raab, 2006).

The Directive has unquestionably had an impact on data processing techniques; its principles have become the benchmark “for the legal definition of personal data, governmental reactions to its usage, and other advancements in data protection legislation” (Bennett, Raab, 2006). Clear definitions of data subjects' rights, requirements for the handling of sensitive personal data, and the establishment of national and international oversight mechanisms are all necessary.

It's also necessary to keep in mind that the Directive was created at a period when computer systems and file systems were used for data processing. By outlining the responsibilities and processes associated with each function, it would be simple to control the risks associated with such a model (Bennett, Raab, 2006). Its primary goal was not to establish a legal framework that could handle upcoming challenges in data processing and privacy, but rather to “harmonize existing regulations to protect the right to informational privacy of the data subject and to establish a common European market for the free movement of personal data” (Bennett, Raab, 2006).

2.4 Individual perception of data protection under the data protection directive 95/46/EC

In light of the Directive's comprehensive approach to data protection, it would be valuable to gauge how both data subjects and data controllers see the Directive. The Eurobarometer results from February 2008 that looked at both views offer some intriguing insights in this regard.

As demonstrated on the figure 1, when compared to the younger Member States, the older Member States' degree of concern seems to be higher (Eurobarometer, 2008). With Austria and Germany topping the hierarchy with 86% and the Netherlands and Finland coming in last at 32% and 36% respectively (Eurobarometer, 2008). 65% of customers in the older Member States are thus extremely or somewhat worried about how the organizations manage their personal data (see figure 1) (Eurobarometer, 2008).

The findings show that there are regional differences. These variations might most certainly be explained, at least in part, by the general state of the economies and markets as well as by the particular state of the direct marketing sector, the primary user of consumer data (Călin et al, 2009). However, other findings, such as the ranking of Malta and Lithuania at the top of the list of countries with the most concerns about how their people' personal data is handled or the disparity between the Czech Republic and Slovakia, may support the idea that there may be some cultural elements at play in this regard (Călin et al, 2009).

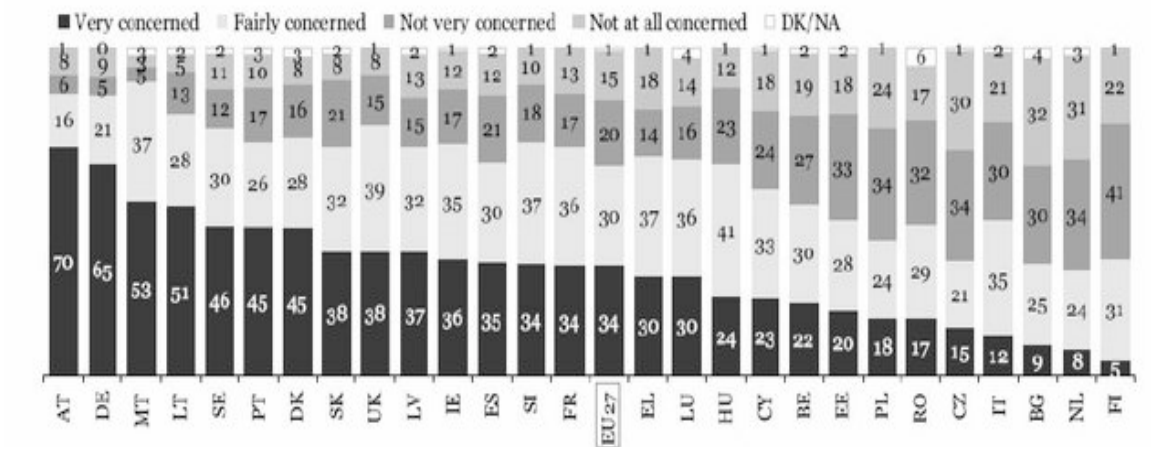

Figure 1. Concerns about personal data held by the organizations. (Source: Data Protection in the European Union. Citizens' Perceptions, Flash Eurobarometer No. 225)

As figure 2 demonstrates, it appears that consumers across all of the member states of the European Union are unaware of the tools and techniques available to them for protecting their personal data: All of the respondents who were questioned stated that people in their country are not very aware of how their personal information is used (See figure 2) (Călin et al, 2009). While consumers from Luxemburg and Denmark tend to have greater awareness – 56 and 59 respectively, consumers from Greece, Cyprus and Hungary seem to be the least knowledgeable with 93%, 90% and 90% respectively (see figure 2) (Eurobarometer, 2008).

In contrast to the older Member States, the New Member States tend to have a higher level of awareness, however the difference does not appear to be very substantial. The most significant finding in this regard is that consumers in the European Union need to get a better understanding of the nature of their personal data, the laws and regulations in place to safeguard it, and the rights they have and should exercise to preserve their privacy (Călin et al, 2009). The lack of knowledge regarding the organizations, methods, and tools for protecting personal data is evident. The majority of respondents in all 27 Member States indicate that they are essentially equally exposed to the risks associated with the "misuse of personal data and, as a result, with abuses against their privacy, regardless of the general state of their home economies and markets or the growth of the direct marketing sector" (Eurobarometer, 2008) (Călin et al, 2009).

