UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE,
LAW AND INTERNATIONAL STUDIES

Master's degree in European and Global Studies

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

The Evolution of Privacy and Personal Data Protection Rights in the Digital Age: A Comparative Analysis of the European Court of Human Rights and the Court of Justice of the European Union Jurisprudence

Supervisor:

Prof. GUIDO GORGONI

Candidate: *Jafar Soleimani Fard*

Student number: 2043191

A.Y: 2023-20234

دیگران چون بروند از نظر از دل بروند

تو چنان در دل من رفته که جان در بدنی

Acknowledgements

First and foremost, I want to thank my loving wife Barfin. Her boundless patience, understanding, and constant encouragement have sustained me throughout this journey. Her unwavering belief in my abilities and her endless support have been my guiding light, and I am eternally grateful for her presence in my life.

I also extend my heartfelt appreciation to my esteemed parents-in-law, Zahra and Reza. Their kindness, support, and words of wisdom have been invaluable to me. I am grateful for their unwavering encouragement and for welcoming me into their family with open arms.

I am deeply indebted to my supervisor, Guido Gorgoni, for their invaluable guidance, expertise, and unwavering support throughout this research endeavor. Their mentorship, insightful feedback, and encouragement have played a pivotal role in shaping this thesis and my academic growth.

Abbreviations

CJEU: The Court of Justice of the European Union

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe).

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

EPIC: Prior Informed Consent IT system

GDPR: General Data Protection Regulation

PLSC: Privacy Law Scholars Conference

DPD: Data Protection Directive

DPA: Data Protection Act

CCPA: California Consumer Privacy Act

US: United States of America

UK: United Kingdom

Abstract

The research will examine the protection of privacy rights and data protection in the jurisdiction of the European Court of Human Rights (ECtHR) and The Court of Justice of the European Union (CJEU) and assess how they relate to the protection of privacy and data protection. Data protection and privacy are both recognized as fundamental human rights, and it is critical to understand how they interact within the ECtHR and CJEU framework. The aim of this study is to answer this question: in its jurisprudence, how does the European Court of Human Rights and The Court of Justice of the European Union balance and deal with data protection rights and privacy protection, and what are the consequences and problems of its approach for human rights law and practice in Europe? The method used is a descriptive-analytical approach that analyzes secondary sources such as books, magazines and court decisions ensure a representative sample of European Court of Human Rights and the Court of Justice of the European Union cases, a random or stratified random selection approach was used, which allows for a thorough assessment of privacy and data protection legal practice within the framework of the European Convention on Human Rights and The Court of Justice of the European Union.

Chapter 1:

The Legal Evolution: From Privacy to Data Protection

1.1 Introduction

The right to respect for private life was first centered on protecting the private sphere, including the home and physical well-being. it has since grown to include the development of one's personality, interactions with others, and links to the external world (Marshall, 2009).

Over time, privacy has consistently faced threats, as evident in literature and legal cases. Initially, the infringement on privacy primarily came from close associates like neighbors and fellow villagers. Subsequently, government bodies, industry, and the media also played a role in compromising privacy. It could be divided into several periods, the past (pre-1980s), the present, and the foreseeable future with emerging privacy surveillance methods. While these periods are unique, they are interconnected because the information and technology used in privacy interference accumulate over time. The onset of one era doesn't mark the end of the previous, as exemplified by the evolving roles of photography and computer technology in invading privacy (Holvast, 2009).

The right to privacy is linked to human dignity as it aims at preserving individual autonomy and personal identity. Aspects of privacy that are particularly important in the context of the use of AI include informational privacy, which refers to information that exists or can be derived about a person and her or his life, as well as decisions made based on that information, and the freedom to choose one's own identity. Differences in its protection on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status are inconsistent with the principle of non-discrimination laid down in articles 2 (1) and 3 of the International Covenant on Civil and Political Rights. Discrimination on these grounds also violates the right to equality before the law contained in article 26 of the Covenant (Office of the High Commissioner for Human Rights, 2021).

Many international treaties and other human rights instruments expand on the ideals articulated in the Universal Declaration of Human Rights. One of the earliest instances of this recognition occurred in Article 12 of the Universal Declaration of Human Rights in 1948, which is often regarded as a significant document in human rights history, even though it lacks legal binding force. The ideas expressed in the Universal Declaration of Human Rights were later expounded on in many international treaties and other human rights instruments.

Notably, the International Covenant on Civil and Political Rights of 1966, in Article 17, specifically addressed the right to privacy, and the UN Human Rights Committee was established to oversee its observance and compliance. Additionally, the right to respect for private life found protection under Article 8 of the European Convention on Human Rights and Fundamental Freedoms, also known as the ECHR or the Convention, established in 1950 (Council of Europe, European Union Agency for Fundamental Rights, 2018).

In terms of Europe, The European Convention on Human Rights was approved on November 4, 1950, and it went into effect in September 1953 as a response to terrible human rights violations committed during World War II. For the purpose of reviewing complaints involving alleged violations of the Convention, the European Court of Human Rights was founded. Due to each individual's ability to submit a complaint to this transnational and regional court, the Court gets a sizable number of complaints. The Court has rendered noteworthy rulings in several matters, including instances involving privacy, and serves as a binding authority for member countries. Article 8 of the Convention, which upholds the right to respect for private and family life, is taken into consideration while analyzing certain circumstances. The European Court of Human Rights' privacy case law covers a wide range of topics, including traditional areas like the home, family, communication, and private life, as well as more contemporary concerns such workplace privacy and employer interference.

Judicial processes have a pivotal role in developing international law, legal systems, and the maintenance of the efficacy of laws, and Judicial practice has the potential to have an impact on future law amendment or modification by revealing flaws and holes in the existing legislation. Through its jurisprudence, the European Court of Human Rights plays a critical role in interpreting the Convention and defining the public's perception of privacy rights. The Court's case-oriented methodology and references to its existing jurisprudence guarantee that rulings are thorough and consistent (Schabas, 2017).

The European Court of Human Rights (ECtHR) has evolved dramatically in a very short period of time, owing mostly to judgments involving mass monitoring tactics. It is now in charge of critically examining the soundness of Member States' laws and even advising those states' legislative branches on required modifications to ensure conformity with the European Convention. This

transformational process has essentially established the court as a sort of European Constitutional Court, notably in instances of privacy. (Van der Sloot, 2020).

Privacy concerns are still important in today's society, as proven by the large number of complaints filed with the European Court of Human Rights on related issues. The Court, as a dynamic component in the field of human rights, has examined various cases and issued methods in a variety of instances, providing a complete grasp of the issues underlying the right to privacy.

The purpose of this research is to answer the following research questions:

- What is the position of the rights to privacy and data protection in the European Convention on Human Rights and the procedure of the European Court?
- What are the scopes of privacy and Data protection in the procedures of the European Court of Human Rights and The Court of Justice of the European Union?
- What criteria do the European Court of Human Rights and The Court of Justice of the European Union consider in their decisions about privacy and data protection?
- What effect has the procedure of the European Court of Human Rights and The Court of Justice of the European Union had on explaining and limiting the right to privacy and data protection?
- How have the procedures of the European Court of Human Rights and The Court of Justice of the European Union impacted the evolution of privacy and data protection?

Due to the theoretical nature of the research topic, the descriptive-analytical method is used using the collection method, which includes the analysis of books, articles, and judgments issued by the European Court of Human Rights. And then these issued opinions, judgments and doctrines will be carefully analyzed.

1.2 Historical Evolution of Privacy

In recent years, there has been an increasing fascination with the idea of privacy among scholars and experts in philosophy and law. To gain an understanding of its complexities and its relationship with security, it is crucial to explore its historical development and multifaceted character.

Throughout history, individuals and their families have held the primary responsibility for safeguarding their own privacy. This practice persisted well into the Middle Ages. However, as governments gradually encroached further into private lives, addressing privacy infringements required external assistance, legal regulations, and the emergence of self-regulation (Holvast, 2009). Examples from history, such as Aristotle's division between the public and private domains and John Locke's thoughts on property ownership, demonstrate the pervasiveness of privacy in key philosophical writings. (DeCew, 2016).

Research reveals that the term 'privacy' was in use in England as early as the fifteenth century. Colonial settlers in New England respected privacy regarding individuals' homes, families, and written communication. Opposition to the first U.S. census in 1790 led to instructions in 1840 to treat individual census returns as confidential, safeguarding citizens' private affairs from public exposure (Holvast, 2009).

Yet, despite its historical relevance, a universally accepted definition of privacy remains elusive. As Thomson (1984) keenly observed, "Nobody seems to have any very clear idea what the right to privacy is." Post (2000) further deepened the complexity by stating that "privacy is a value so complex, so entangled in competing and contradictory dimensions, that I sometimes despair whether it can be usefully addressed at all."

Samuel D. Warren and Louis D. Brandeis significantly contributed to this discourse with their seminal 1890 paper, emphasizing the contemporary societal value of privacy and advocating for its legal protection. They defined privacy as the ‘right to be let alone’ (Warren & Brandeis, 1890).

Privacy, as later categorized by Westin (1967), encompasses four dimensions: isolation, intimacy, anonymity, and reserve. Each dimension serves distinct functions, including personal autonomy, emotional release, self-evaluation, and setting communication limits (Pelteret & Ophoff, 2016). Privacy can historically be divided into two levels: relational and informational. Relational privacy

focuses on regulating interactions with others, such as controlling access to one's home or body. Informational privacy centers on the gathering, storage, and processing of personal data (Dörr, Weaver, and Kende ,2012).

Modern perspectives on privacy, as proposed by Helen Nissenbaum (2009), emphasize conscientious and contextually sensitive sharing of information, aligning with ethical and sociocultural norms unique to various social contexts. Tavani and Moor (2001) underscore individual control of personal information and protection from intrusion and information gathering by others.

A comprehensive understanding of privacy entails safeguarding private information from unauthorized access, restricting access under specific conditions and complying with legal requirements, and respecting the individual's authority over the dissemination of personal information, with clear consent being crucial (Schabas, 2015).

Balancing privacy with other societal interests, particularly security, presents a complex challenge. In various theories of state legitimacy, security often takes precedence over privacy. When security and privacy rights clash, mainstream ideas and popular intuitions tend to prioritize security. However, discerning these conflicts and effectively balancing security and privacy remains intricate, with no established method or theory to guide this nuanced equilibrium (Himma, 2007).

1.3 Emergence of Data Protection Laws

The terms "privacy" and "personal data protection" are sometimes used interchangeably, yet they reflect different ideas. European law distinguishes between privacy and data protection, recognizing that while they are closely related and often overlap, they are not synonymous. Privacy largely emphasizes safeguarding an individual's personal space, whereas data protection involves controlling the processing of data relating to an identifiable person. However, data protection is narrower because it specifically deals with personal data processing, while privacy has a broader scope, encompassing a wider range of personal space and boundaries. Additionally, data protection applies even when it doesn't necessarily involve privacy infringement (Politou et al, 2021). Kalahari, (2018) indicates that "the right to privacy is distinct from the right to data protection because the former is rooted in human rights while the latter is treated as an economic matter, which is a red herring to say the least".

EU law also distinguishes between two fundamental rights. Therefore, it appears that those Fundamental rights must be formally distinguished from one another. The European Court of Human Rights (ECtHR) rules that the processing in question violates one's right to privacy under article 8 ECHR. In reality, complaints about the processing of personal data have been made with the ECtHR. Due to the absence of data protection provisions in the ECHR, the Court relied on article 8 of the Convention (the right to privacy) to rule on these cases (Gellert & Gutwirth, 2013).

According to the European Agency for Fundamental Rights (2018), The right to personal data protection is implicated whenever personal data is processed, and it has a greater scope than the right to privacy. It requires that all processing procedures involving personal data be adequately safeguarded. Data protection pertains to all types of personal data and data processing, regardless of their connection to or influence on privacy. While the processing of personal data might sometimes infringe on the right to privacy, it is crucial to emphasize that showing an infringement on privacy is not a requirement for the activation of data protection legislation.

In terms of phrase and scope, the two rights differ. To begin, the right to respect for private life includes a broad bar on interfering, with particular public interest arguments that may potentially allow intervention in specific cases. Personal data protection, on the other hand, is viewed as a modern and proactive right, establishing a system of checks and balances to protect persons

whenever their personal data is processed. This processing must adhere to key elements of personal data protection, such as independent oversight and recognition of the data subject's rights.

The recognition of the right to privacy concerning the handling of personal data saw a significant shift in approach during the latter part of the 20th century and the early 21st century. This change was driven by the adoption of technologies, in both the governmental and corporate domains. As a result of the widespread adoption of advanced technology and the increasing significance of cross-border data transfers, the concept of personal data protection started to be acknowledged as a distinct and separate right (Kovalenko, 2022).

Legal decisions from national and European courts, as well as the codification of legislation within the European Union, have contributed to the extension of privacy rights in Europe. The EU Charter of Fundamental Rights and the Data Protection Directive are two key legislative documents that have contributed to the framework for privacy protection (Cole et al., 2019).

The fairness principle requires that data processing be fair and lawful to the data subject, while the data quality principle ensures that data is adequate, relevant, and not excessive for its intended purpose (Gellert & Gutwirth, 2013).

The rapid advancement of technology and the changing ways people live their lives have led to an increase in how we interact online. Unfortunately, this has also brought about a growing concern for our privacy. Our personal information has become an asset for companies and a tool for government surveillance. It's quite challenging to strike a balance between these interests and our fundamental rights to privacy and data protection. Often, we have limited control over our data. We might not even be aware of the data that is being gathered, the timing of its collection, or the potential impacts, for both corporations and governments. This lack of awareness creates an opportunity for these companies to violate our rights without our knowledge (Cortez, 2020).

"In 1995, the EU laid the groundwork for data protection with the Data Protection Directive (DPD), aiming to protect individuals' privacy regarding their personal data. As technology advanced, there was an increasing demand for safeguards to protect data. In 2012, the European Commission introduced the General Data Protection Regulation (GDPR) as a revamp to replace the directive.

Years of debates and negotiations in EU institutions followed, culminating in the GDPR's formal adoption by the EU Parliament and Council in April 2016. On May 25, 2018, the GDPR became fully enforceable across the EU, superseding the Data Protection Directive. Notable aspects of the GDPR include enhanced data subject rights, mandatory data breach reporting, strict consent requirements, and the appointment of data protection officers for some organizations. Despite being an EU regulation, the GDPR had a global reach, applying to organizations worldwide processing EU citizens' personal data. EU data protection authorities actively enforced it, issuing fines for non-compliance. Organizations both inside and outside the EU adjusted their data practices to adhere to GDPR standards. The EU's commitment to protecting privacy in this era is highlighted by this event setting a global benchmark for data security" (European Data Protection Supervisor, 2023, August 31).

The GDPR emphasized its alignment with the objectives of the EU Digital Single Market Strategy, which seeks to foster the growth of networks and services by means of regulations and infrastructure. In line with this strategy, the GDPR aimed to promote practices that respect privacy. Regarding GDPR enforcement, an important element was the introduction of fines. Moreover, numerous organizations made changes to their privacy policies to comply with GDPR regulations. This all-encompassing approach was designed to foster trust among European Union citizens when it comes to services, guaranteeing that they feel at ease using them. There are significant differences and similarities between privacy and data protection regulations in the European Union (EU) and the United States (U.S.). One notable difference is their regulatory approach, with the U.S. employing a sectoral approach that can leave new business sectors largely unregulated, allowing for more extensive use of personal data for commercial purposes. In contrast, the EU adopts an omnibus approach that offers stronger privacy protection across various sectors. However, this comprehensive framework can be seen as too rigid by some (Cortez, 2020).

Article 4 GDPR defines personal data as follows “any information relating to an identified or identifiable natural person; 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.” In the realm of data protection, regulations are relatively new. The Data Protection Act, the first privacy act, came into

force in the State of Hesse, Germany, in 1971. Soon after, Sweden and the United States also enacted privacy laws. Privacy protection has since been incorporated into the legal system of countries, except for the United States, where it must be established through amendments (Holvast, 2009).