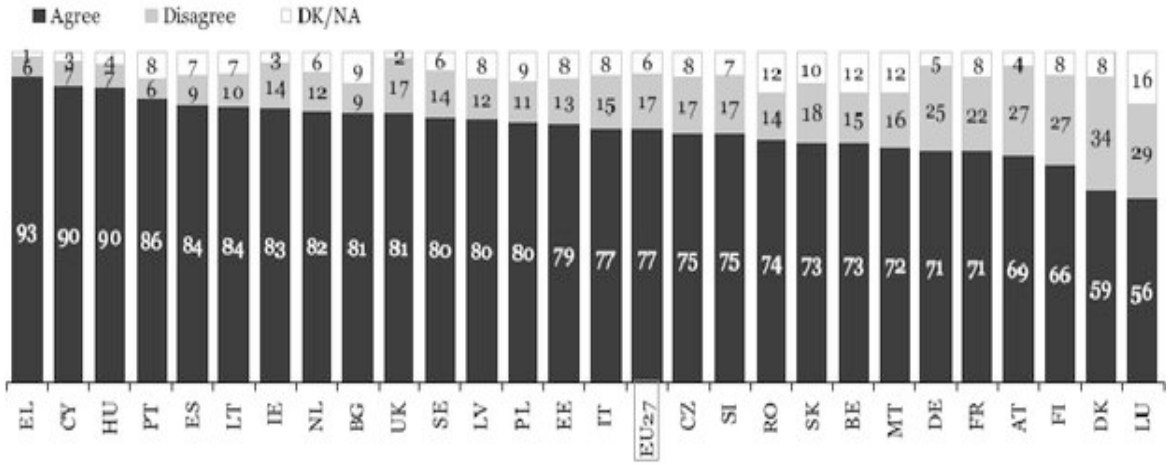

Figure 2. Awareness about the protection of the personal data is low. (Source: Data Protection in the European Union. Citizens' Perceptions, Flash Eurobarometer No. 225)

According to the figure 3, personal data are appropriately safeguarded at the level of the European Union, according to the majority of the respondents to the survey (48%) (Eurobarometer, 2008). However, the relatively large proportion of respondents (45%) who disagreed with this statement and rated the degree of protection as inadequate suggests that there were unsatisfactory results and that generally, data protection regime should be improved to guarantee an appropriate and effective level of protection (Călin et al, 2009).

The discrepancy between the percentages of 85% of Danish respondents in Denmark and that of just 26% of Greek respondents demonstrates the vast differences across all Member States in this regard considering the protection of personal data as sufficiently ensured. (Eurobarometer, 2008).

At the level of the newer member states, the differences across the countries are intriguing, especially in light of the general finding that even while personal data protection is typically well-ensured, additional improvements should be anticipated (Călin et al, 2009). People from Slovenia and Romania appear to be satisfied with the way their personal data is secured as a result. However, there might be a variety of factors supporting this amount of content, from useful information on laws and their application to a possible lack of awareness or interest in privacy and the protection of personal data (Călin et al, 2009).

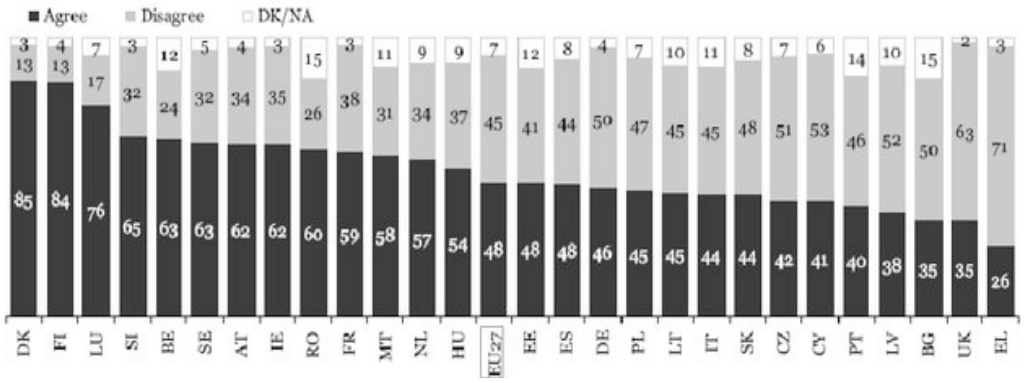

Figure 3. Personal data is protected properly. (Source: Data Protection in the European Union. Citizens' Perceptions, Flash Eurobarometer No. 225)

In general, "European residents were aware of the privacy dangers associated with the processing of their personal data, but they felt that even with the Data Protection Directive, the degree of protection in their own nations may not be sufficient" (Călin et al, 2009). However, methods to raise these degrees of security, such the involvement of data protection authorities, were "either not generally understood or not frequently used" (Călin et al, 2009)

2.5 Evaluating strengths and drawbacks of the Data Protection Directive

Strength	**Evidence**
Serves as reference model for good practice	Legislation that permits practical exercise of fundamental rights derived from ECHR, and considered a leading international model. Other privacy legislations adopt elements from the Directive e.g. Hong Kong, Canada, parts of Latin America
Harmonises data protection principles and to a certain extent enables an internal market for personal data	Implementation of legal rules across Europe for personal data processing that have greater compatibility than prior to the Directive's introduction
Flexible due to a principles-based framework	The Directive defines principles, without going into details for specific sectors/contexts. The exception to this rule is direct marketing
Technology neutral	No reference to specific technologies Security measures not specified Concept of personal data broad enough to be technologically neutral
Improves general awareness of privacy issues	Establishment and increasing numbers of privacy policies, privacy officers, etc. Consumer awareness regarding privacy

Table 1. Evaluation of strengths of the Directive 95/46/EC. Source: Rand Research Europe

According to the RAND research and several other researchers the influence the Directive had on framing and organizing the discourse surrounding data privacy was one of the most commonly mentioned distinct advantages of the Directive (Robinson et al, 2009) (see table 1). Despite the fact that the OECD Guidelines had a significant impact on this discussion, it is the Directive that is to be "credited with creating the legally binding guidelines that have been adopted as national laws in all of the Member States, building on the Council of Europe Convention 108" (OECD, 2007) (Korff, 2002).
The objectives and guiding principles set forth in the Directive have become "central to the discussion on privacy in Europe, following prior precedents set by the OECD Guidelines

and the Council of Europe Convention No. 108" (OECD, 2007). The Directive's guiding principles were frequently invoked whenever privacy concerns are raised in connection with data processing in any industry. This is evident, for instance, in discussions about how long telecom firms should save data under the Data Retention Directive (Directive, 2006).

The European Convention for the Protection of Human Rights and Fundamental Freedoms stipulates that "any derogation from the right to privacy may only be made under certain circumstances, including when it is necessary in a democratic society" (Article 8 of the Convention) (Korff, 2002). The Data Retention Directive must thus "operate in conformity with this principle as it is incorporated into the proportionality requirements of the Directive" (OECD, 2007). "To secure the right to privacy with regard to the processing of personal data and to enable the free movement of personal data between Member States, one of the Directive's primary objectives was to further harmonize data protection laws between Member States" (Article 1 of the Directive). A sufficiently unified European legal framework was intended to enable data controllers to manage personal data "in line with the same principles across all Member States and to ensure that data subjects are informed of their rights regardless of where they or the data controller are located" (Korff, 2002).

The Directive has attempted that "important areas of the processing of personal data are governed by generally equivalent legal standards across the EU. These include the idea of personal data, the prerequisites for validity, the quality and security of the data, the rights of the data subjects, and the potential for implementing these regulations", according to Korff (Korff, 2002).

The Directive promoted data protection mechanisms such as: "notice, model contracts, standard contractual terms, privacy policies, and the appointment of Data Protection Officers" (Călin et al, 2009). It also stated high level goals and the means by which these goals should be fulfilled (Lieshout et al., 2007). By forcing Data Controllers to provide information about the data processing techniques they plan to employ and to ensure their data protection measures are compliant with the Directive, notification, for example, advances the transparency aim.

People have also became more aware of privacy problems because to the transparency laws, particularly those involving notice, permission, and choice (Korff, 2002). Customers' reactions to information on privacy practices changes and direct communications about how their personal data is used show interest and knowledge.

However, the Directive 95/46/EC is often criticized for its drawbacks. Issues with national implementations may be a sign that the Directive's requirements have not been sufficiently harmonised. One sign that the Directive provides too much room for interpretation is, for instance, if implementation works effectively in certain countries but not in others (see table 2)

Weakness	Evidence
The link between the concept of personal data and real risks is unclear	The application scope of the Directive depends too strongly on whether or not the data processed can be defined as "personal" data. It is all or nothing: there is no room for "more or less personal" data (and accordingly "more or less protection"). Special categories of personal data processing are explicitly defined; but financial information and location data are not classified as sensitive. Strict application of the Directive's concepts sometimes leads to unpredictable or counterintuitive results.
Measures aimed at providing transparency of data processing through better information and notification are inconsistent and ineffective	Privacy policies not read in practice, as they are aimed at consumers yet written by/for lawyers Privacy policies do not play a role as a market differentiator Unclear purpose of notification Variety of 20 different notification processes, variety of exemption rules Uneven implementation of the process of registration
The rules on data export and transfer to third countries are outmoded	Definition of 'third countries' is perceived as outmoded in the light of globalisation Adequacy of countries is not relevant to business realities or to data protection Regulation in some other countries is stronger than the EU, but still not recognised as adequate
The tools providing for transfer of data to third countries are cumbersome	Length of time and effort required to get Standard Contractual Clauses, model contracts or Binding Corporate Rules approved is excessive Uneven practices of approval and authorisation; too little coordination between the Member States
The role of DPAs in accountability and enforcement is inconsistent	Unclear rationale for enforcement Uneven implementation of enforcement across Member States either for punishment or to affect behaviours Differing criteria for imposing sanctions
The definition of entities involved in processing and managing personal data is simplistic and static	Globalisation and increased re-use of personal data has outpaced the static definitions of controller and processor.