GDPR outlines a number of grounds that justify personal data processing, such as the fact that the processing is necessary "for the performance of a task carried out in the public interest" or "for the purposes of the legitimate interests pursued by the controller “The Directive outlines the core principles of data protection, including the purpose specification concept.

The UK position as a former member of the EU is notable here. According to the UK government (2023), The Data Protection Act (DPA) 2018 in the United Kingdom regulates how organizations, businesses, and government entities use individuals' personal data. After Brexit GDPR is not valid in the UK and the domestic law implemented instead of GDPR. This law, in the UK, is their way of putting into effect the General Data Protection Regulation (GDPR). There are separate safeguards for personal data relating to criminal convictions and offenses. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances.

Beyond the EU, the US also witnessed significant changes in the data protection law. For example, the California Consumer Privacy Act of 2018 (CCPA) empowers consumers with greater control over their personal information collected by businesses. It grants California consumers the rights to know what data is collected, request deletion of their data (with some exceptions), opt-out of data sale or sharing, and protection against discrimination for exercising these rights. In 2020, Proposition 24, known as the CPRA, expanded CCPA's provisions, introducing new rights such as correcting inaccurate data and limiting the use of sensitive information. Businesses subject

to CCPA must fulfill responsibilities like responding to consumer requests and providing privacy notices. The CPRA amends CCPA but does not create a new law, often referred to as "CCPA, as amended." (CCPA, 2023) It was like a revolutionary movement in the US data protection era and was the first law based on GDPR.

1.4 Significance of Privacy and Data Protection in Contemporary Society

Privacy is not just about personal information; it is also about autonomy. Trust in relationships, ensuring confidentiality, and respect for personal boundaries will be empowered by the use of privacy. Beyond personal security and preventing unauthorized access, privacy is pivotal for fostering freedom of expression and individuality. It makes people feel free to explore their thoughts and identities without fear, as Privacy protects against discrimination, harassment, and harm (Warren & Brandeis, 1890).

While privacy protects individuals, it is not purely atomistic. "Society creates space for individuals due to the social benefits it provides." Privacy is vital to societal structure and civility. It promotes individualism, creativity, and the growth of ideas. It provides room for individuals to build relationships and enjoy democratic rights including voting, expression, and religion. The workplace, as a microcosm of society, fulfills an equally vital duty. Employee privacy is crucial for protecting labor rights like freedom of association (Jervis,2018).

According to Schabas (2017), this is an area where technology advancements have had a significant impact. Previous generations' expectations of anonymity have shifted as a result of various data collection and transfer methods. Many people now consider privacy concerns to be minor. Social media has become a popular platform for sharing personal information with a vast audience. The proliferation of cameras has made it difficult to govern the capture and distribution of photographs. Previously, taking a snapshot required careful planning and implied agreement. Technology has made incursions into the private realm more common and mundane. Many individuals no longer prioritize past sensitivity.

Westin (1967) further explains the enduring importance of privacy by identifying four main functions. Privacy fosters personal autonomy, fosters individual identity, facilitates psychological well-being, and provides a haven for emotional release, allowing individuals to express strong feelings without fear of judgment, thereby avoiding consequences. Potentially prevents mental health. Furthermore, privacy helps with self-evaluation and informed decision-making by providing individuals with the solitude and reflection required to digest information and make the best choices.

Technology's rapid advancements have made it increasingly challenging for individuals to maintain control over their data, intensifying the risk to their privacy (Kovalenko, 2022). While data consumption provides advantages such as connectedness, easy access to products and services, and personalized suggestions, it also introduces hazards, such as the construction of profiles that may enable people to access goods and services. Moreover, discussions about the right balance between privacy and security considerations are initiated when data is employed for law enforcement purposes (Cortez, 2020).

Chapter 2

Privacy and Data Protection in the European Convention of Human Rights

2.1 Introduction

The European Court of Human Rights is an international court established in 1959. It determines on individual or state applications alleging infringement of the civil and political rights guaranteed by the European Convention on Human Rights (1950). The European Court of Human Rights is the court of the Council of Europe. It is based in Strasbourg, France. Since 1998, it has served as a full-time court, and anybody can apply to it directly.

Article 25 of the European Convention on Human Rights provides that: "The Court shall have a registry, the functions and organization of which shall be laid down in the Rules of Court." The Court is composed of 47 elected judges, one from each member state. It investigates complaints (called 'applications') alleging infringement of human rights. Individuals and, on occasion, Member States can file these applications. When the Court determines that a Member State has infringed one or more of the Convention's rights and guarantees, it provides a written explanation. The Court hears applications from individuals, non-governmental organizations, or groups of individuals who claim to have been victims of a violation of the Convention or its Protocols. The Court also hears inter-state cases in which one contracting state claims that another contracting state has violated the Convention or its Protocols (Government of Ireland).

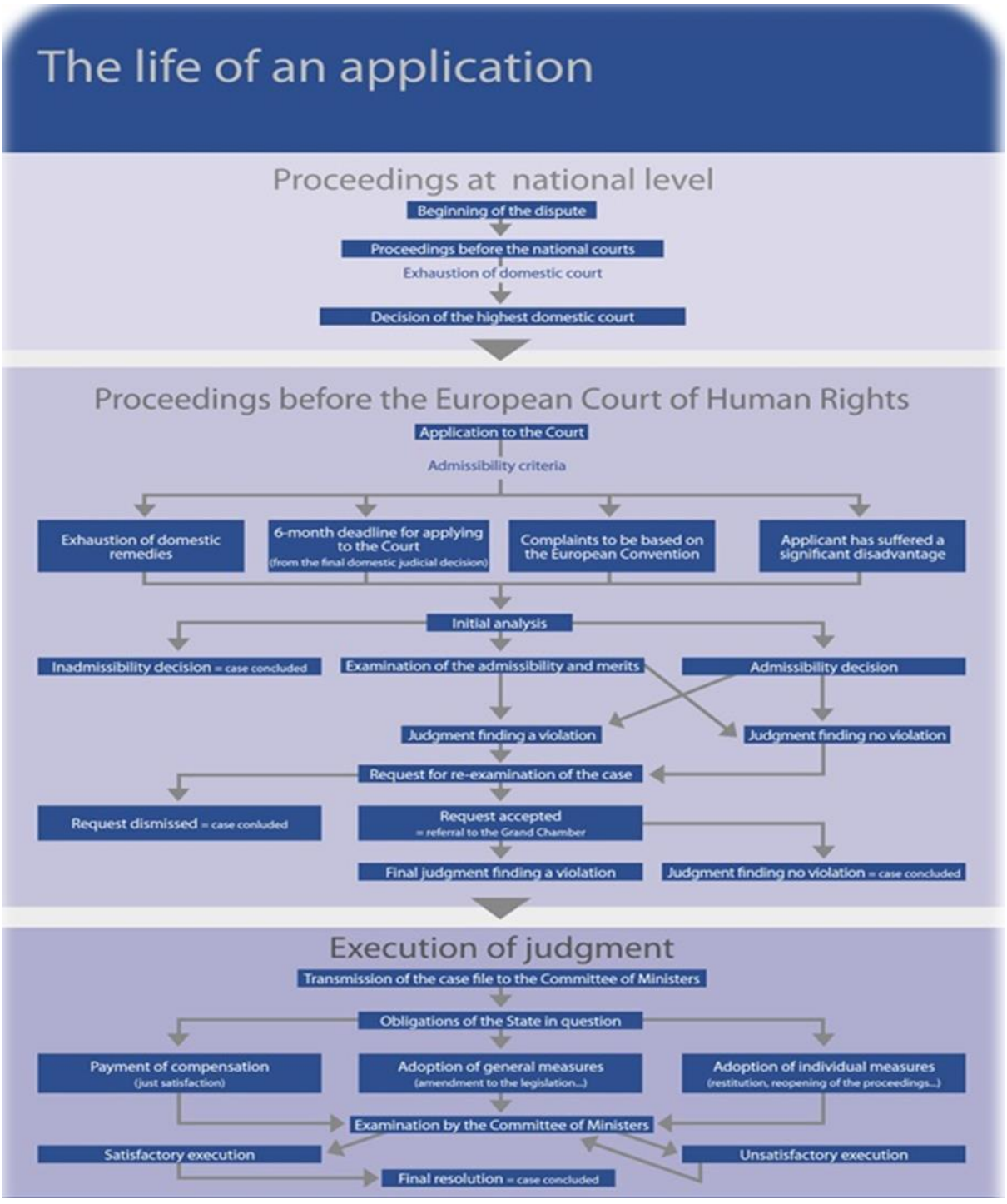
Due to the freedom of individual complaints in this court, the number of complaints submitted to this court has been significant. This court is a transnational and regional court whose decisions are binding on the member countries. Among the most important cases and decisions issued by the court, we can mention the cases related to the right to privacy.

Unlike the European Court of Justice or the US Supreme Court, the ECtHR does not have jurisdiction over national courts. Its jurisdiction is more towards the government as a whole than its judicial institutions. The main task of the ECtHR is to determine whether a state has breached its obligations under the Convention. Accordingly, the ECtHR does not return cases to the domestic court of origin to resolve the remaining legal issues (2012).

Any infringement on the right to privacy must not be arbitrary or unlawful. The term "unlawful" refers to the fact that states may only interfere with the right to privacy if they do so in accordance with the law. The law must be consistent with the principles, goals, and purposes of the International Covenant on Civil and Political Rights, and it must identify in detail the specific

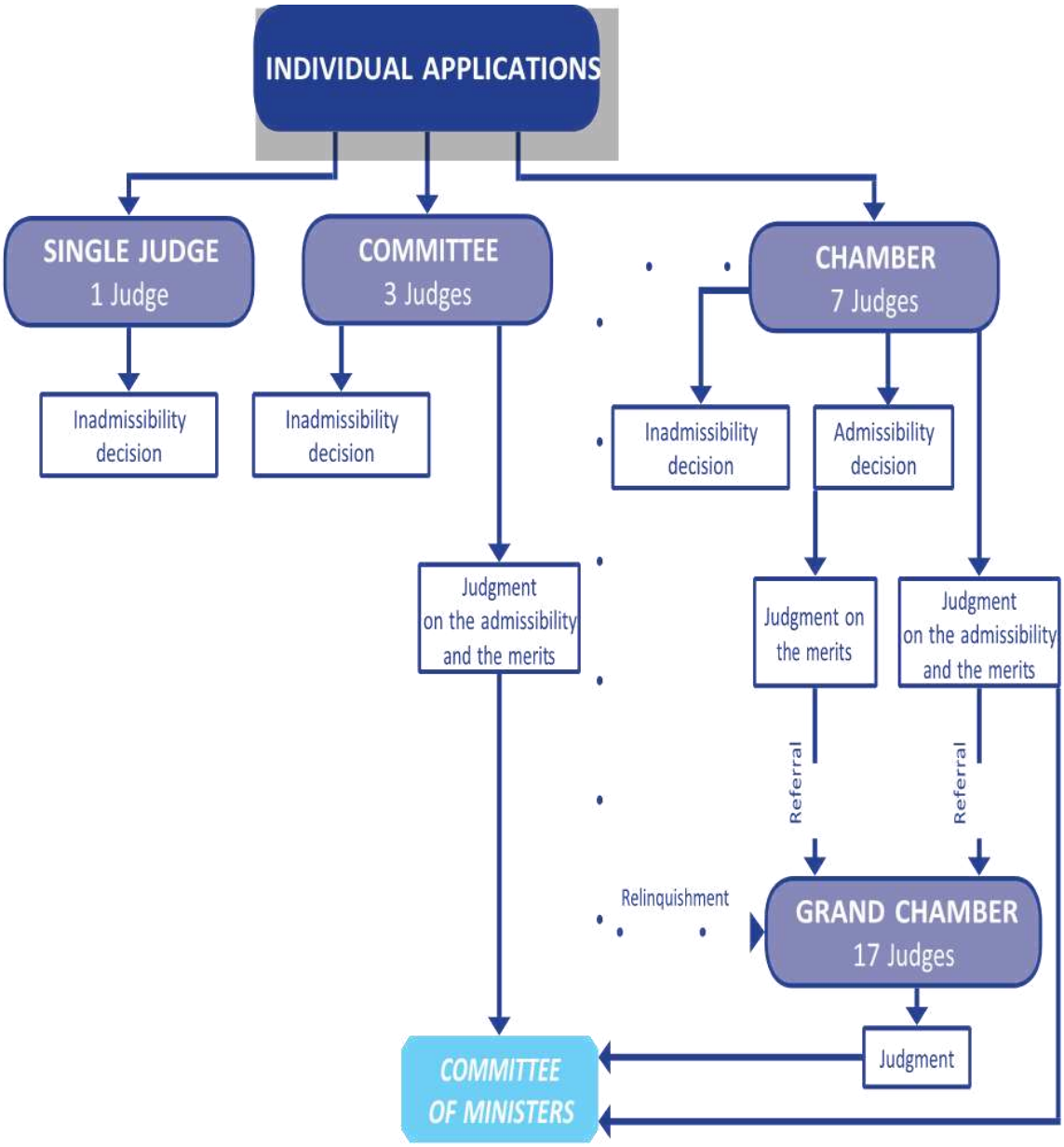
situations under which such interference is authorized (Office of the High Commissioner for Human Rights, 2021).

The European Court of Human Rights' jurisprudence plays an important role in interpreting the Convention and developing public perceptions of privacy rights. The Court's case-oriented methodology and references to its existing jurisprudence guarantee that rulings are thorough and consistent (Schabas, 2017).



1.1 Life of an application

European Court of Human Rights. Case processing. Retrieved from https://www.echr.coe.int/documents/d/echr/Case_processing_ENG



1.2 Court structure

European Court of Human Rights. Case processing. Retrieved from https://www.echr.coe.int/documents/d/echr/Case_processing_ENG

2.2 Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life

Article 8 - Right to respect for private and family life (European Convention on Human Rights, 1950):

1. Everyone has the right to respect for his private and family life, his home, and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8, like articles 9, 10, and 11, has a first paragraph that defines the right and a second paragraph that restricts or limits the extent of the right. The restriction or limitation clauses in the four articles share commonalities but are also unique, adapted to the specific right in question. The Court applies article 8 by determining if there has been a 'interference' with a right under paragraph 1.

Schabas (2017) affirms that Both clauses of Article 8 of the Convention are closely related to provisions of the Universal Declaration of Human Rights, which was approved by the United Nations General Assembly on December 10, 1948. Article 8(1) is derived from Article 12 of the Declaration: "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks on his honor and reputation." Everyone has the right to be protected by the law from such interference or attacks.' Article 29(2) of the Declaration serves as the foundation for article 8(2), which states that everyone's rights and freedoms must be limited by law to ensure morality, public order, and the welfare of a democratic society. Although similar to article 12 of the Universal Declaration, the words 'nor to attacks upon his honor and character' were removed from the Consultative Assembly draft. This disparity was observed in a report published by the Secretary General of the Council of Europe. The provision is organized into four categories: private life, family life, home, and correspondence.

Article 8 narrows this to 'private and family life', and the jurisprudence in the first two categories is overwhelming in comparison to the comparatively few decisions involving home and communication. There is no clear distinction between private and family life, and certain issues, such as settled migrants' right to remain where they are, the right to register marriage, delivery, and matters relating to the deceased, may be reviewed under both categories. Some settled migrants will not have appropriate familial links in the country; thus, their claim will be based on the right to privacy. In practice, the proportionality analysis is likely to be very similar.

It then, as a general rule, evaluates the criteria outlined in paragraph 2 to determine whether the "interference" violates the Convention. However, the Court's opinions on article 8 do not always include a full examination of the conditions in paragraph 2.

After determining that article 8 applies, the Court attempt to analyze the “inconvenience” that the interference generates for the applicant, sometimes ruling that it is serious enough to find a breach, while in other situations adopting the position that it is not.