Table 2. Evaluation of drawbacks of the Directive 95/46/EC. Source: Rand Research Europe

The link between privacy protection and data protection has been criticized as being ambiguous, which has led some to question if the Directive's emphasis is "weak because not all actions of processing personal data covered by the Directive have a clear or discernible impact on privacy" (Lieshout et al., 2007) (see table 2).
The effects of the Directive are described in terms of the processing of personal data rather than potential privacy-related incidents. The strategy of the Directive is mainly based on a "fundamental rights interpretation of data protection, where personal data is believed to be inherently deserving of protection" (Korff, 2002).
Personal data, however, was a very wide concept that generated a lot of discussion. According to some researchers, all information that may be used to identify a specific person should be regarded as personal information (Lieshout et al., 2007). For instance, as

stated by this strict interpretation, internet protocol (IP) addresses constitute personal data regardless of whether the organization processing them has a reasonable chance of connecting them to a specific person. Geographical information and arbitrarily selected user names, even when they have no meaningful connection to a particular person, are likewise troublesome (Lieshout et al., 2007). If the data contains photos of people, it could be subject to the Directive, much as the Google Streetview data.

Another challenging subject was anonymity especially in huge datasets. For "statistical analysis, data mining, etc., vast volumes of anonymized clinical data are used in the field of healthcare research" (Lieshout et al., 2007). However, "regardless of how thoroughly the data is depersonalized", it is still considered personal data legally under this interpretation if there is a chance of connecting the data to a specific person, no matter how unlikely, challenging, or impossible that may be (Korff, 2002).

Mobile location-based services are already anticipated to expand in popularity. In this case, the protection of special categories of data processing, the Directive appears to have favored a "process-oriented approach that focuses on tying particular requirements to formal criteria rather than an outcomes-based approach that would take into account the impact and the necessity of such obligations" (Solove, 2011).

It is important to mention that one of the most well-known aspects of the Directive is the transfer of data to foreign (non-European) countries. The provision's stated goal of protecting European individuals' privacy was compromised by the vast volume of personal data transferred internationally (Craig, Burca, 2009). The Directive's basic rule, known as the adequacy rule, specifies that such transfers are only permitted if the recipient nation provides a sufficient degree of protection. If this is not the case, there are other options, such as obtaining the subject's consent or adopting a set of standard terms.

The adequacy criteria was also thought to be too narrowly focused. It is crucial to be aware of the following when assessing whether a specific subject's personal data is adequately secured in a foreign country: (a) the data controller has taken the necessary steps to accomplish this goal; and (b) the data controller is liable for any occurrences. Nevertheless, the fact that the third nation appears to have an adequate legislative framework that complies with the Directive's requirements does not entirely address this issue (Fogarty, 2009). Some individuals who took part in the interview thought that harmonization with third countries (those outside the EU) would invariably lead to a lesser level of protection.

2.6. Personal data protection under the Regulation (EU) 2016/679

The EU General Data Protection Regulation (GDPR) was agreed upon and finalized on April 27, 2016, following "four years of drafting, lobbying, and negotiations among the EU Member States and many affected organizations" (Fogarty, 2009). On May 4, 2016, its final text was published in the Official Journal of the European Union. The GDPR, which was "created to safeguard personal data pertaining to individuals", went into effect in May 2018 (Regulation (EU) 2016/679, 2016). As stated in the preamble of the GDPR, it superseded the 1995 Data Protection Directive with the intention of addressing "new difficulties for the protection of personal data" brought about by "accelerating technical advancements and globalization" (Regulation (EU) 2016/679, 2016) (Craig, Búrca, 2021).

The GDPR was created to replace the Data Protection Directive 95/46/EC, which was introduced in 1995 and, as a directive, provided considerable opportunity for interpretation during its implementation into different national legislation. A new update to the legal environment inside the EU was also required due to the quick shift in the data landscape brought on by the emergence of ubiquitous and mobile computing and the big data age

(Craig, Búrca, 2021). However, the drastic changes brought forth by the GDPR were projected to have a strong effect on both domestic and international companies. Most importantly, because it is a regulation rather than a directive, therefore it instantly became a legally binding regulation in every Member State. As a result, it helps harmonizing the EU's current data protection laws, enhancing both data protection rights and commercial opportunities in the digital single market (Watchter, Mittelstadt, 2018).

WP29 Position Paper (2009)	Regulation (EU) 2016/679 (GDPR)
Introduce a new "Privacy by Design" principle (pp. 12-15)	Introduces a new 'Privacy by Default and by Design' principle (GDPR Art. 25)
Introduce a new 'accountability' principle (p. 20)	Introduces a new 'accountability' principle (Art. 5§2)
Increase data controllers' responsibilities; introduce data protection impact assessments; reinforce the role of data protection officers (p. 20)	Increases data controllers´ responsibilities; data protection impact assessments are introduced; reinforces the role of data protection officers (GDPR Art. 35-39)
Improve redress mechanisms and introduce class action lawsuits (p. 16)	Improves redress mechanisms and strengthens the role of public interest groups for the enforcement of rights (GDPR Chapter VIII, particularly Art. 80)
Improve transparency; introduce data breach notifications (for high risk breaches) (p. 16, 21)	Improves transparency; data breach notifications become obligatory (for high risk breaches) (GDPR Section 1 and Art. 34)
Strengthen consent requirements (p. 17)	Strengthens consent requirements (GDPR Art. 7)
Give clear institutional, functional and material independence to the DPAs, as the 1995 directive´s Art. 28 was unclear (pp. 21-22)	Strengthens functional (Art. 52§1), institutional (Art. 52§2,5) and material (Art. 52§3,4,6) independence of DPAs
Clarify DPA´s enforcement powers, as the 1995 directive's Art. 28 only contain 3 subparagraphs on enforcement (p. 22)	Contains 16 subparagraphs on investigative and corrective powers (Art. 58§1,2)
Extend legislative advisory powers. WP29 opinions should be addressable more actors (e.g. national parliaments) and treat more issues than 'administrative measures and regulations' (p.22)	Extends the scope of the DPA's opinions to more actors (e.g. national parliaments) and to 'any issue related to the protection of personal data' (Art. 58§3b)
Strengthen the WP29	Renames WP29 to 'European Data Protection Board' with broadened task description (Art. 68 & 70)
Ensure more harmonization in an "unambiguous and unequivocal legal framework" (p. 9)	Directive becomes a regulation

Table 3. Comparison between the WP29 2009 position paper and the final text of the GDPR

The regulation achieves its goals in two ways: “first, by enhancing the well-known data protection principles previously outlined in the data protection directive, such as consent and purpose limitation, and second, by including new concepts like the right to be forgotten, the right to data portability, the requirement for data protection impact assessments, and privacy by design, among others” (Watchter, Mittelstadt, 2018). There has been a considerable amount of debate among academics and legal professionals concerning the fundamental changes that it introduces ever since its initial draft in 2012 (Craig, Búrca, 2021). However two specific GDPR concepts, namely the newly established right to be forgotten and the idea of consent with its revocation, shocked the legal, academic, and corporate worlds. Due to their significant influence on how personal data must be treated under the new legal regulations and the severe repercussions of executing these new standards in the era of big data and the Internet of Things, they both generated protracted discussion. The goal of this work is twofold in this regard: first, to review all debates surrounding the implementation impact of the new, more stringent definitions of “consent revocation” and the “right to be forgotten” on personal data protection; and second, to assess the effectiveness of current approaches, architectures, and cutting-edge technologies in terms of “meeting the technical requirements for the implementation and effective integration of the new requirements” (Watchter, Mittelstadt, 2018).

Data about an individual is generally referred to as personal data. While many Data Protection Acts describe personal data in language that are somewhat similar, the GDPR provides such definition of personal data (Article 4): “«Personal data» means any information relating to an identified or identifiable natural person (“data subject”)”; an “identifiable natural person” is one who can be “identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (Regulation (EU) 2016/679, 2016). According to this definition, personal data are all pieces of information that may be used alone or in conjunction with other pieces of information to identify, make a contact with, or locate a person.

The term "information" should be used liberally and encompass both factual information (such as a person's identity or the presence of a certain drug in their blood) and subjective analyses, such as information, views, and assessments. Although the ECJ has since clarified, relevant legal analysis (the evaluation) does not constitute as personal data, unlike information contained in a residence permit application and data from legal analysis (Cases C-141/12, C-372/12, 2014). Additionally, personal information can be in any format can include text, numbers, images, videos, and more. Additionally, take note that Article 4(1) of the GDPR refers to "information" rather than "data," suggesting that the data may need to have some informative value. It's not always simple to distinguish between information and data (Regulation (EU) 2016/679, 2016). When information is "about a particular person," it is deemed to be pertaining to a data subject. This contains data from a person's file as well as vehicle data that provides insight into the data subject. When someone can "separate" himself from others, that person is said to be recognized or identifiable. This does not imply that the person can be recognized by name; rather, she might be recognized via alternate methods, such a phone number (Craig, Búrca, 2021). This emphasizes the need for a broad interpretation of the definition of "personal data," a position that the Court has consistently supported (Watchter, Mittelstadt, 2018). The phrase "any information" represents "the goal of the EU legislative to attribute a wide scope to that notion, which is potentially inclusive of all forms of information, not just

objective but also subjective." The ECJ determined that metadata (such as location information or IP addresses combined with log files on retrieved web pages) that only permits the indirect identification of the data subject can still be considered personal data because it enables "to know the identity of the person with whom a subscriber or registered user has communicated and by what means, to identify the time of the communication and the location from which that communication took place"(Cases C-141/12, C-372/12, 2014) (Craig, Búrca, 2021).

Both personal and non-personal data are recognized categories under the European data protection framework. There are certain types of data that are never personal (since they are not related to a known or recognizable natural person) and others that were formerly personal but are not anymore (as linkage to a natural person has been removed). Recital 26 of the GDPR contains the legal standard for differentiating between personal and non-personal data (Regulation (EU) 2016/679, 2016).