Article 8(1) is the sole substantive article of the Convention that uses the word “respect”. The word is also used in the title of article 1, as a result of Protocol No. 11. Article 12 of the Universal Declaration of Human Rights, which is taken from Article 8(1) of the Convention, also does not utilize the word “respect”. The Court acknowledges the ambiguity of the idea of “respect”, particularly when it comes to the positive responsibilities it implies. Article 8.1 of the Council of Europe's European Convention for Human Rights (ECHR) and Article 7 of the EU Charter for Fundamental Rights (EUCFR) both protect privacy. However, the Convention does not guarantee absolute protection. Article 8.2 specifies the conditions under which interference with this right is permitted. According to Article 8.2, a legislation is acceptable if it anticipates interference, is essential in a democratic society (and reasonable), and aims to achieve a legitimate goal (Gellert & Gutwirth, 2013).

Under Article 8, the European Court of Human Rights (ECtHR) has recognized the importance of protecting various aspects of an individual's life, such as moral, psychological, and physical integrity, personal development, professional relationships, access to professions, and occupational risk information. Furthermore, the Court of Human Rights has extended privacy protection to the workplace, classifying some professional or commercial activities and premises

as part of an individual's "private life" and "home." As a result, the European Court of Human Rights (ECtHR) has devised a framework for examining disputes involving employee privacy, requiring governments to demonstrate compliance with Article 8(2) for public workers and positive requirements for private employees (Sychenko & Chernyaeva, 2019).

According to the Council of Europe (2022), the Court has concluded that Article 8 of the ECHR can include a wide range of problems, including bodily integrity, access to information and public documents, correspondence and communication secrecy, and domicile protection.

Clause (2) of Article 8 does not allow the "intervention of government authorities", but if these "interventions are in accordance with the law and cases that occur in a democratic society for the reasons of maintaining national security, public safety or economic well-being of the country, prevention of chaos and crimes, and protection of If the health and morals of others or the protection of their rights are deemed necessary, the government is allowed to enter this field. This clause itself is a very important restriction on privacy, and each of these words needs a precise definition. Because if the interpretation is expanded, it leaves the hands of governments free to restrict this right, and governments leave their hands hanging when this right is violated in paragraph 2. The area of government interference in the privacy domain has been examined several times.

The right to make personal choices, such as name and sexual orientation, has led to the recognition of human autonomy as a key principle in interpretation of art. 8 ECHR. The Court appears to prioritize "liberty" over a "bundle of subjective rights" approach to privacy. If the data are inherently linked to a person's privacy, the processing will automatically fall under Article 8 of the ECHR. However, if the data are not "essentially private," the Court will consider the scope of processing, such as whether the data is systematically stored. Does it keep the data, albeit not systematically, with a focus on the data subject? Could the data subject reasonably anticipate the processing to be delayed? In a number of cases, the Court has permitted data processing that violated the privacy of the data subjects because the scope of the processing was such that it interfered with their privacy, but not in all situations (Gellert & Gutwirth, 2013).

Article 8 distinguishes between positive and negative obligations, but the underlying principles apply to all instances. The Court may not always determine whether an interference is due to a denial of a right or a failure of the State to create an acceptable regulatory framework. When

considering private and family life, it's important to strike a balance between individual and community objectives, whether seen positively or negatively. Whether a negative or positive interpretation of article 8 is adopted, the State gains a certain margin of appreciation. In circumstances when the State must strike a balance between competing rights, the margin of appreciation is bigger if one individual's right to private and family life is violated as a result of another's exercise of a basic right. On the other hand, when a very significant aspect of an individual's existence or identity is at issue, the State's buffer is proportionally reduced. The same is true when the activities at stake concern a most sensitive element of private life (Schabas, 2017).

2.3.1 Case studies

In examining the cases of Malone v UK (1984), Barbulescu v Romania (2016), and Rotaru v Romania (2000), Halford v. United Kingdom (1997) a comprehensive understanding of the evolving landscape of privacy rights within the European legal framework emerges.

These cases show how privacy is influenced by technology developments and it brought some new areas beside the traditional ones. They also illustrate how privacy should be balanced between individual liberation and interest of states and employers. Malone v UK played an important role in UK privacy law. Subsequent cases used this case and court opinion about the evolving nature of technology. The case highlighted the risks associated with secret surveillance and emphasized the need for legal discretion to be clearly defined to prevent arbitrary interferences. Privacy rights to the evolving societal and technological landscape. These cases reflect the European court of Human Rights view about privacy which evolves harmonically in society progress. The jurisprudence showed that the privacy rights are not stable and they changed by the advancing technology. The ECHR decisions illustrate that privacy is a main stone of individual autonomy and dignity.

These cases guide us to understand a better knowledge of privacy in an evolving digital world. All cases were sourced from the official website of the court[1], which I downloaded and used as a resource. Over the years, there have been hundreds of cases related to Article 8 of the Convention. Meanwhile, cases dealing with advancements in technology were separated, and we selected the mentioned cases from this group. Additionally, these cases examine the conflict between the right to privacy and personal and collective interests, as well as the extent of government and employer interference.

[1] https://www.echr.coe.int/

2.3.2 Malone v. United Kingdom (1984)

Mr. James Malone was born in 1937 and is resident in Dorking, Surrey. In 1977, he was an antique dealer. The object of the request was to obtain a decision as to whether the facts of the case disclosed a breach by the respondent State of its obligations under Articles 8 and 13 (art. 8, art. 13) of the Convention (Malone v. United Kingdom, 2014, para 2).

On 22 March 1977, Mr. Malone was charged with a number of offenses relating to dishonest handling of stolen goods. His trial, which took place in June and August 1978, resulted in his being acquitted on certain counts and the jury disagreeing on the rest. He was retried on the remaining charges between April and May 1979.

In October 1978, the applicant instituted civil proceedings in the Chancery Division of the High Court against the Metropolitan Police Commissioner seeking, inter alia, declarations to the effect that interception, monitoring and recording of conversations on his telephone lines without his consent was unlawful, even if done pursuant to a warrant of the Secretary of State. The Solicitor General intervened in the proceedings on behalf of the Secretary of State but without being made a party. On 28 February 1979, the Vice-Chancellor, Sir Robert Megarry dismissed the applicant's claim (Malone v. Commissioner of Police of the Metropolis (No. 2), [1979] 2 All England Law Reports 620; also reported at [1979] 2 Weekly Law Reports 700).

The applicant further believed that both his correspondence and his telephone calls had been intercepted for a number of years. He based his belief on delay to and signs of interference with his correspondence. As to his telephone communications, he stated that he had heard unusual noises on his telephone and alleged that the police had at times been in possession of information which they could only have obtained by telephone tapping.

He thought that such measures had continued since his acquittal on the charges against him. It was admitted by the Government that the single conversation about which evidence emerged at the applicant's trial had been intercepted on behalf of the police pursuant to a warrant issued under the hand of the Secretary of State for the prevention and detection of crime. According to the Government, this interception was carried out in full conformity with the law and the relevant procedures. No disclosure was made either at the trial of the applicant or during the course of the

applicant's proceedings against the Commissioner of Police as to whether the applicant's own telephone number had been tapped or as to whether other and, if so, what other, telephone conversations to which the applicant was a party had been intercepted. The primary reasons given for withholding this information were that disclosure would or might frustrate the purpose of telephone interceptions and might also serve to identify other sources of police information, particularly police informants, and thereby place in jeopardy the source in question. For similar reasons, the Government declined to disclose before the Commission or the Court to what extent, if at all, the applicant's telephone calls and correspondence had been intercepted on behalf of the police authorities. It was however denied that the resealing with adhesive tape or the delivery of the envelopes produced to the Commission was attributable directly or indirectly to any interception.

The Government conceded that, as the applicant was at the material time suspected by the police of being concerned in the receiving of stolen property and in particular of stolen antiques, he was one of a class of persons against whom measures of interception were liable to be employed. In addition, Mr. Malone believed that his telephone had been "metered" on behalf of the police by a device which automatically records all numbers dialed. As evidence for this belief, he asserted that when he was charged in March 1977 the premises of about twenty people whom he had recently telephoned were searched by the police. The Government affirmed that the police had neither caused the applicant's telephone calls to be metered nor undertaken the alleged or any search operations on the basis of any list of numbers obtained from metering. 18. In September 1978, the applicant requested the Post Office and the complaints department of the police to remove suspected listening devices from his telephone. The Post Office and the police both replied that they had no authority in the matter (Malone v. United Kingdom para 12-18). Mr. Malone filed a civil action against the Metropolitan Police Commissioner and requested the following declarations: The defendant argued that "tapping" or disclosing conversations on his phone lines without his consent, even with a Home Secretary warrant, violated his property, privacy, and confidentiality rights. On February 28, 1979, the Vice-Chancellor ruled that he lacked the authority to issue a declaration under Article 8 of the Convention. He performed a careful review of the domestic legislation relating to telephone tapping, held in substance that the practice of tapping on behalf of the police as stated in the Birkett report was legal, and so dismissed the lawsuit (Malone v. United Kingdom,1984, para 31).

After the Vice-Chancellor's judgment, the Government reviewed and debated the need for legislation on communication interception. On April 1, 1980, the Home Secretary announced in Parliament that the Government had decided not to introduce legislation after carefully considering the Vice-Chancellor's suggestions (Malone v. United Kingdom, 1984, para 37).

Metering is the procedure of using a meter check printer to record phone numbers, time, and duration of calls. It is a procedure developed by the Post Office for its own use as the corporation in charge of providing telephone services. The aims include charging subscribers accurately, investigating complaints of poor service, and preventing abuse of telephone service. When "metering" a telephone, the Post Office [now British Telecommunications] only uses signals sent to itself. The Post Office is not required by the Crown to preserve such documents. However, if they are kept, they may be required to produce them in civil or criminal actions.

“The usual method is to serve a subpoena duces tecum. The Post Office's position is comparable to that of any other party with relevant documents, such as a bank. The police and the Crown cannot compel the provision of Post Office records beyond customary procedures” (Malone v. United Kingdom ,1984, para 56).

The applicant alleged violation of Article 8 under two heads. In his submission, the first violation resulted from interception of his postal and telephone communications by or on behalf of the police, or from the law and practice in England and Wales relevant thereto; the second from "metering" of his telephone by or on behalf of the police, or from the law and practice in England and Wales relevant thereto (Malone v. United Kingdom ,1984, para 62).

Telephone conversations are considered "private life" and "correspondence" under Article 8, so the admitted measure of interception constituted an "interference by a public authority" with the applicant's right under paragraph 1 of Article 8.

This case played an important role in privacy limitation and showed the government's restrictions about controlling people. Based on this case we could find a practical case which represented the. government limits on surveillance.

The Court distinguished between metering by a service provider for invoicing and similar purposes, which does not violate article 8, and the use of telephone data by law enforcement

personnel for investigative purposes. The release to the police of information regarding numbers that were telephoned by the telephone company constitutes an interference with the right to privacy (Schabas, 2017).

Due to the Interception of Communications Act 1985, the applicant was unable to provide sufficient proof to support their claims. Following the Court's decision in Malone v UK 1984, the 1985 Act was created to establish a clear statutory framework for authorizing the interception of communications on public systems. Except under limited instances, intentional communication interception is a crime. One exception is for interception under a warrant granted by the Secretary of State under section 2 of the Act. The applicant was unable to present evidence of a warrant or interception by a public servant in proceedings before the Industrial Tribunal due to Section 9 of the Act's prohibition on such evidence. After requesting an investigation by the Interception of Communications Tribunal, the applicant was informed that there was no violation of the Act. However, it was unclear whether any interception occurred (Boyle, 1997).

According to Chesterman (2010), the British standards for allowing wiretaps were found to be quite unclear. The Court ruled that the law did not clearly define the scope of discretion granted to public bodies. The Malone Court ruled that individuals should not be able to predict when authorities will intercept their communications. However, the law must be clear enough to indicate when authorities can use such secretive and potentially abusive powers. After this case ruled that the lack of statutory authorization for intercept warrants breached Article 8 of the Convention on Human Rights, the government enacted the Interception of Communications Act in 1985. The Interception of Communications Act 1985 made intentionally intercepting a communication a criminal offense and gave the Secretary of State statutory authority to issue warrants 'in the interests of national security, or for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom'. The Police Act of 1997 made the police's surveillance capabilities statutory (Barnett, 2002).

2.3.3 Halford v. United Kingdom (1997)

Ms Halford was promoted to Assistant Chief Constable with Merseyside Police in May 1983. Based on this fact she was the highest-ranking women officer in the UK. Ms Halford sought unsuccessfully for the position of Deputy Chief Constable on eight occasions over the next seven years, in response to vacancies in Merseyside and other police administrations. Home Office permission was necessary to be considered for advancement to this position. According to the applicant, this was routinely withheld on the recommendation of the Chief Constable of Merseyside Police, who objected to her commitment to gender equality. Following a subsequent rejection to advance her in February 1990, Ms Halford filed an action in the Industrial Tribunal on 4 June 1990 against, among others, the Chief Constable of Merseyside and the Home Secretary, alleging sex discrimination (Halford v. United Kingdom, 1997, para 9-11).

On June 14, 1990, the Merseyside Police Authority's Chairman and Vice-Chairman were constituted as a "Special Committee" to handle the concerns raised by the discrimination case. Ms Halford claims that in response to her complaint to the Industrial Tribunal, certain Merseyside Police Authority officers initiated a "campaign" against her.

Thus, on 14 September 1990, the Special Committee forwarded to the Senior Officers' Disciplinary Committee a report produced by the Chief Constable concerning an alleged instance of misconduct on Ms Halford's part on 24 July 1990. On 20 September 1990, the Disciplinary Committee decided to conduct a formal investigation, refer the case to the Police Complaints Authority, and file charges on 8 February 1991. Ms Halford was suspended on full pay beginning December 12, 1990. The decisions were challenged by way of judicial review in the High Court by her. Mr Justice MacPherson delayed the case in September 1991 in anticipation of a possible settlement. However, the parties were unable to reach an agreement, and the case was remanded to him on December 20, 1991.

Ms Halford had her own office and two telephones, one of which was for personal use as Assistant Chief Constable. These phones were part of the Merseyside police internal telephone network, which was separate from the public network. There were no restrictions on her use of these telephones, and no guidance was given to her, except for an assurance from the Chief Constable shortly after she instituted the proceedings in the Industrial Tribunal that she had authority to attend

to the case while on duty, including by phone. Furthermore, because she was regularly "on call," Merseyside police paid a significant portion of her home telephone charges. Her home phone was a telephone device that was linked to the public telecommunications network via the "network termination point."(Halford v. United Kingdom, 1997, para 11-16).

She claims that calls from her home and workplace phones were intercepted to collect information to use against her in the discrimination proceedings. She presented the Commission with a variety of evidence in support of these charges. Furthermore, she informed the Court that on April 16, 1991, she was advised by an anonymous source that the source had just discovered the Merseyside police investigating transcripts of talks conducted on her home phone. For the purposes of the case before the Court, the Government recognized that the applicant had presented enough evidence to indicate a reasonable chance that calls made from her office phones were intercepted.

They did not, however, accept that she had adduced sufficient evidence to show such a reasonable likelihood in respect to her home phone (Halford v. United Kingdom, 1997, para 17).

On December 6, 1991, Ms Halford applied to the Interception of Communications Tribunal ("the Tribunal") for an investigation under Section 7 of the 1985 Act. In a letter dated February 21, 1992, the Tribunal informed her that its investigation had determined that there was no violation of sections 2 to 5 of the 1985 Act in her case. In a letter dated March 27, 1992, the Tribunal confirmed that it could not clarify whether any interception had actually taken place (Halford v. United Kingdom, 1997, para 19).