Sender	Receiver	Date	Type of good	Price
John Smith	Jane Miller	12 February 2019	Laptop	1309
Sender (Pseudonymized)	Receiver (Pseudonymized)	Date	Type of good	Price
2342	1337	12 February 2019	Laptop	1309
Pseudonym	-	-	-	Name
1337				Jane Miller
2342				John Smith

Table 4. Example of data pseudonymization. Source: author

Pseudonymized personal information that may be linked to an identifiable natural person through the use of supplementary data should be regarded as information on such a person (Craig, Búrca, 2021). A natural person's ability to be "directly or indirectly identified by the controller or another person should be taken into consideration when determining whether that natural person is identifiable" (Watchter, Mittelstadt, 2018). In order to evaluate whether measures are fairly likely to be employed to identify the natural person, consideration should be given to all objective considerations, including the "expenses and the length of time necessary for identification" (Craig, Búrca, 2021).

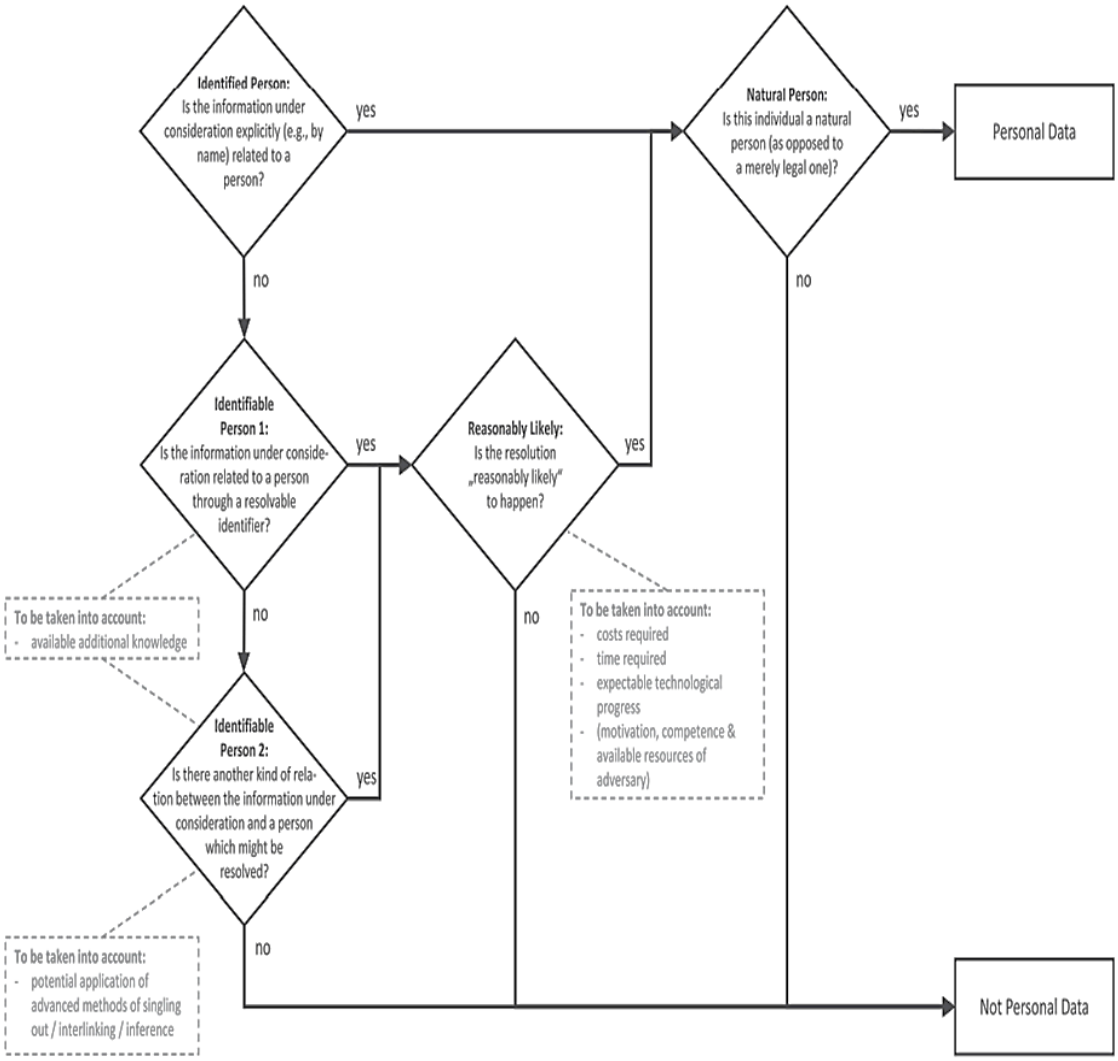

Figure 3. Assessment scheme for identifying the personal data. Source: Author

According to Recital 26 of the GDPR, "the principles of data protection should not be applied to anonymous information, or information that does not relate to an identified or identifiable natural person, or to personal data that has been rendered anonymous in a way that makes it impossible to identify the data subject" (Regulation (EU) 2016/679, 2016).
Since the controller or another party may identify the data subject using "means reasonably expected to be employed," the data is considered personal under the GDPR (Regulation (EU) 2016/679, 2016). Personal information that was never associated with a natural person or is no longer reasonably expected to be associated with a natural person falls under the category of "anonymous information" and is not subject to the Regulation's applicability (see figure 3).
In essence, the criteria established by Recital 26 GDPR adopts a risk-based methodology to classify information (Regulation (EU) 2016/679, 2016). Data should be handled as personal data when there is a plausible possibility of identification. Data can be classified as non-personal data where the risk is just careless, even when identification cannot be

completely ruled out. However, a deeper examination indicates that some of the test's components lack clarity, particularly as a result of divergent interpretations by various supervisory bodies (Craig, Búrca, 2021).