Ms Halford protested to the Commission that the interception of calls made from her office and home telephones constitutes unreasonable inferences with her rights to respect for her private life and freedom of speech, according to Articles 8 and 10 of the Convention. The Government argued that Ms. Halford's workplace phone calls were not protected by Article 8 (art. 8), because she could not have had a reasonable expectation of privacy in relation to them. During the hearing before the Court, counsel for the Government stated that an employer should, in principle, be able to monitor calls made by employees on telephones provided by the employer without the employee's prior knowledge.

There is no evidence that Ms Halford, as a user of the Merseyside police headquarters' internal telecommunications system, was warned that calls made over that system could be intercepted. The Court believes she had a legitimate expectation of privacy for such calls, which was supported by a variety of considerations. As Assistant Chief Constable, she had exclusive use of her office, which included two telephones, one of which was explicitly earmarked for her personal use. Furthermore, in response to a memorandum, she was assured that she may use her office telephones for her sex-discrimination complaint (Halford v. United Kingdom, 1997, para 45).

According to Article 8 para. 2 (art. 8-2), any interference by a public body with an individual's right to respect for private life and correspondence must be "in accordance with the law".

According to the Court's telephone calls conducted from the house are covered by the concepts of "private life" and "correspondence" under Article 8 of the Convention. Indeed, the government did not contest this. Article 8 (art. 8) thus applies to this section of Ms Halford's complaint.

Ms Halford sought restitution for the breach into her privacy and the pain it caused. She informed the Court that in 1992, she needed medical attention for stress.

Given that the interception of Ms Halford's calls on her office telephones at Merseyside police headquarters, which is not subject to any domestic law regulation, appears to have been carried out by the police with the primary goal of gathering material to be used against her in sex-discrimination proceedings, the Court considers what occurred to be a serious infringement of her rights by those involved. However, there is no evidence to establish that Ms Halford's stress was caused by the eavesdropping of her calls rather than her prior issues with Merseyside police. Taking these factors into account, the Court believes that GBP 10,000 is a fair and reasonable amount of compensation (Halford v. United Kingdom, 1997, para 76).

According to the case (Halford v. United Kingdom, 1997, paragraph 83) that both professional and personal phone calls may fall under the definitions of "private life" and "correspondence" in Article 8 § 1.

Ms Halford was not warned about the possibility of interception when using the internal telecommunications system at Merseyside Police Headquarters. The Court ruled that she had a reasonable expectation of privacy during such calls (Halford v. United Kingdom, 1997, para 45).

On June 25, 1997, nine justices from the Court of Human Rights unanimously found a violation of the Convention. The Court also decided that domestic law did not provide a way for a complaint like this to be resolved. This lawsuit addressed, for the first time, the subject of employees' right to privacy at work. Government attorneys unsuccessfully contended that the tapped telephones were government property and hence not protected under the Convention. cases such as Halford v United Kingdom (1997) had successfully challenged domestic law (Barnett, 2002).

The Court has frequently applied Article 8 to employment, professional, and business activity. In the case of communications in the workplace by telephone or e-mail, and use of the Internet, employees may have a reasonable expectation of privacy (Schabas, 2017).

This decision confirms the Court's broad reading of the terms 'private life' and 'correspondence' in Article 8. Many will appreciate the Court's recognition that calls made from both business and residential locations are covered by these provisions. However, it appears that there is no universal principle stating that such calls will always be covered. In its decision, the Court stated that the specific circumstances of this case were crucial in determining whether such calls were covered. The evidence was strong. The applicant was not informed that calls could be intercepted; she was provided two telephones, one for private use, and was assured that she could use her office telephones for the purposes of her sex discrimination lawsuit. In less compelling circumstances, it appears that such calls may possibly be held as not 'private'.

Employers will, understandably, aim to reduce privacy expectations by establishing clear contractual rules governing the types of surveillance that will be utilized. However, Article 8 may necessitate the release of information in any situation. Outside the workplace, Article 8 has been associated with a positive responsibility to supply persons with information about their personal history and health (even to the point of creating information) in order to ensure that their privacy is protected. Furthermore, presuming Article 8 is invoked, secret surveillance is unlikely to be 'in compliance with law' if information is not provided. The point was articulated in Malone v United Kingdom, albeit in the context of police surveillance. It should follow that if secret monitoring is to be conducted at the workplace, some previous indication must be given as to the kinds of situations and reasons for which it will be utilized (unless that would defeat its entire purpose) (Ford, 2002).

According to Mann (2002) The basis for the decision was that she had a reasonable expectation that such calls would remain private. Advanced telecommunications devices like internal networks and personal devices, people's expectations have changed and become more complex. This case was very important since the nature of communication due to advances in technology has changed while the court also has updated judgment criteria too.

2.3.4 Bărbulescu v. Romania (2016)

The applicant was born in 1979. From August 1, 2004 until August 6, 2007, he worked as a sales engineer for a Romanian private corporation ("the employer"), in Bucharest. At his employer's request, he set up an instant messaging account on Yahoo Messenger, an online chat service that allows for real-time text transmission over the internet, to answer client inquiries. He already has an additional personal Yahoo Messenger account. According to the employer's internal regulations, employees were barred from using corporate resources in the following ways:

> "Any disturbance of order and discipline on company premises shall be strictly forbidden, in particular:
>
> ...
>
> – ... personal use of computers, photocopiers, telephones or telex or fax machines."

(Bărbulescu v. Romania,2016, para 10, 11,12)

The regulations made no mention of the employer's ability to monitor employee conversations. According to documents presented by the Government, the applicant was notified of the employer's internal regulations and signed a copy of them on December 20, 2006, after becoming acquainted with their contents (Bărbulescu v.Romania, para 13,14).

During the time he was being observed, the applicant exchanged communications with his brother and fiancée; the conversations were personal in nature, with some being intimate. The transcript also included five communications exchanged by the applicant with his fiancée via his personal Yahoo Messenger account; these messages did not contain any intimate information (Bărbulescu v.Romania, para 21).

The company terminated the applicant's employment agreement. The applicant filed an application with the Bucharest County Court ("the County Court"), challenging his dismissal. He requested that the court set aside his dismissal, order his employer to pay him the amounts owed to him in terms of wages and other entitlements, and reinstate him in his position; and third, order the employer to pay him 100,000 Romanian lei (approximately 30,000 euros) in damages for the harm caused by the manner of his dismissal, as well as reimburse his costs and expenses. The applicant claimed that his dismissal by his employer was founded on a violation of his right to privacy and

correspondence, and that by failing to revoke that measure, the domestic courts failed to fulfill their duties to defend the right in question. He relied on Article 8 of the convention (Bărbulescu v.Romania,para24-25).

In a judgment issued on December 7, 2007, the County Court rejected the applicant's application and confirmed that his dismissal was valid. The applicant made an appeal to the Bucharest Court of Appeal ("the Court of Appeal"). He restated the points he had made before the first-instance court, claiming that the court had not struck a fair balance between the interests at stake, unfairly prioritizing the employer's interest in having discretion over its employees' time and resources. He also claimed that neither the internal regulations nor the information notice provided any indication that the employer could monitor employees' communications. The Court of Appeal denied the applicant's appeal in a judgment dated June 17, 2008 (Bărbulescu v.Romania, para 29, 30).

The pertinent provisions of the Romanian Constitution include:

Article 26

“1. The public authorities shall respect and protect intimate, family and private life.”

Article 28

“The secrecy of letters, telegrams, other postal communications, telephone conversations and any other lawful means of communication is inviolable.”

As written at the time, the Labor Code offered:

> “1. The employer shall in principle have the following rights:
>
> ...
>
> (d) to supervise how [employees] perform their professional tasks;
>
> ...
>
> 2. The employer shall in principle have the following duties:
>
> ...
>
> (i) to guarantee the confidentiality of employees’ personal data.”

In its decision of January 12, 2016, the Chamber determined that Article 8 of the Convention applied in the current case. Regarding the concept of reasonable expectation of privacy. The Court notes that in the proceedings before the Chamber, the applicant claimed that his employer's decision to terminate his contract was based on a violation of his right to respect for his private life and correspondence, as guaranteed by Article 8 of the Convention, and that by failing to revoke that measure, the domestic courts failed to fulfill their obligation to protect the right at issue. On January 12, 2016, the Chamber deemed the complaint admissible (Bărbulescu v.Romania, para 61).

The government maintained that the petitioner had no right to "privacy" in the conversations he exchanged through an instant messaging account set up for business purposes. They argued that messages sent by an employee utilizing the technical facilities provided by his employer had to be viewed as professional in nature unless the person clearly labeled them as private, citing French and Cypriot case law. They noted that it was not technically possible using Yahoo Messenger to mark messages as private; nevertheless, the applicant had an adequate opportunity, during the initial stage of the disciplinary proceedings, to indicate that his communications had been private, but had chosen to maintain that they had been.

The Government relied on three additional considerations to argue that Article 8 of the Convention was not relevant in this case. To begin with, there was no evidence that the transcript of the applicant's communications had been disclosed to his work colleagues; the applicant had produced the full transcript of the messages in the proceedings before the domestic courts, without requesting any restrictions on access to the documents in question. Second, the national authorities used the transcripts of the messages as evidence since the applicant had requested it and the prosecuting authorities had previously determined that the surveillance of his communications was lawful.

The applicant made no representations regarding the applicability of Article 8 of the Convention, but frequently stated that his contacts had been private in character. He further claimed that, because he had created the Yahoo Messenger account in question and was the only one who knew the password, he had a reasonable expectation of privacy in his discussions. He further claimed that he had not been notified by his company about the surveillance of his communications (Bărbulescu v.Romania, para 65. 66).

At this level of its analysis, it deems it useful to emphasize that "private life" is a wide concept that cannot be exhaustively defined. At this point in its investigation, it believes it is important to emphasize that "private life" is a wide concept that cannot be fully defined. Article 8 of the Convention preserves the right to personal development, whether in terms of personality or personal autonomy, which is a key element guiding the interpretation of the Article 8 safeguards. The Court recognizes that everyone has the right to live privately, free of unwelcome scrutiny.

It also argues that it would be too limiting to limit the concept of "private life" to an "inner circle" in which the individual may live his or her own personal life as he or she chooses, thus eliminating totally the outside world not covered within that circle. Article 8 thus ensures a right to "private life" in its broadest sense, including the freedom to lead a "private social life," i.e., the ability for the individual to form his or her social identity. In this regard, the right in question enshrines the ability of approaching others to create and develop connections with them.

The Court finds that the term "private life" might include professional activities or activities that take place in a public context. Restrictions on an individual's professional life may fall under Article 8 if they have an impact on how he or she builds his or her social identity through relationships with others. In this regard, it is worth noting that the majority of people have a considerable, if not the greatest, opportunity to create relationships with the outside world while working. It is obvious from the Court's case-law that communications from business premises as well as from the home can be encompassed by the notions of "private life" and "correspondence" within the meaning of Article 8 of the Convention.

The Court's case law makes it clear that communications from both commercial and residential premises may be covered by the concepts of "private life" and "correspondence" under Article 8 of the Convention. In order to determine whether the concepts of "private life" and "correspondence" are applicable, the Court has on various occasions considered whether individuals had a reasonable expectation that their privacy would be respected and preserved.

In that regard, it has stated that a reasonable expectation of privacy is a substantial, but not always conclusive consideration (Bărbulescu v.Romania, para 70).

Applying these principles to the current case, the Court first notes that the type of online instant messaging service at issue is merely one of the forms of communication that allow people to have a private social life. Simultaneously, the concept of "correspondence" encompasses the sending and receiving of communications, even if they are transmitted from an employer's computer (Bărbulescu v.Romania, para 74, 75).

After considering all of the foregoing, the Court decides that the applicant's professional interactions were covered by the principles of "private life" and "correspondence". As a result, Article 8 of the Convention applies in this case (Bărbulescu v.Romania, para 81).

While the borders between the State's positive and negative responsibilities under the Convention are difficult to define precisely, the underlying principles are identical. In all cases, respect must be had in particular to the fair balance that has to be struck between the competing interests of the individual and the community as a whole, subject in any case to the State's margin of appreciation (Bărbulescu v.Romania, para 112).

“The Convention's Article 8 has been violated by eleven votes to six. The finding of a violation is sufficient justification for the applicant's non-pecuniary damage. The respondent State must pay the applicant EUR 1,365 (one thousand three hundred and sixty-five euros) in costs and expenses within three months. That from the expiry of the above-mentioned three months until settlement, simple interest will be payable on the aforesaid amount at a rate equal to the European Central Bank's marginal lending rate during the default period plus three percentage points; Unanimously dismisses the applicant's remaining claim for just satisfaction.”

Since 1992, the European Court of Human Rights has broadened the scope of Article 8 of the ECHR to include workplace communication interceptions. Article 8 protects private life and correspondence, including telephone calls, e-mails, internet usage monitoring, and instant messaging. The ECtHR defines 'interferences' under Article 8 to include drug testing, video surveillance, storing and releasing information collected during a security evaluation, disclosing information about a criminal conviction to a prospective employer, and investigating the sexual lives and discharge of homosexual members of the UK armed forces (Grygorovych, 2016).

In employee surveillance cases like Barbulescu v Romania, the Court emphasizes the necessity of building relationships with colleagues, which many people do while at work. The Court ruled that Mr. Barbulescu's professional activities were protected by the right to private life, and his Messenger Account communications were considered 'correspondence' under Article 8. The Court's analysis of whether the right to private life was exercised went beyond that. Consistent with its approach in surveillance matters both within and outside the workplace, it then considered whether Mr Barbulescu had a reasonable expectation that his privacy would be maintained. The concept of “reasonable expectation of privacy standards” was borrowed from the United States legal system. It was established by the Supreme Court to address the limitations of geographical conceptualizations of privacy shown by improvements in surveillance technology.

By assessing whether or not the individual had an expectation of privacy that society recognizes as reasonable, the test was intended to inspire a more expansive approach to the way privacy was defined. Paradoxically, the ECtHR's application appears to achieve the opposite result. Recognizing that the pluralistic approach to Article 8 risks indeterminacy, the Court is eager to limit its reach. In order to determine whether the right to privacy is violated, it examines if the employee was informed that (s)he would be observed. The majority ruled that, even if Mr. Barbulescu was notified, he was being monitored, he was not informed of the 'extent and character' of the anticipated monitoring. Nor was he aware that the substance of his communications could be accessed (Jervis, 2018).

This case also shows how the court deals with technological advances. In this case, the court updated its judgment with the advancement of technology and its use, and limited the monitoring of the work environment to informing and legislating.

2.3.5 Rotaru v Romania (2000)

The applicant, born in 1921, was a lawyer by profession. He is currently retired and resides in Bârlad. In 1946, after the communist regime was established, the applicant, who was then a student, was refused permission by the prefect of the county of Vaslui to publish two pamphlets, "Student Soul" (Suflet de student) and "Protests" (Proteste), because they expressed anti-government sentiments. Dissatisfied with the refusal, the applicant addressed two letters to the prefect, protesting the new regime's suppression of freedom of expression. As a result of these letters, the applicant was arrested on July 7, 1948.

On September 20, 1948, the Vaslui People's Court convicted the applicant of insulting behavior and sentenced him to a year in jail.(Rotaru v Romania , 2000, para 7,8 and 9) The applicant sued the RIS, claiming that he was never a member of the Romanian legionary movement, that he attended the Faculty of Law at Iaşi University rather than the Faculty of Sciences, and that some of the other information provided by the RIS in its letter of December 19, 1990 was false and defamatory. Under the Civil Code's tort liability provisions, he sought damages from the RIS for the non-monetary harm he had suffered. He further sought an order, without citing any specific legislative law, that the RIS alter or destroy the file holding information about his alleged legionnaire history.

On June 13, 1995, the applicant filed a damages case against all of the judges who denied his request to have the file modified or deleted. He based his action on Article 3 of the Civil Code, which deals with denials of justice, and Article 6 of the Convention. According to the applicant, both the County Court and the Vaslui Court of Appeal declined to register his lawsuit (Rotaru v Romania, para 14-15).

The relevant provisions of the Constitution read as follows:

A. The Constitution Article 20

> "(1) The constitutional provisions on citizens' rights and liberties shall be interpreted and applied in accordance with the Universal Declaration of Human Rights and with the covenants and other treaties to which Romania is a party.

(2) In the event of conflict between the covenants and treaties on fundamental human rights to which Romania is a party and domestic laws, the international instruments shall prevail."

Article 21

"(1) Anyone may apply to the courts for protection of his rights, liberties and legitimate interests.

(2) The exercise of this right shall not be restricted by any statute."

B. The Civil Code

The relevant provisions of the Civil Code are worded as follows:

Article 3

"A judge who refuses to adjudicate, on the pretext that the law is silent, obscure or defective, may be prosecuted on a charge of denial of justice."

Article 998

"Any act committed by a person who causes damage to another shall render the person through whose fault the damage was caused liable to make reparation for it."

Article 999

"Everyone shall be liable for damage he has caused not only through his own act but also through his failure to act or his negligence."

According to the applicant's submission, the keeping and use of the file on him violated the law because domestic law was not sufficiently precise to indicate to citizens under what circumstances and on what terms public authorities were authorized to file and use information about their private lives. Furthermore, domestic law did not adequately specify the way of exercise of those authorities and did not provide any safeguards against abuses (Rotaru v Romania, para 50).

“The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the 'law', requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention ... The phrase thus implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 ... Especially where the power of the executive is exercised in secret, the risks of arbitrariness are evident (Rotaru v Romania, 2000, para 55).

The Court notes in this context that section 8 of Law no. 14/1992 specifies that information impacting national security can be obtained, documented, and maintained in secret files.

The "quality" of the legal rules relied on in this case must therefore be examined, with a view, in particular, to determine whether domestic law laid down with sufficient precision the circumstances under which the RIS could store and use information relating to the applicant's personal life. (Rotaru v Romania, 2000, para 56).

It also observes that, while Section 2 of the Law enables the competent authorities to allow interferences essential to prevent and counter threats to national security, the grounds for such interferences are not specified with sufficient detail (Rotaru v Romania, 2000, para 58).

The Court decided that the RIS's retention and use of information on the applicant's private life were not "in accordance with the law," which is sufficient to establish a violation of Article 8. Furthermore, in this case, that reality hinders the Court from assessing the validity of the purpose sought by the ordered measures and determining whether they were "necessary in a democratic society" if the aim was lawful. As a result, an article 8 violation occurred (Rotaru v Romania, 2000, para 62, 63).

Schabas, (2017) believes that, Article 8.2 governs how private information is stored and released. Article 8 applies to information or data that is not necessarily private or secret. Where public information is routinely collected and preserved in official files, article 8 may be invoked.

Laws granting discretion to public authority must be clear and describe how it will be exercised According to the Court, such information, when systematically collected and preserved in a file held by State agents, falls within the scope of "private life" under Article 8, Section i of the

Convention. Article 8 was accordingly invoked. The Court determined that both the storage and use of that material, together with a refusal to give the applicant the opportunity to reject it, constituted an interference with his right to respect for family life as granted by Article 8, Section I. In that connection, the Court noted that in its judgment of 25 November 1997 the Bucharest Court of Appeal had confirmed that it was lawful for the RIS to hold the information as depositary of the archives of the former security services.

That being so, the Court could conclude that the storing of information about the applicant's private life had had a basis in Romanian law. Regarding the need of foreseeability, the Court noted that no domestic law provision limited the exercise of those rights. Domestic law, for example, did not specify the types of information that could be recorded, the categories of people against whom surveillance measures such as gathering and storing information could be used, the circumstances under which such measures could be used, or the procedure to be followed. Similarly, the law included no provision for limiting the age or duration of information storage. As a result, the Court decided that domestic legislation did not properly define the extent and method of exercising the relevant discretion granted to public authorities. The Court found that the RIS's preservation and use of information about the applicant's private life were not "in accordance with the law," which was enough to prove a violation of Article 8 *(2000).*

The Court noted that the RIS's letter of December 19, 1990, contained information regarding the applicant's life, including studies, political activity, and criminal record, some of which were obtained almost 50 years ago. The Court ruled that material collected and retained in a file by State agents falls under "private life" as defined in Article 8 § 1 of the Convention. Article 8 was accordingly invoked. The law did not limit the age or duration of information retention.

The Court ruled that the RIS violated Article 8 by holding and using information on the applicant's private life that was not "in accordance with the law". In this case, the Court was unable to assess the constitutionality of the mandated measures and determine if they were "necessary in a democratic society" (assuming the goal was legitimate) (Directorate General Human Rights and Rule of Law, 2018).

The Court found that collecting and using information without allowing the applicant to reject it violated his right to respect for family life under Article 8 § 1.

In some other cases the court mentioned some related points with this case. for instance, Liberty and Others v. The United Kingdom and Big Brother Watch and Others v. The United Kingdom. In this case the court describes the relation between the authority's power to surveillance and the danger of arbitrariness. The legislation must consequently be accessible to the individual affected and predictable in terms of its repercussions. It is consequently critical to have clear, specific guidelines on secret surveillance methods, especially when the technology available for usage becomes increasingly sophisticated. Domestic legislation must be sufficiently explicit to provide citizens with an adequate indication of the situations and conditions under which public authorities are empowered to resort to any such actions. It will also be required to establish clear precise guidelines that offer citizens a sufficient indication of the circumstances and conditions under which the authorities are authorized to make such a request.

Chapter3
Privacy and Data Protection in the Charter of Fundamental Rights of the European Union

3.1 Introduction to Chapter

European data protection legislation is a relatively new topic of EU law. Prior to the establishment of European data protection law, data protection laws existed in Europe. Several country states began to legislate on data protection issues from the 1960s onwards, developing key ideas that have since formed part of the European data protection law.

Despite the European Parliament's constant advocacy for European data protection legislation, the European Communities did not pursue legislative initiatives during the initial period of data protection regulation. The Commission, which eventually rebranded itself as a proponent of EU data protection law, declined to propose such legislation for various reasons.

Initially, the company stated that it had no plans for 'data banks', indicating a limited understanding of data protection. For a long time, the Commission was almost solely concerned with the economic promise of digitalization, computerization, and telecommunications, ignoring the corresponding need for European data protection regulation.

As a result, the EU first failed to shape this emerging field in Europe and beyond. As the need for international coordination increased, new international organizations stepped in to fill the hole. In 1980, the OECD issued guidelines on privacy and transborder flows of personal data, building on the US's fair information practice principles. These guidelines included concepts such as data collection and use limitation, data quality and security, and purpose specification principles (Streinz, 2021).

According to Fact Sheets of the European Union (2023) “The Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data was the first legally binding international instrument adopted in the field of data protection. Its purpose was to secure, for every individual, respect for their rights and fundamental freedoms, and in particular their right to privacy, with regard to automatic processing of personal data. The Protocol amending the Convention seeks to broaden its scope, increase the level of data protection and improve its effectiveness”.

The Treaty of Lisbon revised the EU's data protection law, emphasizing the importance of fundamental rights protection while also addressing potential national security consequences. Until recently, the EU's data protection was governed by a variety of legislative instruments.

Former first-pillar instruments include Directive 95/46/EC on data protection (replaced by the General Data Protection Regulation in May 2018), Directive 2002/58/EC on e-privacy (modified in 2009; new proposal currently under consideration), Directive 2006/24/EC on data retention (declared invalid on 8 April 2014 by the Court of Justice of the European Union in the case Digital Rights Ireland Joined Cases C-293/12 and C-594/12 (ECLI: ECLI:EU:C:) as well as former third-pillar instruments such as the Council Framework Decision 2008/977/JHA of November 27, 2008 on the protection of personal data processed in the context of police and judicial cooperation in criminal matters (replaced in May 2018 by the Data Protection Law Enforcement Directive).

The Court of Justice competed with national constitutional courts. Prior to the Charter, the Court relied primarily on Strasbourg case law. After the Charter went into effect, Luxembourg avoided making allusions to the right to privacy, which is included in both the Charter and the ECHR. This could explain why the latter does not explicitly state a right to data protection (Craig and de Búrca , 2021).

According to information on the Court of Justice of the European Union website (2024) the main Role Of the court is to ensure the EU law is interpreted and applied consistently in all EU nations; beside that, ensure that countries and EU institutions comply with EU law.

The Court of Justice consists of one judge from each EU country, plus 11 advocates general.

The General Court has two judges from each EU country. It was established in 1952.The Court of Justice of the European Union (CJEU) interprets EU law to ensure that it is applied consistently throughout all EU nations and resolves legal disputes between national governments and EU institutions. It can also be used by people, businesses, or organizations to take legal action against an EU institution if they believe it has violated their rights. The CJEU issues decisions on cases presented before it.

The European Court of Justice has significantly broadened data privacy protection, based on the legally enforceable Charter of Fundamental Rights of the European Union to assure a leading level of protection in the sector. The concept of data protection as a fundamental right is strongly ingrained in European society. According to Recital 1 of the GDPR, 'the protection of natural persons in relation to the processing of personal data is a basic right'(European Agency for Fundamental Rights, 2018).

According to Bratic (2013),''the ECJ's jurisdiction has been greatly shaped by the preliminary reference procedure, which allows (and often requires) national courts to refer disputed issues to

the EU judicial body. In response, the ECJ typically elucidates the applicable legal standard and then returns the case to the domestic court for final disposition. Because the ECJ can leave the ultimate determination of a dispute to the domestic court, a culture of deference in internal affairs, termed the "margin of appreciation," has developed in the ECJ's human rights case law.’’

Article 7 of the European Union's Charter of Fundamental Rights states:

"Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications."

The European Union's Charter of Fundamental Rights clearly addresses the protection of personal data:

Article 8 - Protection of personal data

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.

According to GDPR Article 5(e), data must be maintained in a form that allows data subjects to be identified for no longer than is required for the purposes for which the personal data are processed. As a result, if they are no longer required, the controller must anonymize them or erase them at the request of the data subject. The controller must also consider the risk of re-identification based on the "time, resources, and effort required in light of the nature of the data."

base on article 5 of GDPR

“Personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

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 or organizational measures (‘integrity and confidentiality’).

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

Advancements in technology bring people serious concerns about the protection of their privacy. Due to these governments and legal systems had to play in this playground. The digital age has changed the traditional concept of privacy and has made the legal institutions to adapt and evolve in response to these changes. The digital age has changed the traditional concept of privacy and has made the legal institutions to adapt and evolve in response to these changes. Court of justice of the European Union played an important role in shaping this new area in European Union.

The main aim of this chapter is examination of key cases that have pivotal influence on EU legal system which shed light on the dark sides of the concept of privacy and data protection. Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (2014), was like a revolution that changed the digital world and granted “right to be forgotten" which made people able to control their identity in the online world and after that people could request to remove their personal data.

Furthermore, the CJEU's decision in Schrems v. Data Protection Commissioner (2015) and its subsequent ruling in Schrems II (2020) are significant cases in understanding the complexities of international data transfer and EU-US privacy shield framework.

Besides that, cases such as Digital Rights Ireland v. Minister for Communications (2014) and Tele2 Sverige AB v. post-och telestyrelsen (2016) showed the state surveillance boundaries and protection of individuals communication data against intrusion by governmental authorities.

3.2.1 Google Spain SL, Google Inc v Agencia Española de Protección de Datos

Based on the case «On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) (‘La Vanguardia’), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr. Costeja González’s name in the search engine of the Google group (‘Google Search’), he would obtain links to two pages of La Vanguardia’s newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr. Costeja González’s name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts» (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González ,2014,para 14).

According to Google Spain and Google Inc., the activity of search engines cannot be considered processing of data that appears on third-party web pages displayed in the list of search results, because search engines process all information available on the internet without discriminating between personal data and other information. Furthermore, even if that action is classed as 'data processing', the operator of a search engine cannot be considered a 'controller' of that processing

because it has no knowledge of the data and has no control over it. According to the Greek Government's submission, the activity in question constitutes such 'processing'; however, because search engines serve only as intermediaries, the companies that run them cannot be considered 'controllers' unless they store data in a 'intermediate memory' or 'cache memory' for a period that exceeds what is technically required. The Court has already stated that the operation of loading personal data on an internet page must be viewed as such 'processing' within the meaning of Article 2(b) of Directive 95/46 (Google Spain ,2014, para 21-26).

In this regard, it should be noted that the processing of personal data carried out in the context of a search engine's activity differs from and is in addition to that carried out by website publishers, which consists of loading that data on an internet page.

Furthermore, it is undisputed that the activity of search engines plays a critical role in the overall dissemination of those data in that it makes them available to any internet user conducting a search on the basis of the data subject's name, including internet users who would not have found the web page on which those data are published. Furthermore, it is undisputed that the activity of search engines plays a critical role in the overall dissemination of those data in that it makes them available to any internet user conducting a search on the basis of the data subject's name, including internet users who would not have found the web page on which those data are published.

court stated at 55 paragraph of the case that:

“In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out ‘in the context of the activities’ of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.”

Google Spain and Google Inc. argue that, under the principle of proportionality, any request for the removal of information must be addressed to the publisher of the website in question because he bears the responsibility for making the information public, is in a position to assess the legality of that publication, and has the most effective and least restrictive means of rendering the information inaccessible. Furthermore, requiring a search engine operator to remove internet-

published information from its indexes would fail to take into account the basic rights of website authors, other internet users, and the operator itself.

According to the Austrian Government, a national supervisory authority may order such an operator to delete information published by third parties from its filing systems if the data in question has previously been found to be illegal or incorrect, or if the data subject has successfully objected to the publisher of the website on which that information was published.
Mr Costeja González, the Spanish, Italian, and Polish governments, as well as the Commission, argue that the national authority may directly order the operator of a search engine to remove from its indexes and intermediate memory information containing personal data published by third parties, without first contacting or simultaneously contacting the publisher of the web page on which that information appears. Furthermore, according to Mr. Costeja González, the Spanish and Italian governments, and the Commission, the fact that the information was lawfully published and is still available on the original web page has no bearing on the operator's obligations under Directive 95/46. On the other hand, according to the Polish government, that reality is such that it releases the operator from its obligations (Google Spain, 2014, para 64, 65).
Article 7 of the Charter ensures the right to privacy, and Article 8 clearly asserts the right to personal data protection. Article 8(2) and (3) specify that 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, that everyone has the right to access data collected concerning him or her and the right to have the data rectified, and that compliance with these rules is to be subject to control by an independent authority.
Article 7 of the Charter ensures the right to privacy, and Article 8 clearly asserts the right to personal data protection. Articles 8(2) and (3) state that such data must be processed fairly for specified purposes and on the basis of the person's consent or some other legitimate basis laid down by law, that everyone has the right to access data collected about him or her and the right to have the data rectified, and that compliance with these rules is subject to oversight by an independent authority.
Articles 6, 7, 12, 14, and 28 of Directive 95/46, among others, put these requirements into action. According to Article 12(b) of Directive 95/46, Member States must ensure that every data subject has the right to obtain from the controller, as appropriate, the rectification, erasure, or blocking of

data whose processing does not comply with the provisions of Directive 95/46, particularly because the data is incomplete or inaccurate. As this final point relating to the case when certain requirements referred to in Article 6(1)(d) of Directive 95/46 are not observed is stated by way of example and is not exhaustive, it follows that the non-compliant nature of the processing, which is capable of conferring upon the data subject the right guaranteed in Article 12(b) of the directive, may also arise from non-observance of the other conditions of lawfulness. That is imposed by the directive upon the processing of personal data.

according to paragraph 100 of the judgement:

"Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the

preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question".

The Court's interpretation of data protection laws. The Court of Justice's recognition of the 'right to be forgotten' in Google Spain exemplifies a fundamental-rights-driven interpretation of the established data protection right of erasure. The answer focused on whether Google Inc's data processing was related to its subsidiary Google Spain's promotion and sale of advertising space in the EU. The Court took a comprehensive approach to data protection matters, emphasizing the importance of protecting individuals' basic rights and avoiding circumvention.