Personal data is relevant when identification is "reasonably expected" to happen; if not, the information in question is non-personal (Watchter, Mittelstadt, 2018). A few national supervisory agencies have adopted GDPR interpretations that substantially support this risk-based strategy. The UK Information Commissioner's Office (ICO), for example, emphasizes that the pertinent criteria is "the identity or likely identification" of a data subject in its relativist interpretation of Recital 26 GDPR (Information Commissioner's Office, 2012). Because "it is impossible to know with confidence what data is now accessible or what data could be made public in the future", leads to the assumption that "the danger of reidentification through data linking is basically unpredictable" (Information Commissioner's Office, 2012). According to the Irish Data Protection Authority, an anonymization technique can be effective without having to demonstrate that it is impossible for the data subject to be recognized (Cases C-293/12, C-594/12, 2014). Instead, the data can be declared anonymous if it can be demonstrated that it is improbable that a data subject would be recognized given the specifics of the case and the level of technology.

Conclusions

While privacy has a very old history, it is still a very current issue today. Definitions of privacy and the right to privacy attracted the attention of legal experts, and later the issue was governed by regional and international human rights agreements. However, there are still some issues with privacy protection.

Invasion of privacy is a concept that is evolving, according to media discussions. Transparent and distinct infractions have given way to trespasses that are mainly invisible, unreported, and persistent. The imagined limits of privacy appear to be eroding. The boundaries of one's privacy are now largely defined by their information, ideas, and movements rather than by the more obvious physical barriers like property lines, walls, or their bodies. The most influential social agents, over whom people have little authority, are also invading these aspects of privacy.

The ability to participate in contemporary society will depend on the sharing of personal information as technology develops. New categories of personal information or even new types of personal information will emerge when new technologies are developed, formed, and embraced by society in addition to a growth in the volume of personal information processed online. Technology's quick advancements provide a number of difficulties for society, especially for data protection authorities trying to create progressive laws that can handle how personal information is evolving. Due to this possibility, the privacy regime will always be a source of policy conflict.

The relationship between privacy and data protection perceptions and other societal objectives was taken into consideration. The discussion surrounding privacy, data protection, and security is the most prominent of these situations. Although poll findings varied widely, they usually showed a nuanced picture of the citizenry, highlighting variance and aspects of trust in and mistrust of authorities as well as a contextual approach to the perception of security measures. It's possible that "the public" has a far more complex strategy in this area than many policymakers may believe. Thus, future studies should concentrate on how issue-specific institutions impact the EU's contemporary digital

agenda generally or, conversely, how issue-specific institutions at the national level affect the GDPR's implementation and enforcement.

References:

Bennett C.J., Raab, C. (2006). The Governance of Privacy: policy instruments in a global perspective. 2nd Edition, MIT Press, London.

Bloustein, E. J. (1964). Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser. New

Bratman, B. E. (2002). Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy. Tennessee Law Review Vol. 69. 2002.

Călin, V., Carmen, P., Diana, B. (2009). "european union consumers' views on the protection of their personal data: An exploratory assessment ". Annales Universitatis Apulensis Series Oeconomica, 2(11), 988–995. https://doi.org/10.29302/oeconomica.2009.11.2.44

Cases C-293/12 and C-594/12 Digital Rights Ireland [2014] EU:C:2014:238, para 26. Available at: https://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051 [accessed 19 September 2022]

Cohen, R., Gotlieb, C. C. (1989). Educating Tomorrow's Professionals. Journal of Business Ethics, 8(2/3), 193–199. http://www.jstor.org/stable/25071887

Convention 108. (1981). Retrieved November 1, 2022, from https://iapp.org/resources/article/convention-108/

Craig, P., Búrca G. De. (2021). The evolution of Eu law. Oxford University Press.

Data Protection Commission. (2019). Guidance on Anonymisation and Pseudonymisation. accessed 9 January 2020 Available at: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf [accessed 10 September 2022]

De Hert, P. (2004). Privacy and Data Protection Concepts in Europe. Computers Freedom & Privacy, 2004, 20-23 April 2004 Berkeley. p. 4.

Directive 2006/24/EC (2006). of the European Parliament and of the Council of 15 March 2006 on "The retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks" and amending Directive 2002/58/EC. Available: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML [accessed 10 September 2022]

Dyson, E. (2008). How loss of privacy may mean loss of security. Scientific American. Retrieved September 25, 2022, from https://www.scientificamerican.com/article/how-loss-of-privacy-may-mean-loss-of-security/

ENISA. (2016). Security Economics and the Internal Market. ENISA. Retrieved September 26, 2022, from https://www.enisa.europa.eu/publications/archive/economics-sec

EUR-Lex (2016) Regulation (EU) 2016/679 [online] Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed 18 December 2020].