The Court recognized that Google works as an economic whole. The company's advertising business focuses on the European market and is tied to its global search engine, regardless of organizational structure or data processing location (Craig, P., & de Búrca, G. 2021).

Craig and de Búrca (2021) argued that the Court's interpretation of data protection law is influenced by fundamental rights to data protection and privacy, which not only serve as rhetorical devices but also have worldwide implications. The right to be delisted (also known as the 'right to be forgotten') recognized by the Court of Justice in Google Spain is perhaps the clearest example of a fundamental-rights-driven reinterpretation of a long-standing data protection right—the right to erasure. The Court emphasized that economic interests do not override data subjects' fundamental rights, but failed to account for the complexity deriving from multipolar constellations in which numerous fundamental rights are implicated. Inadvertently, the ruling made Google the de facto arbiter of opposing interests. This reflects the institutional complexity of European data protection regulation in practice.

Google v. Spain highlighted the intersection of technology and law. The EUCJ's recognition of the right to be forgotten has had a significant influence on Google Inc.'s activities. From June to mid-September 2014, Google Inc. received 135,000 requests to erase 470,000 links, prompting Google Inc. to establish an entire division to process the right to be forgotten requests.

The ECJ did not adopt the Advocate General's advisory opinion and found unfavorable judgments for Google Inc. (and/or Google Spain SL). The ECJ recognized Google Inc. and Google Spain SL

as processors and controllers of personal data under EU Directive 95/46. The ECJ also recognized the right to be forgotten (Eckart, 2017).

EU data subjects can request that erroneous, inadequate, irrelevant, excessive, or outdated search results about them be removed. The Court ruled that interfering with privacy and data protection rights is only permitted if the public has a compelling interest in acquiring the material, such as a prominent figure.

The case raised many other issues, such as intermediary liability and the importance of maintaining a public archive, but the current contribution focuses on the territorial reach of EU law, particularly in light of US-EU jurisdictional issues in the context of how the decision was implemented. The Google Spain verdict has had an extraterritorial impact, but not to an undue extent. The judgment did not address the right to be forgotten territorial scope or its potential application beyond the EU. Despite its European origins, the ruling has had a significant impact on third-party states. In a US-EU context, the First Amendment's restriction on creating or enforcing a "right to be forgotten" reinforces concerns about its transferability across borders (Mistale, 2017).

Individuals have the right to challenge erroneous, inadequate, irrelevant, or excessive personal information used for data processing. The CJEU acknowledged that this right is not absolute. It must be balanced with other rights, including the public's right to obtain information. Erasure requests must be evaluated on a case-by-case basis to strike a balance between protecting the data subject's privacy and the legitimate interests of internet users.

The CJEU recommended factors to consider during the balancing exercise. If information is sensitive to an individual's private life and there is no public interest in its availability, data protection and privacy take precedence over the public's right to access it. If the data subject is a public figure or the material is of a sort that warrants public access, it may be acceptable to violate fundamental data protection and privacy rights. The CJEU observed that this right is not absolute and must be balanced with other rights, including the public's right to access information. To reconcile the fundamental rights to personal data protection and privacy of data subjects with the legitimate interests of all internet users, each request for erasure should be assessed individually. A search engine can facilitate access to private information that would otherwise be difficult to

find or link. This could potentially violate data subjects' fundamental rights to privacy and data protection.

3.2.2 Schrems v. Data Protection Commissioner (2015)

The request was made in proceedings between Mr. Schrems and the Data Protection Commissioner ('the Commissioner') over the latter's refusal to investigate Mr. Schrems' complaint that Facebook Ireland Ltd ('Facebook Ireland') transfers its users' personal data to the United States of America and stores it on servers in that country (Schrems v. Data Protection Commissioner, 2015, para 2).

Mr. Schrems, an Austrian resident living in Austria, has been using the Facebook social network ('Facebook') since 2008. Any person located in the European Union who intends to use Facebook must sign a contract with Facebook Ireland, a subsidiary of Facebook Inc., which is based in the United States. Some or all of the personal data of Facebook Ireland users residing in the European Union is transferred to Facebook Inc. servers in the United States for processing.

On June 25, 2013, Mr. Schrems filed a complaint with the Commissioner, essentially requesting that the latter utilize his statutory powers by prohibiting Facebook Ireland from transmitting his personal data to the US. In his complaint, he claimed that the legislation and practice in place in that country did not adequately protect personal data housed on its territory from public authorities' surveillance activities. Mr. Schrems refers to Edward Snowden's revelations on the activities of the US intelligence agencies, particularly the National Security Agency ('the NSA') (Schrems v. Data Protection Commissioner, 2015, para 26-28).

Mr. Schrems filed an action in the High Court, disputing the decision at issue in the main proceedings. After analyzing the evidence presented by the parties to the main proceedings, the High Court concluded that electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable public interests.

However, it said that Edward Snowden's revelations indicated a significant 'over-reach' by the NSA and other federal agencies. According to the High Court, Union citizens have no meaningful right to a hearing. Ex parted and secret procedures are used to oversee the activity of intelligence services. Once the personal data has been transported to the United States, it is capable of being

accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of their large-scale indiscriminate surveillance and interception. According to the High Court, Irish law prohibits the transfer of personal data outside national territory unless the other country provides adequate protection for privacy and basic rights and freedoms.

The importance of the Irish Constitution's guarantees of privacy and inviolability of the residence necessitates that any interference with such rights be proportionate and legal. The High Court ruled that bulk and indiscriminate access to personal data obviously violates the principle of proportionality and the fundamental values safeguarded by the Irish Constitution. To be considered consistent with the Irish Constitution, interception of electronic communications must demonstrate that it is targeted, that the surveillance of specific individuals or groups of people is objectively justified in the interests of national security or crime suppression, and that appropriate and verifiable safeguards are in place.

The High Court thinks that this matter involves the execution of EU legislation as referred to in Article 51 of the Charter, and thus the legitimacy of the decision at question in the main proceedings must be reviewed in light of EU law. The High Court ruled that Decision 2000/520 fails to meet Charter Articles 7 and 8, as well as the principles established by the Court of Justice in Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238). The High Court further observes that in his action, Mr. Schrems concerns the constitutionality of the safe harbor regime created by Decision 2000/520, which gives rise to the decision at issue in the main proceedings.

Thus, even though Mr. Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on the basis of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorized the Commissioner to break free, if appropriate, In those circumstances, the High Court resolved to pause the proceedings and refer the following questions to the Court of Justice for a preliminary decision:

"Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case,

the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding? Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?"
(Schrems v. Data Protection Commissioner, 2015, para 29-36).

Regarding the powers available to national supervisory authorities in relation to transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to establish one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. Furthermore, such duty arises from the main law of the European Union, specifically Article 8(3) of the Charter and Article 16(2) TFEU (Schrems v. Data Protection Commissioner, 2015, para 40).

The guarantee of national supervisory authorities' independence is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning individual protection in relation to the processing of personal data, and it must be interpreted in light of that aim. It was developed to increase the protection of persons and bodies harmed by the authorities' choices. The establishment of independent supervisory authorities in Member States is thus, as stated in recital 62 in the preamble to Directive 95/46, a fundamental component of the protection of individuals in relation to the processing of personal data.

To assure that protection, the national supervisory authorities must, in particular, strike a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests that need free flow of personal data (Schrems v. Data Protection Commissioner, 2015, para 42).

However, the operation of transferring personal data from a Member State to a third country involves, in itself, processing of personal data within the sense of Article 2(b) of Directive 95/46.

Transfers of personal data to third countries that do not provide an acceptable level of protection must be forbidden. Article 25 of Directive 95/46 puts a number of requirements on Member States and the Commission in order to restrict transfers of personal data to third countries based on the level of protection provided in each of those countries. That provision, in particular, makes it clear that the determination of whether a third country provides an acceptable degree of protection can be made by either the Member States or the Commission, as noted by the Advocate General in point 86 of his Opinion (Schrems v. Data Protection Commissioner, 2015, para 49-50).

As evidenced by the referring court's interpretations of the questions filed, Mr. Schrems claims in the main proceedings that US law and practice do not provide an acceptable level of protection under Article 25 of Directive 95/46. As the Advocate General observes in points 123 and 124 of his Opinion, Mr. Schrems expresses questions about the legitimacy of Decision 2000/520, which the referring court appears to share. In such circumstances, having reference to what has been stated in paragraphs 60 to 63 of the current judgment and in order to offer the referring court a thorough answer, it should be evaluated whether that decision conforms with the requirements arising from Directive 95/46 read in the light of the Charter (Schrems v. Data Protection Commissioner, 2015, para 67).

As demonstrated by the referring court's interpretations of the questions presented, Mr. Schrems alleges in the main proceedings that US law and practice do not guarantee an adequate level of protection under Article 25 of Directive 95/46. As the Advocate General notes out in paragraphs 123 and 124 of his Opinion, Mr. Schrems raises concerns regarding the legality of Decision 2000/520, which the referring court appears to share. In such circumstances, having regard to what has been stated in paragraphs 60 to 63 of the current judgment, and in order to provide a thorough response to the referring court, it should be determined whether that decision complies with the requirements arising from Directive 95/46 read in light of the Charter. First, as the text of Article 25(6) of Directive 95/46 indicates, that provision requires that a third country 'ensures' an acceptable level of protection through domestic legislation or international agreements. Second, the same paragraph assesses the adequacy of the third country's protection 'for the protection of the private life and basic freedoms and rights of individuals'(Schrems v. Data Protection Commissioner, 2015, para 70,71).

The word 'adequate' in Article 25(6) of Directive 95/46 clearly indicates that a third nation cannot be expected to provide a degree of protection equivalent to that guaranteed by the EU legal order.

However, as the Advocate General points out in point 141 of his Opinion, the term 'adequate level of protection' must be interpreted as requiring the third country to ensure, through domestic law or international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in light of the Charter. Using a self-certification system does not contradict Article 25(6) of Directive 95/46, which states that a third country must provide adequate protection through domestic law or international commitments. However, the system's reliability relies on effective detection and supervision mechanisms to ensure compliance (Schrems v. Data Protection Commissioner, 2015, para 81).

Decision 2000/520 establishes that 'national security, public interest, or law enforcement requirements' take precedence over the safe harbor principles, which means that self-certified United States organizations receiving personal data from the European Union are required to disregard those principles without limitation where they conflict with those requirements and thus prove incompatible with them.

Given the general nature of the derogation outlined in the fourth paragraph of Annex I to Decision 2000/520, that decision allows for interference with the fundamental rights of individuals whose personal data is or may be transferred from the European Union to the United States, based on national security and public interest requirements or domestic US legislation. To demonstrate the presence of an interference with the fundamental right to respect for private life, it is not important whether the information in question relating to private life is sensitive or if the persons concerned have experienced any unpleasant consequences as a result of that interference. In terms of the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees.

The requirement for such protections is all the more important when personal data is submitted to automatic processing and there is a considerable danger of illicit access to that data.

Without having to investigate the content of the safe harbor principles, it can be inferred that Article 1 of Decision 2000/520 fails to meet the conditions outlined in Article 25(6) of Directive 95/46, read in light of the Charter, and is thus illegal (Schrems v. Data Protection Commissioner, 2015, para 98).

On those grounds, the Court (Grand Chamber) hereby rules:

"1.Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

2.Decision 2000/520 is invalid."

After Edward Snowden's Controversy about how the United States National Security Agency obtained access to huge amounts of data provided to U.S. firms and organizations under the Safe Harbor Privacy Principles, this case brought the matter before the court. The principles specifically permitted departure from their safeguards whenever US statute imposed conflicting responsibilities on those firms and organizations for the sake of national security, the public interest, or law enforcement requirements (Brkan, 2019).

The US's sectoral approach to data privacy differs from the EU's overall approach to data protection, presenting a difficulty. Although US observers argued otherwise, it was clear from a European perspective that the US did not give. Data protection and privacy advocates highlighted worries about a lack of compliance by US firms, as well as a lack of openness and enforcement by US authorities, notwithstanding the benefits of unrestricted personal data transfers for commercial interests. The European Commission diligently recorded their concerns in a series of studies on the Safe Harbor framework, culminating in two 2013 communications outlining the regime's flaws. The Court defined 'sufficient' as 'basically identical', increasing the level of protection required and limiting the European Commission's discretion (Craig and de Búrca 2021).

As mentioned in (European Agency for Fundamental Rights, 2018) “Following the Schrems case, the Court of Justice in 2014 gave a great impulse to the protection of personal data as enshrined in the Charter, by affirming the primacy of the European model of data protection over less protective legal systems:”

The Court noted that the Safe Harbor (now replaced by the Privacy Shield) applied only to US enterprises that adhered to it, and that US public agencies were not subject to it. Furthermore, the United States' national security, public interest, and law enforcement requirements took precedence over the Safe Harbor scheme, so US undertakings were required not to apply the scheme's protective rules whenever they conflicted with such requirements. The United States Safe Harbor scheme thus allowed interference with the fundamental rights of persons as enshrined in the Charter by United States public authorities, and the Commission's decision of adequacy did not refer to the existence of rules in the United States intended to limit any such interference or the existence of effective legal protection against the interference, but only to the formal adequacy of the Safe Harbor scheme (European Agency for Fundamental Rights, 2018).

The ECJ at paragraph 94 opined that “In particular, legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter”.

Cross-border data transfers must comply with GDPR safeguards in two ways: data transfers must be compliant not only with the lawfulness of processing but also with the special provisions set out in Articles 44-49. This also includes subsequent transfers.

In addition to consent, Article 6 of the General Data Protection Regulation (GDPR) specifies additional authorization grounds, such as contract fulfillment or the protection of essential interests. Article 9 of the GDPR establishes different legal obligations for sensitive personal data that require a higher level of protection. Once the general conditions for data transfers have been met, the next stage is to establish if transfers to a third nation are permissible. Secure third countries are those for whom the European Commission has recognized an adequate level of data protection through an adequacy judgment. Transferring data to certain countries is clearly approved (European Agency for Fundamental Rights, 2018).

On February 2, 2016, the European Commission and the United States Department of Commerce achieved an agreement on a new framework for transatlantic transfers of personal data for commercial reasons, known as the EU-U.S. Privacy Shield (IP/16/216). This new framework will protect individuals' fundamental rights when their data is transferred to the United States and provide legal clarity for corporations. The College of Commissioners formally endorsed the Privacy Shield on July 12, 2016, following an affirmative vote by the Member States (article 31 committee) on July 8.

The EU-US Privacy Shield incorporates the conditions outlined by the European Court of Justice in its opinion on October 6, 2015, which found the previous Safe Harbor system invalid (European Commission, 2016).

3.2.3 Schrems II

The following case analysis is primarily based on the summary provided by Hendrik Mildebrath in the European Parliamentary Research Service's report on the CJEU judgment in the Schrems II case (Mildebrath, 2020).

In its July 2020 Schrems II judgment, the Court of Justice of the European Union (CJEU) declared the European Commission's Privacy Shield Decision invalid due to invasive US surveillance

programs, rendering personal data transfers illegal. Furthermore, the Court imposed stricter criteria for the transfer of personal data using standard contract clauses (SCCs). When transferring data using SCCs, data controllers or processors must ensure that the data subject receives a level of protection comparable to the GDPR and the EU Charter of Fundamental Rights. Additional measures may be necessary to compensate for gaps in third-country legal systems. Otherwise, operators must cease the transmission of personal data beyond the EU.

The Privacy Shield framework allows for the authorized movement of personal data from the EU to the US while ensuring stringent data protection rules and safeguards. On the basis of this framework, EU (and later European Economic Area, EEA) enterprises could legally transfer personal data to US-based companies that were listed in the Privacy Shield list. The US Department of Commerce administers admission to this list, while the US Federal Trade Commission oversees compliance. While participation is voluntary, accredited organizations are required to follow the Privacy Shield Principles, which became enforceable under US law. Unjustified violation may result in legal action under section 5 of the Free Trade Commission Act or withdrawal from the Privacy Shield list. The July 2020 verdict aligns with the Court's recent efforts to tighten protection levels. Notably, the CJEU invalidated the 2004 Passenger Name Record (PNR) Agreement between the EU and the US in 2006, objected to the entry into force of the EU-Canada PNR Agreement in its Opinion 1/15 issued in 2017, and invalidated the Safe Harbor Decision in the Schrems I verdict in 2015.

On August 1, 2016, the Privacy Shield principles replaced the Safe Harbor principles, which were invalidated. Despite improvements, the European Parliament's 2018 resolution and the European Data Protection Board (EDPB) criticized the new law's privacy shortcomings. In February 2020, the Chair of the Parliament's Civil Liberties Committee also raised his worries after a delegation visit to the United States. In its 2019 third annual review of the Privacy Shield, the European Commission maintained the US level of data protection as appropriate.

Following the Schrems I verdict, Facebook Ireland explained that it sent data to its US parent firm through SCCs. Max Schrems reformulated his complaint with the Irish Data Protection Authority (DPA) on December 1, 2015. He argued that the SCC Decision did not justify the transfer of

personal data to the US due to interference with his fundamental rights to privacy, data protection, and effective judicial protection.

The DPA addressed Schrems' concerns in a draft decision and filed an action with the Irish High Court. The Court subsequently requested a preliminary hearing. Meanwhile, another transfer mechanism, the Privacy Shield Decision, emerged as relevant to the case, prompting the CJEU to rule on its legitimacy.

On July 16, 2020, the CJEU invalidated the European Commission's Privacy Shield Decision and upheld the validity of the SCC Decision while imposing stricter restrictions for SCC-based transfers. (i) The Court determined that the US did not provide an essentially equal, and thus sufficient, degree of protection as promised by the GDPR and CFR.US surveillance programs like PRISM and UPSTREAM violate data and privacy rights (Article 45(1) GDPR, read in conjunction with Articles 7, 8, and 52(1) CFR). These programs do not limit US authorities' powers and lack actionable rights for EU citizens against them.

The Ombudsman mechanism, contrary to the European Commission's adequacy findings, exacerbates deficiencies by interfering with the right to effective judicial protection (Article 45(1) GDPR, read in light of Article 47 CFR). This is due to concerns about the institution's independence and enforceability of decisions.

(ii) The Court upheld the legitimacy of the SCC Decision, stating that SCCs do not provide legal or illegal reasons for data transmission (no panacea). The CJEU requires data controllers or operators transferring data using SCCs to provide data subjects with a level of protection comparable to the GDPR and CFR, with additional measures to compensate for gaps in third-country legal systems. Otherwise, operators must halt data transfer. Supervisory authorities must monitor transfers and restrict transfers if they determine that data subjects are not offered substantially similar protection.

The Court's judgment means EU companies cannot legally send data to the US under the Privacy Shield arrangement. Companies who continue to transfer data using an invalid mechanism risk a €20 million penalty, or 4% of their global revenue, under Article 83(5)(c) GDPR.

However, analysts dispute the Court's broader implications for operators. Some argue that traditional SCCs can be used by most companies, while others suggest that SCCs should only be used for transfers to the US if they are not subject to surveillance laws or have 'additional safeguards' in place.

The DPA of North Rhine Westphalia warned that enterprises using US communication services or transatlantic cables may be exposed to US surveillance measures. To save SCC-based data transfers, such organizations would have to compensate for shortcomings in safety with - as yet undetermined - 'extra protections'. The Court emphasized that protective contract clauses are not binding on third parties or authorities, making them ineffective. Additionally, intelligence agencies' use of cryptanalytic and quantum computing raises concerns about the effectiveness of protective technical measures like encryption. The EDPB and the Conference of the German Data Protection Authorities (DSK) state that corporations can transfer data based on corporate regulations, but must assure essential equivalency. The EDPB's guidelines question the applicability of Article 49(1)(a) GDPR derogations for repeated data transfers, albeit affirming their viability. The EDPB has announced that enforcement would not be suspended during the regulatory grace period. The DPAs in Berlin, Hamburg, and the Netherlands advise blocking transfers to the United States. The Berlin DPA even recommends retrieving data from the US. Many DPAs emphasize the necessity for additional investigation and case-by-case assessments.

US Secretary of Commerce Wilbur Ross and Secretary of State Mike Pompeo expressed 9unhappiness with the verdict, citing potential negative impact on the US$7.1 million transatlantic economic partnership. Both emphasized the importance of data flows for economic growth as well as the post-Covid-19 recovery, and promised to collaborate closely with the EU. European Commission Vice-President Věra Jourová and Commissioner Didier Reynders agreed to collaborate and propose modernizing standard contract conditions. While Digital Europe and others support a third, longer-term adequacy agreement, Business Europe suggests an intermediate option to minimize negative economic impact.

US Secretary of Commerce Wilbur Ross and Secretary of State Mike Pompeo expressed unhappiness with the verdict, citing potential negative impact on the US$7.1 million transatlantic

economic partnership. Both emphasized the importance of data flows for economic growth as well as the post-Covid-19 recovery, and promised to collaborate closely with the EU. European Commission Vice-President Věra Jourová and Commissioner Didier Reynders agreed to collaborate and propose modernizing standard contract conditions. While Digital Europe and others support a third, longer-term adequacy agreement, Business Europe suggests an intermediate option to minimize negative economic impact.

Max Schrems and the European Data Protection Supervisor urge the US to modify its monitoring laws and comply with the Court's recommendations.

According to article 45 of GDPR:"1. A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its

participation in multilateral or regional systems, in particular in relation to the protection of personal data.

The main factor here is the adequate level of data protection. In the absence of a Commission adequacy decision indicating adequate data protection in the relevant third state, the data controller may proceed with the transfer with suitable preventative measures. The contract between the personal data exporter (controller) and the recipient, established in the EU11, may include standard data protection clauses (Tracol, 2020).

3.2.4 Tele2 Sverige AB v. post-och telestyrelsen

The requests were made in two proceedings between (i) Tele2 Sverige AB and Post- och telestyrelsen (the Swedish Post and Telecom Authority; 'PTS'), concerning an order sent by PTS to Tele2 Sverige requiring the latter to retain traffic and location data in relation to its subscribers and registered users (Case C-203/15), and (ii) Mr. Tom Watson, Mr. Peter Brice and Mr. Geoffrey Lewis, on the one hand, and the Secretary of State for the Home Department (United Kingdom) (European Court of Justice, 2016, para 1).

Directive 2002/58 states in Recitals 2, 6, 7, 11, 21, 22, 26, and 30 that it aims to uphold fundamental rights and ideals outlined in the Charter. This Directive, in particular, intends to ensure that the rights outlined in Articles 7 and 8 of the Charter are fully respected.

The Internet is upending established market structures by providing a single, worldwide platform for the delivery of a diverse variety of electronic communications services. Publicly available electronic communications services over the Internet provide new opportunities for users, but they also introduce new hazards to their personal data and privacy. This Directive does not address issues concerning the protection of basic rights and freedoms in activities that are not subject to Community law.

As a result, it does not alter the existing balance between the individual's right to privacy and the ability of Member States to take the measures referred to in Article 15(1) of this Directive that are

necessary for the protection of public security, defense, State security (including the State's economic well-being when the activities relate to State security matters), and the enforcement of criminal laws. As a result, this Directive has no bearing on Member States' ability to conduct lawful interception of electronic communications or take other measures, if necessary, for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the European Court of Human Rights. Such measures must be suitable, absolutely proportionate to their stated aim, and required in a democratic society, with adequate safeguards in conformity with the European Convention on the Protection of Human Rights and Fundamental Freedoms. (para 2,3) Article 3 of Directive 2002/58 entitled "Relevant Services" stipulates:

“This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices’(European Court of Justice, 2016, para 3).

Article 22 of Directive 95/46, which is in Chapter III of that directive, is worded as follows:

‘Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.”

The order for reference in Case C-203/15 indicates that the Swedish legislature amended the lagen (2003:389) om elektronisk kommunikation [Law (2003:389) on electronic communications; 'the LEK'] and the förordningen (2003:396) om elektronisk kommunikation [Regulation (2003:396) on electronic communications]. Both of these laws, in the versions pertinent to the dispute in the main proceedings, contain provisions governing the retention of electronic communications data and national authorities' access to it (European Court of Justice, 2016, para 15).

On 9 April 2014, Tele2 Sverige, a Swedish provider of electronic communications services, informed the PTS that, following the ruling in the case of Digital Rights Ireland and Others that Directive 2006/24 was invalid, it would cease to retain electronic communications data covered

by the LEK on 14 April 2014, and would erase data retained prior to that date (European Court of Justice, 2016, para 47).

On April 15, 2014, the Rikspolisstyrelsen (the Swedish National Police Authority, Sweden) filed a complaint with the PTS, alleging that Tele2 Sverige had stopped sending it the relevant on that basis, on June 19, 2014, the PTS told Tele2 Sverige that it had violated national legislation by neglecting to maintain the LEK-covered data for six months for the purpose of combating crime. The PTS issued a ruling on June 27, 2014, directing Tele2 Sverige to begin data retention no later than July 25, 2014.ata.Tele2 Sverige believed that the 2014 report was based on a misinterpretation of the Digital Rights judgment, and that the obligation to retain data violated the Charter's fundamental rights, so they filed an action before the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm) challenging the order of June 27, 2014.

Since that court dismissed the action on October 13, 2014, Tele2 Sverige filed an appeal with the referring court. The referring court believes that the Swedish legislation's conformity with EU law should be considered in light of Article 15(1) of Directive 2002/58. While that directive establishes the general rule that traffic and location data should be erased or made anonymous when no longer required for communication transmission, Article 15(1) introduces a derogation from that general rule by allowing Member States, where justified on one of the specified grounds, to limit that obligation to erase or render anonymous, or even to make provision for data retention. As a result, under some conditions, EU law permits for the keeping of electronic communications data.

In those circumstances, the Kammarrätten i Stockholm (Administrative Court of Appeal of Stockholm, Sweden) decided to halt the proceedings and refer the following questions to the Court for a preliminary determination:‘(1)Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime … compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

By the second question in Case C-698/15, the Court of Appeal (England & Wales) (Civil Division) seeks in essence to ascertain whether, in the Digital Rights judgment, the Court interpreted Articles

7 and/or 8 of the Charter in such a way as to expand the scope conferred on Article 8 ECHR by the European Court of Human Rights (European Court of Justice, 2016, para 48-51).

Paragraph 3 of Article 52 of the Charter aims to ensure consistency between the Charter and the ECHR without compromising the autonomy of Union law or the Court of Justice of the European Union. In particular, as specifically stated in the second line of Article 52(3) of the Charter, the first statement does not restrict Union law from giving more protection than the ECHR. Finally, Article 8 of the Charter addresses a basic right that differs from that guaranteed in Article 7 of the Charter and has no parallel in the ECHR. However, in accordance with the Court's settled case-law, the basis for making a request for a preliminary ruling is not to provide advisory opinions on general or hypothetical concerns, but rather that it is necessary for the proper resolution of a dispute affecting EU law. The response to the second question in Case C-698/15 does not appear to provide any interpretation of EU law essential for the resolution of the disagreement (European Court of Justice, 2016, para 127-132).

On those grounds, the Court (Grand Chamber) hereby rules:

"1.Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

2.Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent

administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

3.The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible" (European Court of Justice, 2016, para 134).

National metadata retention rules were scrutinized equally under EU law, resulting in similar outcomes (Craig & Búrca, 2021).

This decision highlights the significant impact of data retention on privacy and personal data protection, building on the Digital Rights Ireland case. This violates both Articles 7 and 8 of the EU Charter, as well as Article 11's provision of free expression. The Decision underlines the value of free expression as a foundation for a democratic society. Retaining data without the individual's knowledge might influence behavior and create a sense of perpetual surveillance. As technology advances, personal data is increasingly vulnerable to misuse and abuse. The decision is a great step towards protecting fundamental rights in the face of technological progress. Nonetheless, national authorities have defended data retention as important for maintaining national security. Thus, striking the right balance is tough. Member states must evaluate their national data retention regulations to comply with EU law and combat terrorism, while also ensuring public safety (Villarica, 2018).

The preservation of traffic and location data for all subscribers, registered users, electronic communication, and metadata was not differentiated or limited based on the aim sought. Retaining a person's data was not contingent on their involvement in severe crimes or their communications being significant for national security. Given the lack of either a required link between the retained data and a threat to public security, or time period or geographical area restrictions, the CJEU concluded that the national legislation went beyond what was strictly necessary for the purpose of combating serious crime. Given the lack of a requisite relationship between the retained data and a threat to public security, as well as time or geographical area constraints, the CJEU determined that the national legislation went beyond what was strictly necessary for combating serious crime. The CJEU ruled that national legislation requiring indiscriminate data retention without a threat to public security or specific conditions (e.g. time period, geographical area, group of people involved in a serious crime) goes beyond what is strictly necessary and cannot be justified in a democratic

context (Council of Europe, European Court of Human Rights, European Data Protection Supervisor, & European Union Agency for Fundamental Rights, 2018).

3.2.5 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others

On 11 August 2006, Digital Rights filed a case in the High Court, claiming that it possessed a mobile phone registered on 3 June 2006 and had used it since that day. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications, and " asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order" (Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others , 2014, para 17).

The High Court, finding that it would be unable to answer the problems presented about national law until the validity of Directive 2006/24 was first considered, decided to pause proceedings and refer the following questions to the Court for a preliminary determination:

"(a)Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime? And/or (b) Ensuring the proper functioning of the internal market of the European Union?

2.Specifically, (i)Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?

(ii) Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union ("the Charter")] and Article 8 ECHR?

(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv)Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?

3.To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?" (The Digital Rights Ireland case, 2014, para 18).

The origin of the request for a preliminary ruling in Case C-594/12 lies in several actions brought before the Verfassungsgerichtshof by the Kärntner Landesregierung and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants, respectively, seeking the annulment of Paragraph 102a of the 2003 Law on telecommunications (Telekommunikationsgesetz 2003), which was inserted into that 2003 Law by the federal law amending it (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) for the purpose of transposing Directive 2006/24 into Austrian national law. They take the view, inter alia, that Article 102a of the Telekommunikationsgesetz 2003 infringes the fundamental right of individuals to the protection of their data.

The Verfassungsgerichtshof is particularly concerned with whether Directive 2006/24 is compatible with the Charter because it provides for the long-term storage of numerous sorts of data relating to an unlimited number of individuals. The Verfassungsgerichtshof believes that data retention primarily affects individuals whose actions do not justify the retention of data about them. Those individuals are at a higher risk of authorities investigating the data relating to them, becoming acquainted with the content of those data, learning about their private lives, and using those data for multiple purposes, especially given the unquantifiable number of people who have access to the data for a minimum of six months.

According to Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24, the main objective of that directive is to harmonies Member States "by providers of publicly available electronic

communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organized crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter"(The Digital Rights Ireland case , 2014, para 21- 24).

Those data, taken together, may allow for very precise conclusions to be drawn about the private lives of the people whose data has been retained, such as their daily habits, permanent or temporary places of residence, daily or other movements, activities, social relationships, and the social environments they frequent (The Digital Rights Ireland case, 2014, para 27).

To demonstrate the presence of an interference with the fundamental right to privacy, it is not relevant whether the information on the private life implicated is sensitive or whether the people involved have been inconvenienced in any manner (The Digital Rights Ireland case, 2014, para 33).

The court at paragraph 34 of the case believe that :"... the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter." The responsible national authorities' access to the data represents an additional violation of that fundamental right. As a result, Articles 4 and 8 of Directive 2006/24, which establish rules for the access of competent national agencies to data, violate the rights provided by Article 7 of the Charter as well.