EUR-Lex. (1995). Directive 95/46/EC [online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 [accessed 21 December 2020].

Eurobarometer. (2008). Flash Eurobarometer 226: Data Protection – Data Controllers' Perceptions (2008). [online] Available: https://www.unidata.unimib.it/?page_id=605 [accessed 21 September 2022].

European Court of Human Rights. (2018). Retrieved December 24, 2023, from https://www.echr.coe.int/Documents/Convention_ENG.pdf

Fogarty, E. A. (2009). Protectors of privacy: Regulating personal data in the global economy. Review of Policy Research, 26(6), 886–888. https://doi.org/10.1111/j.1541-1338.2009.00421_4.x

Fried, C. (1968). Privacy. The Yale Law Journal Vol. 77, No. 3..

Gavison, R. (1980). Privacy and the Limits of Law. The Yale Law Journal Vol. 89, No. 3.

Gellert, R., Gutwirth, S. (2013). The legal construction of privacy and data protection. Computer Law and Security Review Vol. 29, No. 5.

Gerety, T. (1977). Redefining Privacy. Harvard Civil Rights-Civil Liberties Law Review Vol. 12, No. 2. p. 281.

González, J. Á. (2015). Eastern and Western Promises in Jonathan Franzen's "Freedom". Atlantis, 37(1), 11–29. http://www.jstor.org/stable/24757728

Hoven, Jvd. (2008). Information Technology, Privacy and the Protection of Personal Data in Weckert, J., Hoven, Jvd.; (eds) Information Technology and Moral Philosophy Cambridge University Press, 2008, p 311.

Information Commissioner's Office. (2012). Anonymisation: Managing Data Protection Risk Code of Practice. Available at: https://ico.org.uk/media/1061/anonymisation-code.pdf [accessed 4 September 2022]

Joined Cases C-141/12 and C-372/12 YS . (2014). EU:C:2014:2081. Available at: https://curia.europa.eu/juris/liste.jsf?num=C-141/12&language=en [accessed 19 September 2022]

Konvitz, M. R. (1966). Privacy and the Law: a Philosophical Prelude. Law and Contemporary Problems Vol 31, No. 2.

Korff, D. (2002). EC Study on Implementation of Data Protection Directive 95/46/EC (2002). Centre for Internet & Human Rights; Yale University - Information Society Project; http://dx.doi.org/10.2139/ssrn.1287667 [accessed 10 September 2022]

Lieshout et al. (2007). RFID technologies: Emerging issues, challenges and policy options. Retrieved September 27, 2022, from https://www.researchgate.net/publication/235218448_RFID_Technologies_Emerging_Issues_Challenges_and_Policy_Options

OECD (2007). Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. Available at: www.oecd.org/sti/privacycooperation [accessed 10 September 2022]

Official Journal of the European Communities (2020). Charter of Fundamental rights of the European Union. Retrieved September 18, 2022, from https://www.europarl.europa.eu/charter/

Posner, R. A. (1978). The Right of Privacy. Georgia Law Review Vol. 12, No. 3. (1978)

Post, R. (2001). "Three Concepts of Privacy", The Georgetown Law Journal, Vol. 89, No. 2001, pp. 2087-2098.

Reynolds, O. M. (1969). [Review of PRIVACY AND FREEDOM, by A. F. Westin]. Administrative Law Review, 22(1), 101–106. http://www.jstor.org/stable/40708684

Robinson, N,, Hans G., Maarten B., Lorenzo V. (2009). Review of the European Data Protection Directive. Santa Monica, CA: RAND Corporation, 2009. Available at: https://www.rand.org/pubs/technical_reports/TR710.html. [accessed 10 September 2022]

Schwartz, P. M. (1995). Privacy and Participation: Personal Information and Public Sector Regulation in the United States. 80 Iowa L Rev 554.

Solove, D. J. (2011). Nothing to Hide: the False Tradeoff between Privacy and Security. New Haven & London: Yale University Press, 2011.

Szabó, M., D. (2005). On the differences between EU and US privacy protection see more: Whitman, J. Q.: The Two Western Cultures of Privacy: Dignity versus Liberty. The Yale Law Journal Vol. 113, No. 6. (2004) pp. 1151-1221.

The 2002 Proposals for Amendment of the Data Protection Directive (95/46/EC). (2002). made by Austria, Finland, Sweden and the United Kingdom - Explanatory Note. Available at: http://www.dca.gov.uk/ccpd/dpdamend.htm [accessed 13 September 2022]

Warren, S. D., Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193–220. https://doi.org/10.2307/1321160

Watchter S., Mittelstadt, B. (2018). "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" *Columbia Business Law Review*, Vol. 2019, Issue 2.

West, R. (2008). The psychology of security: why do good users make bad decisions? Communications of the ACM. vol 51, No 4, pp 34 -40.

Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues Vol 59, No. 2. pp. 431-434.

York University Law Review Vol. 39, 1964. p. 973., p. 974.

Received 10 February 2023, accepted 02 June 2023