The responsible national authorities' access to the data represents an additional violation of that fundamental right. As a result, Articles 4 and 8 of Directive 2006/24, which establish rules for the access of competent national agencies to data, violate the rights provided by Article 7 of the Charter as well (The Digital Rights Ireland case, 2014, para 34-35).

The battle against international terrorism in order to maintain international peace and security is a purpose of universal interest, as evidenced by the Court's case law. The same applies to the fight

against serious crime in order to guarantee public security. Regarding the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, given the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities that are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable. As a result, the preservation of such data may be deemed reasonable for achieving the goal targeted by that directive (The Digital Rights Ireland case , 2014, para49).

That assessment cannot be called into question by the fact, cited in particular by Mr. Tschohl and Mr. Seitlinger, as well as by the Portuguese Government in their written observations submitted to the Court, that there are several methods of electronic communication that do not fall within the scope of Directive 2006/24 or allow for anonymous communication. While this circumstance does limit the effectiveness of the data retention measure to achieve the desired result, it does not render the measure inappropriate, as the Advocate General points out in paragraph 137 of his Opinion

Regarding the necessity of data retention as required by Directive 2006/24, it must be noted that the fight against serious crime, particularly organized crime and terrorism, is critical to ensuring public security, and its effectiveness may be heavily reliant on the use of modern investigation techniques. However, no matter how vital an objective of common interest is, it does not justify a retention measure like the one created by Directive 2006/24 as being necessary for the purpose of that struggle (The Digital Rights Ireland case, 2014, para 51).

In terms of the right to respect for private life, the preservation of that fundamental right requires, according to the Court's recognized case-law, that derogations and limitations in connection to the protection of personal data must apply only in so far as is strictly necessary (The Digital Rights Ireland case, 2014, para 52).

Regarding the question of whether the interference caused by Directive 2006/24 is strictly necessary, it should be noted that, pursuant to Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail, and Internet telephony. As a result, it applies to all forms of technological communication, which are becoming increasingly common and

important in people's lives. Furthermore, under Article 3 of regulation 2006/24, the regulation applies to all subscribers and registered users. As a result, it infringes on the fundamental rights of nearly all Europeans (The Digital Rights Ireland case, 2014, para 52).

Directive 2006/24 has a broad impact on all individuals who use electronic communications services, although it does not put those whose data are retained in a situation that could lead to criminal prosecution. It applies even to people for whom there is no evidence that their actions have any connection to major crime, no matter how indirect or remote. Furthermore, it has no exceptions, therefore it applies even to people whose conversations are subject to professional secrecy requirements under national law.

“On those grounds, the Court (Grand Chamber) hereby rules:

Directive 2006/24/EC 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 is invalid” (The Digital Rights Ireland case, 2014, para 73).

Digital Rights Ireland Ltd. is a combination of actions from Ireland and Austria challenging the 2006 EU Data Retention Directive. The order was issued during the United Kingdom's leadership of the Council of Europe, following the 2005 London bombings and heightened security concerns. However, when the order was adopted, there were early indicators of problems. Several states' constitutional courts rejected implementing legislation, and Sweden paid a three million Euro fee for refusing to execute the directive.

The court ruled that metadata allows officials to establish accurate conclusions about a person's private life, while dragnet data gathering causes a chilling effect due to the perception of constant observation. Retaining and providing government access to data violates privacy and protection. The court determined that surveillance is necessary for public security, which is a basic right under Article 6 of the Charter. However, the directive's retention and access requirements were disproportionate to that interest.

The mandate was overbroad because it applied to all data, regardless of suspicion, and did not include any criteria for limiting government access or protections to avoid abuse. The directive did

not establish "clear and precise rules" for accessing data or determining how long nations should keep it. Furthermore, the data retention policy was not "strictly necessary" to protect public safety. It is important to recognize that these cases did not entirely dismiss the importance of security and freedom of information (quite to the contrary), but the court recognized that advances in technology have fundamentally changed the world's capability to intrude upon a person's private life (Gibson, 2014).

Conclusion:

Nowadays, the importance of privacy is no longer deniable. Although privacy has a long history, with the emergence of new communications, the importance of this issue is felt more than ever. Privacy and the right to have it are one of the legal rights that always have a special place in legal discussions, and many experts have written about this issue. This right, like other ones, has always seen the color of change. Having privacy gives a person peace of mind and inner satisfaction and preserves their dignity. But this right, like many other rights, is sometimes attacked and violated.
Privacy is not an impenetrable barrier like rights such as freedom from torture, but rather, this right possesses the ability to be flexible when it conflicts with more fundamental rights.
The exploration of the right to privacy and data protection within the European legal system in these three chapters indicates the strong relationship between individuals' rights and societal interests in a world that is rapidly becoming more digitized. As Brkan (2019) mentions "in the constitutional shaping of the concept of the essence of fundamental rights, the case law of the Court of Justice of the EU ("CJEU" or "the Court") in the field of privacy and data protection plays a crucial role".
Chapter 1 discusses the evolution of privacy and its journey up to recent years, culminating in the establishment of data protection measures. It emphasizes the dynamic nature of privacy and data protection, which introduce new demands. In this chapter the similarities and differences between privacy and data protection studied.
Chapter 2 discussed the ECHR cases in terms of privacy. The article 8 of the European Convention on Human Rights serves as the main source for evaluating these cases.

Case of Halford v. The United Kingdom (1997) was one of the pioneer cases about workplace privacy which was also impacted by technology development. Malone's case protected privacy rights against public authorities and showed that the government should be bound by law and they have limitations.

The case of Barbulescu v. Romania expanded the privacy areas to the workplaces too. Beside that it dedicated this role which reasonable expectation is a necessary role in employer and employee relationship. This progress is also mentioned in GDPR article 88:

”1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the workplace.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.
The ECtHR decided that the employer's monitoring of the applicant's personal communications via a work-provided messaging platform violated his right to privacy. These cases established vital steps for protecting people from arbitrary surveillance by state authorities or employers.

Chapter 3 showed the importance of CJEU decisions in shaping EU data law. The CJEU supported individuals' rights to control their personal data and put restrictions on data processing activities by private firms and public authorities.

Google Spain struck a compromise between privacy and public access to information, whereas Digital Rights Ireland Ltd. prioritized security.

The CJEU determined that, in certain instances, search engine operators may be forced to remove connections to third-party websites from search results lists based on a person's name. This may be true even if the content of the third-party website is completely legal. The court found that search results can create a profile of a person's private life by combining seemingly unrelated facts. The court ruled that individuals can submit requests to search engine operators to delete personal

data linkages from search results connected with their names. In most cases, a person's privacy and data protection rights under Articles 7 and 8 of the Charter take precedence over the operator's economic and public interests in making information available through a search. However, there may be specific reasons that justify interfering with their rights. The sensitivity of the data, the relevance of the data in the requestor's public life, the public interest in having the information linked, and the age of the data are all factors that must be addressed on an individual case basis. The court ruled that there is no obligation for the data prejudice the requestor (Gibson, 2014).

Both Schrems v. Data Protection Commissioner and Schrems II Cases discuss the privacy shield framework and concerns regarding the adequate level of protection for personal data transferred from the EU to the US. Data transfers have been impacted by the CJEU decision. The invalidation of the Privacy Shield had a significant impact on data transfers, requiring companies to find alternatives. In Schrems II (2020) the court highlights the divergence between EU and US legal frameworks concerning data protection.

References

1. Arnull, A. (2010). The Court of Justice of the European Union: Multidisciplinary Perspectives (Swedish Studies in European Law, Vol. 10). Oxford University Press.
2. Barnett, H. (2002). Constitutional and Administrative Law (4th ed.). Routledge. https://www.taylorfrancis.com/books/9781135331103
3. Boyle, Fiona. (1997) Right to private life european convention on human rights articles & (and) 13 private life correspondence interception of telecommunications effective domestic remedy halford v. the United Kingdom; european court of human rights. Journal of Civil Liberties, 2(3), 224-228
4. Brkan, M. (2019). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. German Law Journal, 20(6), 864-883. doi:10.1017/glj.2019.66
5. California Attorney General. (2023, September 1). California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa
6. Chesterman, S. (2010). "Ordinary Citizens" or a License to Kill? The Turn to Law in Regulating Britain's Intelligence Services. Buffalo Public Interest Law Journal, 29(1). Retrieved from https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=1035&context=bpilj
7. Claire E M Jervis, Barbulescu v Romania: Why There is no Room for Complacency When it Comes to Privacy Rights in the Workplace, Industrial Law Journal, Volume 47, Issue 3, September 2018, Pages 440–453, https://doi.org/10.1093/indlaw/dwy002
8. Council of Europe, European Court of Human Rights, European Data Protection Supervisor, & European Union Agency for Fundamental Rights. (2018). Handbook on European data protection law (2018 edition).
9. Council of Europe. (2012). The European Court of Human Rights in 50 Questions European Convention on Human Rights. (1950). Article 8: Right to respect for private and family life. https://www.echr.coe.int/documents/convention_eng.pdf

10. Council of Europe. (2022). Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence. Retrieved from https://www.echr.coe.int/documents/d/echr/guide_art_8_eng
11. Court of Justice of the European Union. (2024). Retrieved from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en
12. Crocetti, P., Peterson, S., & Hefner, K. (2021). What is data protection and why is it important? https://www.techtarget.com/searchdatabackup/definition/data-protection
13. DeCew, J. (2016) Privacy and its importance with advancing technology Ohio Northern University Law Review, 42(2), 471-492.
14. Directorate General Human Rights and Rule of Law. (2018). Case law of the European Court of Human Rights concerning the protection of personal data. Council of Europe
15. Dörr, D., Weaver, R. L., & Kende, M. S. (Eds.). (2012). The right to privacy in the light of media convergence: Perspectives from three continents. De Gruyter.
16. Eckart, J. P. (2017). The court case heard around the world google spain sl v. agencia espanola de proteccion de datos the right to be forgotten and what it may mean to the United States. Dartmouth Law Journal, 15(1), 42-101.
17. European Agency for Fundamental Rights. (2018). Handbook on European Data Protection Law: 2018 Edition. Publications Office of the European Union http://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en
18. European Commission. (2016). Press release., Retrieved from https://ec.europa.eu/commission/presscorner/detail/hr/MEMO_16_2462
19. European Data Protection Supervisor. (2023, August 31). History of the General Data ProtectionRegulation Retrieved From https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

20. European Union. (2012). Charter of Fundamental Rights of the European Union. Available at https://www.refworld.org/docid/3ae6b3b70.html
21. Fact Sheets of the European Union. (2023, September 16). Personal Data Protection. Retrieved from http://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection.
22. Ford, M. (2002). Two conceptions of worker privacy. Industrial Law Journal, 31(2), 135–155. https://doi.org/10.1093/ilj/31.2.135
23. Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. Computer Law & Security Review (CLSR), 29, 522-530. Available at: http://works.bepress.com/serge_gutwirth/107/
24. Gibby, O. (2016). The Right to Privacy in Employment: A Comparative Analysis. Hart Publishing1
25. Gibson, E. (2014). Digital Rights Ireland Ltd. v. Minister for Communications & Google Spain SL v. Agencia Española De Protección De Datos (C.J.E.U.). International Legal Materials, 53(5), 889–926. doi:10.5305/intelegamate.53.5.0889
26. Gormley, K. (1992). One hundred years of privacy. Wisconsin Law Review, 1992(5), 1335-1442.
27. Gov.uk. (2023, September 3). Data Protection. https://www.gov.uk/data-protection
28. Himma, K. E. (2007). Privacy vs. Security: Why Privacy is Not an Absolute Value or Right. Social Science Research Network.
29. Holvast, J. (2009). History of Privacy. In V. Matyáš, S. Fischer-Hübner, D. Cvrček, & P. Švenda (Eds.), The Future of Identity in the Information Society. Privacy and Identity 2008. IFIP Advances in Information and Communication Technology, vol 298. Springer. https://doi.org/10.1007/978-3-642-03315-5_2
30. Kovalenko, Y. (2022). The right to privacy and protection of personal data: emerging trends and implications for development in jurisprudence of European court of human rights. Masaryk University Journal of Law and Technology, 16(1), 37-58.

31. Kulhari, S. (2018). Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity (1st ed.). Nomos Verlagsgesellschaft mbH. http://www.jstor.org/stable/j.ctv941qz6
32. Mann, Jane. (2002). Privacy at work in the United Kingdom. International Business Lawyer, 30(4), 150-154.
33. Marshall, J. (2009) Chapter 2. Personal freedom and human rights law Personal Freedom through Human Rights Law? 11–32. https://doi.org/10.1163/ej.9789004170599.i-234.6
34. McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. Big Data & Society, 4(1), 205395171668699. https://doi.org/10.1177/2053951716686994
35. Mildebrath, H. (2020, September). The CJEU judgment in the Schrems II case. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
36. Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life American Behavioral Scientist (Stanford University Press), 58.
37. Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations Informing Science: The International Journal of an Emerging Transdiscipline, 19, 277–301
38. Politou, E., Alepis, E., Virvou, M., & Patsakis, C. (2021). Privacy and Data Protection Challenges in the Distributed Era. Springer. https://doi.org/10.1007/978-3-030-85443-0
39. Post, R.C. (2000). Three concepts of privacy. Geo Law J., 89, 2087.
40. Schabas, W. A. (2015), The European Convention on Human Rights: A Commentary, Oxford
41. Streinz, T. (2021). The Evolution of European Data Law. In P. Craig & G. de Búrca (Eds.), *The Evolution of EU Law* (3rd ed.). Oxford. https://doi.org/10.1093/oso/9780192846556.003.0029

42. Sychenko, E., & Chernyaeva, D. (2019). The Impact of the ECHR on Employee's Privacy Protection. Italian,abour Law e-Journal, 12(2), Article 10015. https://doi.org/10.6092/issn.1561-8048/10015
43. Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. ACM SIGCAS Computers and Society, 31(1), 6–11.
44. Taylor, Mistale. (2017). Google spain revisited: the misunderstood implementation of landmark decision and how public international law could offer guidance. European Data Protection Law Review (EDPL), 3(2), 195-208.
45. Thomson, J. (1984) 'The Right to Privacy in Schoeman, D. F. Philosophical Dimensions of Privacy, Cambridge, Cambridge University Press, pp. 272-289
46. Tracol, X. (2020). "Schrems II": The return of the Privacy Shield. Computer Law & Security Review, 39, 105484. https://doi.org/10.1016/j.clsr.2020.105484
47. Villarica, M. M. F. (2018). Tele2 Sverige AB v. Post-Och Telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, and Geoffrey Lewis (C.J.E.U.). International Legal Materials, 57(1), 125–154. doi:10.1017/ilm.2018.4
48. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy, Harvard Law Review, 4(5), 193. https://doi.org/10.2307/1321160
49. Westin, A. F. (1967). Privacy and freedom. New York, NY: Atheneum.

Cases:

1. *Barbulescu v. Romania, Application no. 61496/08, Judgment of 5 September 2017. Retrieved from https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-177082%22%5D%7D*
2. *CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post- och telestryrelsen and Secretary ofState for the Home Department v. Tom Watson and Others [GC], 21 December 2016*
3. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, [2014] ECLI:EU:C:2014:238, 2014 2 C.M.L.R. 41 (CJEU).*
4. *European Parliamentary Research Service. (2020). The CJEU judgment in the Schrems II case. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf*
5. *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12 (2014). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131*
6. *Halford v. United Kingdom, Application no. 20605/92, Judgment of 25 June 1997. Retrieved from https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-58039%22]}*
7. *Malone v. United Kingdom, Application no. 8691/79, Judgment of 2 August 1984. Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76869%22]}*
8. *Rotaru v Romania, Application no. 28341/95, Judgment of 4 May 2000. Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}*
9. *Schrems v. Data Protection Commissioner, Case C-362/14 (2015). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362*